



Kaseya 2

**Virtual System
Administrator™**

User Guide

Version 7.0

English

January 28, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at <http://www.kaseya.com/legal.aspx>. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Configuration	1
Configuring the Server.....	2
System Security.....	2
Minimum System Requirements	2
Updating or Moving the VSA	2
Logon and Browser Settings	3
Getting Started	7
VSA Modules.....	8
Page Layout	8
Notification Bar	10
Toolbox.....	11
Status Monitor	12
Administrator Notes.....	12
Bookmarks.....	13
Logoff.....	14
Color Scheme	14
Agents.....	14
Check-in Icons.....	15
Live Connect.....	15
Quick View.....	16
Agent Badges.....	16
Data Table Column Options.....	17
Learning More	18
Agent	19
Agent Overview	20
Agents	21
Agent Icons	21
Machine ID / Machine Group Filter	23
View Definitions	24
Filter Aggregate Table	27
Advanced Filtering	27
Agent Status	28
Agent Logs	31
Log History	32
Event Log Settings	34
Deploy Agents	35
Creating an Agent Install Package.....	37
Manually Installing the Agent	37
Automating the Installation of the Agent	38
Maintaining Agent Install Packages	39
Configuring Agent Settings	40
Configuring Agent Settings Using Policies	41
Configuring Agent Settings Using Templates.....	41
Agent Install Command Line Switches	42
Install Issues and Failures.....	44

Installing Multiple Agents	44
Installing Linux Agents	46
Supported Linux Functions	47
Supported Apple Functions	48
Create	48
Delete	52
Rename	53
Change Group	55
Copy Settings	55
Import / Export	57
Suspend.....	58
Agent Menu	59
Check-In Control.....	61
Working Directory	64
Edit Profile	65
Portal Access.....	67
Enabling Ticketing for Portal Access Users on Unsupported Browsers	68
Set Credential.....	68
LAN Cache	69
Assign LAN Cache	72
Update Agent.....	72
File Access	74
Network Access.....	75
Application Blocker	77

Agent Procedures **79**

Agent Procedures Overview.....	80
Schedule / Create	80
Action Buttons	81
Scheduling Agent Procedures.....	82
Creating / Editing Agent Procedures.....	83
IF-ELSE-STEP Commands.....	84
64-Bit Commands.....	103
Using Variables	104
Variable Manager	107
Manage Files Stored on Server	108
Folder Rights	108
Distribution.....	109
Agent Procedure Status	110
Pending Approvals	111
Patch Deploy	112
Application Deploy.....	113
Creating Silent Installs	115
Packager.....	116
Get File	116
Distribute File.....	118
Application Logging	119

Audit **121**

Audit Overview	122
View Assets	123
vPro tab	125
Manage Credentials	126

Credentials Log	127
Run Audit.....	128
Audit Summary	129
Configure Column Sets	131
Machine Summary.....	131
System Info.....	134
Installed Applications.....	136
Add/Remove.....	137
Software Licenses	137
Documents	138

Info Center **139**

Inbox.....	140
Schedule.....	141
Reports	142
Report Definitions.....	143
Report Folder Trees	144
Publishing a Report Immediately	145
Data Filters	145
Scheduling / Rescheduling a Report.....	145
Managing Scheduled Reports.....	146
Approving / Rejecting Reports	147
Report and Report Set User Security.....	148
Setting the Report Header Logo	148
Report Sets.....	148
Report Set Definitions	149
Report Set Folder Trees.....	149
Report Templates	150
Folder Tree	152
Add / Edit Report Template.....	153
Table	155
Bar Chart.....	158
Pie Chart	161
Name Value Part	163
Report Parts	166
Name Value Parts	167
Folder Tree.....	168
Add / Edit Data Set.....	168
Well Known Parameters.....	170
Report Contexts	173
Name Value Instances	174
Cover Page, Header, Footer	175
Defaults.....	176
Legacy Report Definitions	176
Antivirus - Antivirus Installation Statistics.....	179
Anti-Malware - Anti-Malware Installation Statistics	179
Audit - Aggregate Table	179
Audit - Disk Utilization	179
Audit - Inventory	180
Audit - Machine Changes.....	180
Audit - Machine Summary.....	180
Audit - Network Statistics	181
Backup - Backup	182
Desktop Management - Power Savings.....	182
Desktop Management - User State.....	184

Executive - Executive Summary	184
System Activity.....	185
Network Health Score	186
KDS - Domain Activity	189
Data Backup Summary	189
Data Backup Usage Over Time	189
Logs - Admin Notes.....	190
Logs - Agent Log	190
Logs - Agent Procedure	190
Logs - Alarm Log.....	191
Logs - Configuration Changes	191
Logs - Event Logs	191
Logs - Event Logs Frequency	192
Logs - Log Monitoring	192
Logs - Network Statistics Log.....	192
Logs - Remote Control	193
Mobile Devices - Device Applications	193
Mobile Devices - Device Status	193
Mobile Devices - Device Summary	194
Mobile Devices - Lost Devices	194
Monitoring - Logs.....	194
Monitoring - Monitor 95th Percentile	195
Monitoring - Monitor Action Log	195
Monitoring - Monitor Alarm Summary	196
Monitoring - Monitor Configuration.....	196
Monitoring - Monitor Log	197
Monitoring - Monitor Set.....	197
Monitoring - Monitor Trending	197
Monitoring - Uptime History.....	197
Patch - Patch Management.....	198
Policy Management - Agents Policy Status	199
Policy Management - Policy Info & Association.....	199
Security - Configuration.....	199
Security - Security	199
Security - Historical Threats	200
Security - KES Log.....	200
Service Billing - Past Billed Invoices	200
Service Billing - Sales Order Summary.....	200
Service Billing - Unbilled Revenue by Customer	201
Service Billing - Unbilled Revenue by Item Type	201
Service Billing - Work Order Summary	201
Service Desk - Custom Tickets	201
Service Desk - Service Goals	202
Service Desk - Service Hours	203
Service Desk - Service Times	203
Service Desk - Service Volumes.....	203
Service Desk - Tickets	204
Software - Software Applications Changed	204
Software - Software Applications Installed.....	205
Software - Software Licenses	205
Software - Software Licenses Summary	205
Software - Software Operating Systems.....	206
Software Deployment - Profile Status by Machine.....	206
Software Deployment - Recent Deployments	206
Software Deployment - Software Installed by Machine	207
Software Deployment - Machine Changes	207

Ticketing - Customizable Ticketing	207
Ticketing - Ticketing	208
Time Tracking - Timesheet Summary	209
Time Tracking - Timesheet Entries	209
Management Dashboard	209
View Dashboard	210
Layout Dashboard	211

Monitor **213**

Monitor Overview	214
Monitor Terms and Concepts	216
Dashboard List	219
Alarm List	220
Alarm Network Status.....	220
Alarm Summary Window	221
Alarm Rotator	222
Alarm Ticker	223
Network Status.....	223
Group Alarm Status.....	223
Monitoring Set Status.....	224
Machine Status	225
Device Status.....	226
Monitor Status	226
Machines Online.....	226
Top N - Monitor Alarm Chart.....	226
KES Status	226
KES Threats	226
Dashboard Settings	227
Alarm Summary	227
Suspend Alarm	229
Live Counter	230
Monitor Lists	231
Update Lists By Scan	232
Monitor Sets	234
Define Monitor Sets.....	235
Counter Thresholds.....	236
Enable Matching.....	239
Services Check	239
Process Status	240
Monitor Icons.....	241
SNMP Sets	241
Define SNMP Set	243
SNMP Set Details.....	244
Add SNMP Object	246
SNMP Icons	247
Alerts.....	248
Alerts - Summary.....	248
Alerts - Agent Status	250
Alerts - Application Changes.....	253
Alerts - Get Files.....	255
Alerts - Hardware Changes	258
Alerts - Low Disk	260
Alerts - Agent Procedure Failure.....	262
Alerts - Protection Violation.....	264
Alerts - New Agent Installed.....	266

Alerts - Patch Alert	268
Alerts - Backup Alert.....	271
Alerts - System	275
Event Log Alerts	276
Assign Event Set tab.....	279
Set Alert Actions tab.....	279
Edit Event Sets.....	280
Format Email Alerts for Event Sets	282
SNMP Traps Alert.....	283
Assign Monitoring	286
Auto Learn - Monitor Sets	290
Monitor Log.....	291
System Check	293
Assign SNMP	297
SNMP Quick Sets.....	302
Auto Learn - SNMP Sets.....	304
SNMP Log	305
Set SNMP Values.....	306
Set SNMP Type.....	308
Parser Summary.....	309
Log Parser	312
Log File Parser Definition.....	314
Assign Parser Sets	317
Log File Set Definition	322
Viewing Log Monitoring Entries.....	322

Remote Control **325**

Remote Control Overview	326
Control Machine	326
K-VNC Toolbar Options	328
Reset Password	330
Preinstall RC.....	331
Uninstall RC.....	332
User Role Policy	333
Machine Policy	334
FTP	336
SSH	338
Task Manager.....	338
Chat	339
Send Message.....	341
Kaseya Remote Control	342
Live Connect.....	344
Customized New Ticket Link.....	349

System **351**

System Overview.....	352
VSA Logon Policies.....	353
User Settings	353
Preferences	353
Scheduling and Daylight Savings Time	355
Change Logon.....	355
System Preferences	356
Check-in Policy.....	356

Naming Policy	358
User Security	359
Users	360
Master User vs. Standard Users	361
Create a New Master User	362
If Your Account Is Disabled.....	363
Changing Passwords Used by External Applications	363
User Roles.....	365
Machine Roles.....	367
Scopes	369
Sharing User-Owned Objects	370
Logon Hours.....	372
User History.....	372
Orgs/Groups/Depts/Staff	372
Manage	372
Manage - General tab	373
Manage - Machine Groups tab	374
Manage - Departments tab	374
Manage - Staff tab	375
Manage - Custom Fields tab.....	376
Manage - Systems Management tab.....	376
Set-up Types	376
Server Management.....	377
Request Support	377
Configure.....	377
Change Reporting Configuration	382
Indexing the Audit Results Table	384
Default Settings.....	384
License Manager.....	386
Import Center	388
System Log	389
Statistics	389
Logon Policy.....	391
Application Logging.....	392
Outbound Email.....	392
Customize.....	393
Color Scheme.....	393
Site Customization	394
Logon Page.....	394
Site Header	394
Agent Icons	395
Deploy Header	395
Org Custom Field Title	396
Creating Custom Agent Icons	396
Local Settings.....	397
Customize: Live Connect	398

Ticketing **399**

Ticketing Overview	400
View Summary	400
Create/View	403
Delete/Archive	405
Migrate Tickets	408
Notify Policy	408
Access Policy	410

Assignee Policy	411
Due Date Policy	411
Edit Fields	412
Email Reader	414
Email Mapping	416

Database Views 417

Database Views and Functions	419
Excel Usage	419
Crystal Reporting Usage	420
Views and Functions Provided	423
fnMissingPatchCounts_UsePolicy / fnMissingPatchCounts_NoPolicy	425
fnOSCounts	426
vAddRemoveList	427
vAdminNotesLog	427
vAgentConfiguration	427
vAgentLabel	428
vAlertLog	429
vBackupLog	430
vBaseApplicationInfo / vCurrApplicationInfo	431
vBaseCpuInfo / vCurrCpuInfo	432
vBaseDiskInfo / vCurrDiskInfo	432
vBaseDriveManufacturer / vCurrDriveManufacturer	433
vBasePciInfo / vCurrPciInfo	433
vBasePrinterInfo / vCurrPrinterInfo	434
vCollectionMember	434
vConfigLog	435
vEventDetail	435
vEventInstanceDetail	436
vEventInstanceHistoryDetail	438
vLicenseInfo	439
vMachine	440
vMonitorAlarmAlert	442
vMonitorAlarmCounter	443
vMonitorAlarmProcess	444
vMonitorAlarmService	445
vMonitorAlarmSNMP	446
vMonitorAlarmSystemCheck	447
vNetStatsLog	448
vNtEventLog	448
vOnBoardDeviceInfo	449
vPatchApprovalPolicyStatus	449
vPatchApprovalStatus	450
vPatchConfiguration	451
vPatchPieChartCountsNoPolicy	453
vPatchPieChartCountsUsePolicy	454
vPatchPolicy	454
vPatchPolicyMember	456
vPatchStatus	456
vPatchStatusByAgent	458
vPortInfo	461
vScriptLog	461
vScriptStatus	462
vSystemInfo	462
vSystemInfoManual	463

vTicketField	464
vTicketNote.....	464
vTicketSummary	465
vUptimeHistory	465
vvProAssetDetails	466

API Web Services 469

VSA API Web Service	470
VSA API Web Service - Overview.....	470
Enabling VSA API Web Service.....	471
Special Fields.....	471
Sample API C# Application.....	472
Sample API ASP Page	474
VSA API Web Service Security.....	477
Web Links - Inbound and Outbound	479
Limiting Requests by IP Address and User	481
VSA API Web Service - Operations	482
AddMachGrouptoScope.....	482
AddOrg.....	482
AddOrgDepartment.....	482
AddOrgDeptStaff.....	482
AddOrgToScope	483
AddScope.....	483
AddScopeOrg.....	483
AddTicRequest	484
AddUserToRole.....	484
AddUserToScope.....	484
AdminGroupAccess	484
AssignRole	484
AssignScope	485
Authenticate	485
AuthenticateWithAppSessionID.....	487
CloseAlarm.....	487
CreateAdmin	487
CreateAgentInstallPackage	487
CreateMachineGroup.....	488
CreateRole	488
DeleteAdmin.....	488
DeleteAgent	489
DeleteAgentInstallPackage.....	489
DeleteMachineGroup	489
DeleteOrg.....	489
DeleteRole	490
DeleteScope.....	490
DisableAdmin	490
Echo	490
EchoMt.....	490
EnableAdmin.....	491
GetAlarm	491
GetAlarmList	492
GetGroupLicenseInfo.....	493
GetLogEntry	493
GetMachine.....	493
GetMachineCollectionList	496
GetMachineGroupList	496

GetMachineList	497
GetMachineUptime	497
GetNotesList	498
GetOrgLocation	498
GetOrgTypes	498
GetOrgs	499
GetOrgsByScopeID	499
GetPackageURLs	500
GetPartnerUserLocation	500
GetPublishedViewColumns	500
GetPublishedViewRows	501
GetPublishedViews	503
GetRoles	506
GetScopes	506
GetSessionDetails	506
GetTicket	507
GetTicketList	508
GetTicketNotes	508
GetTicRequestTicket	508
GetVerboseMachineGroupList	509
LockFunctionAccess	509
MergeAgent	509
MoveMachineToAnotherGroup	509
Primitives	510
RemoveUserFromRole	511
RemoveUserFromScope	511
RenameMachine	511
ResetPassword	512
RoleMembership	512
SendAdminMessage	512
SetAdminPassword	512
SetGroupLicenseInfo	513
SetLicenseByOrg	513
SetPartnerUserLocation	513
UpdateOrg	513
UpdateTicket	513
UpdateUser	515
Agent Procedure API Web Service	517
Enabling the Agent Procedure API Web Service	517
Agent Procedure API Web Service - Operations	517
AddScriptAssignment	517
AddScriptPrompt	517
Echo	517
EchoMt	518
GetScriptAssignmentId	518
GetScriptIdFromScriptName	518
Monitoring API Web Service	518
Enabling the Monitoring API Web Service	518
Monitoring API Web Service - Operations	519
AssignEventAlertToMachine	519
AssignEventLogMachineSettings	519
CreateEventSet	519
CreateEventSetDefinition	519
DeleteAllEventAlertsFromMachine	520
DeleteAllEventLogMachineSettings	520
DeleteEventAlertFromMachine	520

DeleteEventLogMachineSettings.....	520
DeleteEventSet	520
DeleteEventSetDefinition	521
GetEventAlertList	521
GetEventLogMachineSettingsList.....	522
GetEventSetDefinitionList	523
GetEventSetList	523
KSD API Web Service	523
Enabling KSD API Web Service.....	523
KSD API Web Service Data Types	524
RefItem.....	524
CustomField	524
Note.....	524
Attachment	525
RelatedIncident	525
ServiceDeskDefinition.....	525
Incident Summary	528
Incident.....	528
KSD API Web Service - Operations.....	530
AddIncident	530
AddServDeskToScope.....	531
GetIncident	531
GetIncidentList	531
GetIncidentList2	532
GetServiceDesk	533
GetServiceDesks	533
Primitives.....	533
QueueAddIncident	534
UpdateIncident.....	534
Sample Messages.....	534
GetServiceDesks Request.....	535
GetServiceDesks Response	535
GetServiceDesk Request.....	535
GetServiceDesk Response.....	535
GetIncidentList Request.....	542
GetIncidentList Response.....	542
GetIncident Request	542
GetIncident Response	542
AddIncident Request.....	544
AddIncident Response.....	544
Update Incident Request	545
UpdateIncident Response.....	546

Glossary	547
-----------------	------------

Index	567
--------------	------------

Chapter 1

Configuration

In This Chapter

- Configuring the Server.....2
- System Security.....2
- Minimum System Requirements2
- Updating or Moving the VSA2
- Logon and Browser Settings3

Configuring the Server

The server is the heart of the system. Users access all functions through this server's web interface. The agents, on all managed machines, connect to this server to get any instructions/tasking orders. Your server must be accessible to both users and agents.

For configuring the server, see the latest [installation instructions](#)

(<http://help.kaseya.com/webhelp/EN/VSA/7000000/install/index.asp#home.htm>).

System Security

We designed the system with comprehensive security throughout. Our design team brings over 50 years of experience designing secure systems for government and commercial applications. We applied this experience to uniquely combine ease of use with high security.

The platform's architecture is central to providing maximum security. The agent initiates all communications back to the server. Since the agent will *not* accept any inbound connections, it is virtually impossible for a third party application to attack the agent from the network. *The system does not need any input ports opened* on the managed machines. This lets the agent do its job in virtually any network configuration without introducing any susceptibility to inbound port probes or new network attacks.

The VSA protects against man-in-the-middle attacks by encrypting all communications between the agent and server with AES 256 using a key that rolls every time the server tasks the agent. Typically at least once per day. Since there are no plain-text data packets passing over the network, there is nothing available for an attacker to exploit.

Users access the VSA through a web interface after a secure logon process. The system never sends passwords over the network and never stores them in the database. Only each user knows his or her password. The client side combines the password with a random challenge, issued by the VSA server for each session, and hashes it with SHA-256. The server side tests this result to grant access or not. The unique random challenge protects against a man-in-the-middle attack sniffing the network, capturing the random bits, and using them later to access the VSA.

Finally, for maximum web security, the VSA web pages fully support operating as an SSL web site.

Minimum System Requirements

See up to date [minimum system requirements](#)

(<http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm>).

Updating or Moving the VSA

If you are updating from an earlier version of Kaseya to this version, or want to update or move your existing K2 server to the latest version, see the latest [installation instructions](#)

(<http://help.kaseya.com/webhelp/EN/VSA/7000000/Install/index.asp#home.htm>).

Logon and Browser Settings

To logon to Virtual System Administrator™

1. Use your browser to display the logon page of your VSA server.
2. Enter your user name and password.

Note: For initial logon, use the master user account name and password entered during installation.

3. Check the **Remember my username and domain (if any) on this computer** checkbox to save the username and domain name to a cookie on the local computer so you don't have to re-enter each time you log in. The password is not stored.

Note: The **Discovery** add-on module can be used to manage VSA user logons and Portal Access logons using domain logons (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#7293.htm>).

4. Click the **Logon** button.

Note: To prevent unauthorized access after making configuration changes, log off or close the session by terminating the browser application.

Enabling Browser Cookies, JavaScript and Popups

Your browser must have cookies and JavaScript enabled in order to proceed. Popups for the VSA website are recommended.

Internet Explorer

To Enable Cookies in Internet Explorer 9, 10, 11

1. Click the **Tools** menu or gear icon.
2. Select **Internet Options**.
3. Switch to the **Privacy** tab.
4. Select a privacy setting no greater than **Medium High** (i.e. the setting must not be High nor Block All Cookies).
5. Click **OK**.

To Enable JavaScript in Internet Explorer 9, 10, 11

1. Click on the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Security** tab.
4. Click on **Internet** in the **Select a Web** content zone.
5. Press the **Custom level...** button.
6. Scroll down to the **Scripting** section.
7. In **Scripting of Java applets**, click the **Enable** option.
8. Click **OK**.

To Enable Popups in Internet Explorer 9, 10, 11

1. Click the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Privacy** tab.

Configuration

4. Click **Settings**. The **Pop-up Blocker Settings** dialog displays.
5. Enter the URL or IP address of your VSA in the **Address of website to allow** field.
6. Click **Close**, then **OK**.

Firefox

To Enable Cookies in Firefox

1. Click the **Firefox** menu.
2. Select **Options**.
3. Switch to **Privacy** settings.
4. Set History to **Remember History**. (You can also **Use custom settings for history** and make sure **Accept cookies from site** is checked.)
5. Click **OK**.

To Enable JavaScript in Firefox

1. Click the **Firefox** menu.
2. Click **Addons**.
3. Click **Plugins**.
4. Click the **Java** plugin to select it.
5. Select the **Always Activate** option.

To Enable Popups in Firefox

1. Click on the **Firefox** menu.
2. Select **Options**.
3. Switch to the **Content** tab.
4. Click **Exceptions...** The **Allowed Sights - Pop-ups** dialog displays.
5. Enter the URL or IP address of your VSA in the **Address of web site** field.
6. Click **Allow**.
7. Click **Close**, then **OK**.

Chrome

To Enable Cookies in Chrome

1. Click the **Wrench** icon.
2. Select **Settings**.
3. Click **Show advanced settings**.
4. In the **Privacy** section, click **Content settings**.
5. Select the **Allow local data to be set (recommended)** option.
6. Click **OK**, then **Close** for all the parent dialogs.

To Enable JavaScript in Chrome

1. Click the **Wrench** icon.
2. Select **Settings**.
3. Click **Show advanced settings**.
4. In the **Privacy** section, click **Content settings**.
5. Select the **JavaScript** feature.
6. Select the **Allow all site sites to run JavaScript (recommended)** option.

7. Click **OK**, then **Close** for all the parent dialogs.

To Enable Popups in Chrome

1. Click the **Wrench** icon.
2. Select **Settings**.
3. Click **Show advanced settings**.
4. In the **Privacy** section, click **Content settings**.
5. Select the **Pop-ups** feature. (You may have to scroll down to see it.)
6. Select the **Do not allow any site sites to show pop-ups (recommended)** option.
7. Click **Manage Exceptions...** The **Pop-up Exceptions** dialog displays.
8. In the **Add new hostname pattern edit box** at the bottom of the list, enter the URL or IP address of your VSA.
9. Set **Action** to **Allow**.
10. Click **OK**, then **Close** for all the parent dialogs.

Chapter 2

Getting Started

In This Chapter

VSA Modules.....	8
Page Layout	8
Notification Bar	10
Toolbox.....	11
Status Monitor	12
Administrator Notes	12
Bookmarks.....	13
Logoff.....	14
Color Scheme.....	14
Agents	14
Check-in Icons.....	15
Live Connect.....	15
Quick View.....	16
Agent Badges	16
Data Table Column Options	17
Learning More	18

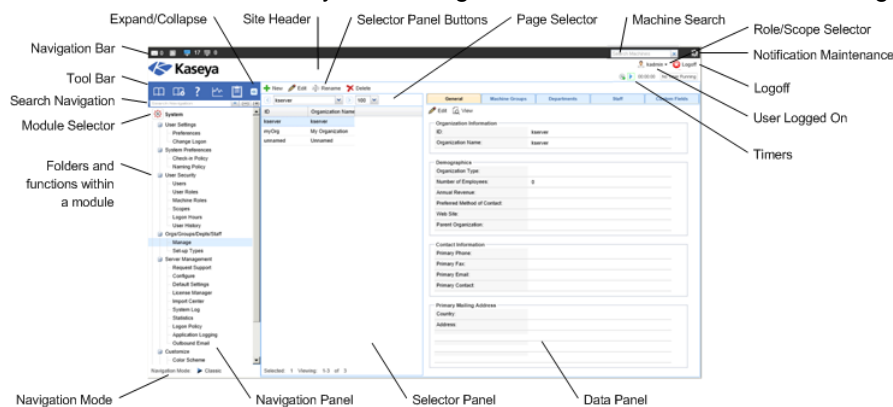
VSA Modules

All VSA functions can be accessed through modules located along the left side of the user interface. Within each module are the core functions that allow users to perform a variety of tasks on remotely managed **machines** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#6779.htm>) and the Kaseya Server.





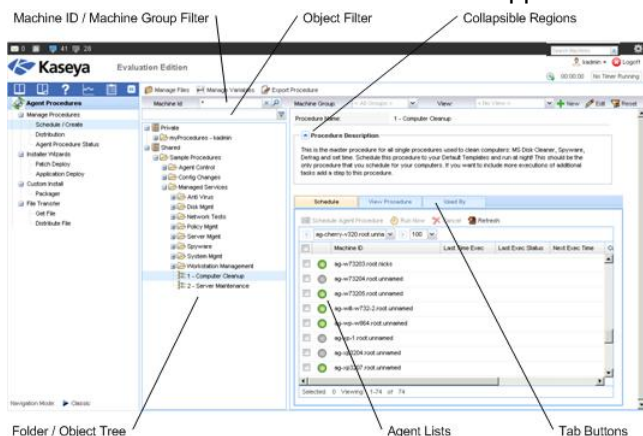
Page Layout

The user interface of Kaseya 2 is designed to be flexible while streamlining the choices a user makes.



- **Navigation Panel** - The module tabs and function panes are combined into a single expandible-collapsible explorer like navigation panel.
- **Navigation Modes** - Two modes are available:
 - **Tree-Based** - Allows you to select and expand individual folders within a module.
 - **Classic** - Displays one module at time. Defaults to fully expanded. Defaults to a collapsed folder view which can then be selectively expanded.
- **Selector Panel** - Many Kaseya 2 functions display a middle selector panel to select one or more records. The selector panel can be scrolled, filtered and sorted independently from any other pane.
- **Data Panel** - On the right hand side of the screen, is a data panel designed as a series of tabbed views, providing quick access to each property or data view no matter how complex a function might be. Many of the tabs have fields you can edit and buttons that provide additional functionality.

- **Module Selector** - At the top of the navigation panel is a module selector. Clicking the visible module displays all the installed modules in the VSA. Clicking any of the other modules selects that module and displays the folders and functions within that module the user has access rights to see.
- **Notification Bar** - Displays the status and counts for categories of notifications. Notifies you when a specified RSS feed has been updated.
- **Notification Maintenance** - Customizes the display of notifications, by category.
- **Toolbar** - The toolbar, just above the module selector, provides instant access to the global functions **Show Bookmarks**, **Add Bookmark**, **Help**, **Status**, and **Notes**. This feature can be hidden using the gear  icon in the top right corner of the **Notification Bar** (page 10).
- **Search Navigation** - Enter a string to find all navigation items that match the string. This feature can be hidden using the gear  icon in the top right corner of the **Notification Bar** (page 10).
- **Expand/Collapse** - A << icon on the right side of the toolbar collapses the navigation panel. Once collapsed a >> icon expands the navigation panel.
- **Selector Panel Buttons** - At the top of the selector panel is a page-specific button bar. Typically these buttons include creating, editing and deleting records listed in the selector panel. Additional buttons display, depending on the page and your logon access rights.
- **Page Selector** - If the selector panel list is longer than one page, the page selector enables you to browse through multiple pages. You can set the number of rows displayed on each page.
- **Site Header** - A customizable site logo and header text displays in the upper left corner.
- **Machine Search** - Enter a string without spaces into the edit box and all machine names containing that string display in a drop down list.
- **Role/Scope Selector** - Selects the combination of role and scope that is currently active for your logon. If you have more than one role or scope available to you, you can switch roles or scopes anytime during your logon.
- **Logged On User / Logoff** - Displays the username of the user currently logged on and a logoff link.
- **Unread Messages** - The number of unread messages displays in the upper right corner. You can click this counter at any time to display your VSA inbox immediately.
- **Timers** - Records time entries that can be applied to timesheets and other work type records.



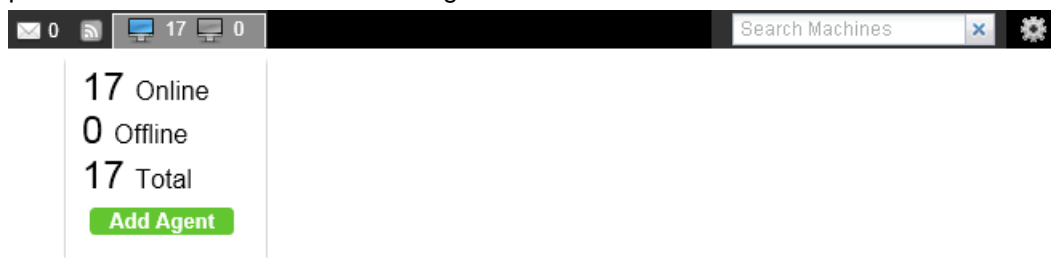
- **Machine ID / Machine Group Filter** - If a page displays an agent list, then the Machine ID / Machine Group filter displays at the top of the page. The filter enables you to limit the list of agents displayed on the machine, by individual machine, machine group, organization or by view definition.
- **Folder / Object Trees** - Certain functions display a folder tree in the selector panel instead of list of records. Typically two folder trees are provided, one **Private** and one **Shared**, but sometimes only the **Shared** folder tree displays. You can create new objects in these folder trees, and in the **Shared** folder tree, share them with other users.
- **Tree Filter** - All folder trees panels can be filtered by entering a string into the tree filter.

Getting Started

- **Agent Lists** - Agents lists display on many VSA pages. In the new user interface, agents frequently display in one of the tabs in the data panel on the right side of the page.
- **Tab Specific Buttons** - Any tab in the data panel on the right side of the page can display a tab specific set of buttons. Tab specific buttons affect the child record just below it. For example, when you want to run an agent procedure immediately, you select the procedure in the folder tree in the middle panel, then select one or more of the agents in the tab, then click the "Run Now" tab button to execute the agent procedure.
- **Collapsible Regions** - Panels, tabs and dialogs are sometimes segmented into collapsible regions. Clicking the down arrow lets you hide that region of the user interface. A collapsed region displays an expand button, enabling you to expand that region again.

Notification Bar

A notification bar displays at the top of the VSA window and is visible from any module. The bar's icons provide immediate notifications throughout the VSA environment.



Types of notifications include:

- **Service Desk tickets** - Multiple notification icons can be created for different desks, groups of desks, or other filter criteria.
- **RSS announcements** - Multiple icons for different RSS feeds can be specified.
- **System notifications** - Includes both "critical" and "warning" level system-level messages.
- **Inbox messages** - Multiple icons can be created for different types of inbox message.
- **Agents up / agents down counters** - Clicking either one of these counters displays a dialog that enables you to select an agent install package and immediately install it on the computer you are currently logged on to.



Machine Search

A **Machine Search** edit box displays on the right side of the notification bar. Enter a string without spaces into the edit box and all machine names containing that string display in a drop down list. Search strings are matched against the following types of information.

- display name
- current login
- last login name
- mach name
- admin contact
- contact name
- contact phone
- contact email
- ip address
- ipv6 address
- default gateway
- connection gateway ip
- primary wins server


- dns server 1
- dns serve 2
- os type
- os info
- mac addr
- org name
- group name

The drop-down list displays the following information for each machine ID found:

- The computer name.
- The VSA administrator name responsible for this machine ID.
- The contact name for this computer.
- The number of tickets associated with this machine. Click the  icon to display the tickets in a ticket table.
- The number of alarms associated with this machine. Click the  icon to to display the **Alarm Summary** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4112.htm>) page for this machine.

The `admin contact`, `contact name`, `contact phone`, and `contact email` can all be specified using the Agent > **Edit Profile** (*page 65*) page. All other fields are collected from audits and display on the Agent > **Agent Status** (*page 28*) page or Audit > **Machine Summary** (*page 131*) page.


Notification Bar Settings

A gear icon  at the far right of the notification bar provides access to **Notification Bar Settings**, enabling the user to customize the notification bar. Customization includes:

- Selecting different icons for each type of notification.
- Selecting which system-level warnings you want to be reminded of.
- Setting how "noticeable" the notification is: silent, subtle, or flyout.
- Using the separator bar to group icons.
- Hiding notifications that have no items to show.

You can also move any notification icon left or right simply by dragging it along the notification bar.

Left Side Navigation

A gear icon  at the far right of the notification bar provides access to a **Left Side Navigation** pair of options.

- **Shortcuts** - If checked, displays the tool bar above the navigation pane.
- **Search Navigation** - If checked, displays the search box above the navigation pane.

Alerts

Currently, the only alerts displayed by the notification bar are alerts generated using the **Agent Procedures SendAlert()** (*page 98*) command. Additional types of alerts will be supported in future releases.


Toolbox



The **Toolbox** provides the user with a common area to access frequently used commands and functions. The **Toolbox** is accessible from any module, giving users convenient access to frequently used features of the VSA.

Getting Started

Notes

Click the **Notes** icon  to display the **User Notes** (page 12) window. **User Notes** provides a place to record and retrieve what previous user actions were performed on each machine.

Status


Click the **Status** icon  to display the **Status Monitor** (page 12) window. **Status Monitor** continuously monitors selected machines, notifying you when they go online or offline.

Help

Click the **Help** icon  to display context-sensitive help for the currently selected function page.

Status Monitor

Toolbox > Status

The status monitor  continuously monitors selected machines, notifying you when they go online or offline. If someone is currently logged onto the machine, **Status Monitor** displays their user name in bold along with the IP address of the machine. Master role users can also display the list of logged on VSA users.

Turn off sound

A unique audible tone sounds each time a machine goes online, machine goes offline, a user logs in, or a user logs out. Turn these sounds off by checking this box.

Refresh Rate

Refreshes the browser every 30 sec, 1, 2, or 5 minutes. Each browser refresh gets the latest status from **Virtual System Administrator™**. To get an immediate update, click the **Refresh** link.

List logged on users

Uncheck this box to hide the list of users.

Note: This option is available to master role users only.

Sort By

List machines in any of the following order:


- **Connection Gateway** - Numerically, left to right, by IP address. Best for grouping machines by how they are connected on the network.
- **Group ID** - Alphabetically by group ID.
- **Machine ID** - Alphabetically by machine ID.

Hide offline machines

Uncheck this box to list all machines. Offline machines have a grayed out icon.

Administrator Notes

Administrator Notes allows you to log what you did to a machine or group of machines into the system database. The next time you have a problem with any machine, check the notes and see what other VSA users have done on that machine. The system time-stamps each administrator note and

associates the note with a VSA user name. Open the notes editor by clicking the Notes icon  in the **Toolbox** (page 11), or in **Live Connect** (page 344), **Machine Summary** (page 131), or **Quick View** (page 16).


Note: You can print **Administrator Notes** using **Info Center > Reporting > Reports > Logs - Admin Notes** (page 190).

Note: **Audit > Documents** (page 138) provides a different method of documenting a machine, by uploading documentation files for a specific machine to the Kaseya Server.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using **System > User Security > Scopes** (page 369). Check the box in front of the machines you wish to apply the note to.


Time

Displays the time-stamp when the note was first entered. The time-stamp can be edited by clicking the edit icon  next to the specific note whose time-stamp you wish to change.


Admin

Logon name of the user that entered the note. If a different user edits the note, this field is updated with the new user's name.

Delete the note

Delete the note by clicking the delete icon  next to it. If more than one machine has the same note entered by the same user and has the same time-stamp, the system asks if you want to delete all occurrences of the note.

Edit the note

Change a note by clicking the edit icon  next to it. Click the **Apply** button to commit the changes. Click **Cancel** to restore the original text. If more than one machine has the same note entered by the same user and has the same time-stamp, the system asks if you want to modify all occurrences of the note.

Note

Displays the user entered note for the selected machine.

Notes per Page

Number of notes to display at a time. Choices are 10, 30, and 100.

Bookmarks



You can bookmark any item on the navigation pane. Bookmarks are defined by user. If you work with the same set of navigation items each day, this can save you navigation clicks.




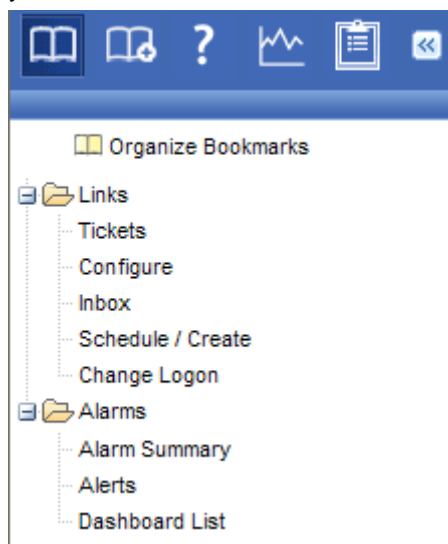
- Click the **Add Bookmark** icon to add a navigation item to your list of bookmarks.



- Click the **Bookmark Show** icon to display the list of bookmarks you have saved.

Getting Started

 - Click the **Organize Bookmarks** icon in the bookmark list to create bookmark folders and organize your bookmarks.



Logoff

Click the **Log Off** link to prevent unauthorized access to the server and return to the logon page. The **Log Off** link is located in the upper right-hand corner of the window and is accessible from any tab and function.

Note: For increased security, it is recommended that users log off and terminate all browser sessions when not administering the server.

Color Scheme

System > Customize > Color Scheme


The **Color Scheme** page determines the set of colors displayed by the VSA environment. **Color Scheme** selection applies to all users within the same **partition** (page 564).


To change color schemes:

1. Select a color scheme in the middle pane.
2. Click the **Set Scheme** button.

Agents









The VSA manages machines by installing a software client called an **agent** on a managed machine. The agent is a system service that does not require the user to be logged on for the agent to function and does not require a reboot for the agent to be installed. The agent is configurable and can be totally invisible to the user. The sole purpose of the agent is to carry out the tasks requested by the VSA user. Once installed:

- An agent icon—for example the  agent icon—displays in the system tray of the managed machine. **Agent icons** (page 21) can be custom images or removed altogether.


- Each installed agent is assigned a unique VSA **machine ID / group ID / organization ID** (page 556). Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available agent licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > **Deploy Agents** (page 35) inside the VSA.
- **Multiple agents** (page 44) can be installed on the same machine, each pointing to a different server.
- A **check-in icon** (page 15) displays next to each machine ID in the VSA, displaying the overall status of the managed machine. For example, the  check-in icon indicates an agent is online and the user is currently logged on.
- Clicking a check-in icon displays a single machine interface for the managed machine called **Live Connect** (page 15). **Live Connect** provides instant access to comprehensive data and tools you need to work on that one machine.
- Hovering the cursor over a check-in icon displays an **agent quick view window** (page 16) immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent quick view window.

Check-in Icons

Once a machine ID is created, an agent check-in icon displays next to each machine ID account in the VSA. These icons indicate the agent check-in status of each managed machine. Click a check-in icon to display **Live Connect** (page 15). Hovering the cursor over a check-in icon displays the **agent quick view window** (page 16).


-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Live Connect

Live Connect is a web-based, single-machine user interface. You can access **Live Connect** by Ctrl+clicking the agent icon , or by clicking **Live Connect** button in **Quick View** (page 16). **Live Connect** enables you to perform tasks and functions solely for one managed machine. A menu of tabbed property sheets provide access to various categories of information about the managed machine.



Additional menu items display, depending on the add-on modules installed and the operating system of the target machine.

This same **Live Connect** window displays when a machine user clicks the  agent icon in the system tray of the managed machine, with certain restrictions applied. This machine user view of **Live Connect**

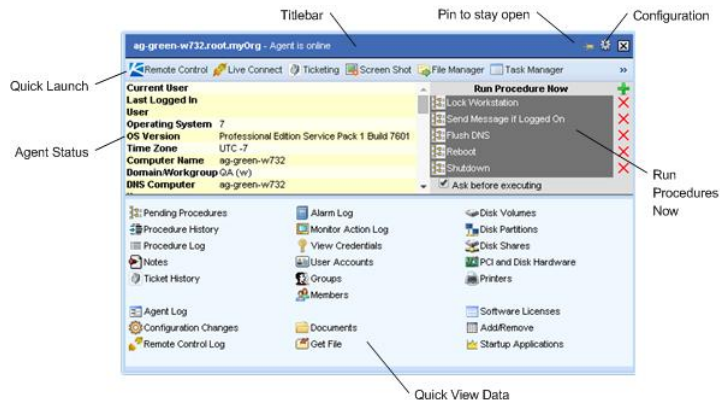
Getting Started

is called **Portal Access**.

Note: For more details, see [Remote Control > Live Connect](#) (page 344).

Quick View

Hovering the cursor over a check-in icon displays an agent **Quick View** window immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent **Quick View** window. You can use **agent badges** (page 16) to display **Special Instructions** text in the bottom of the the **Quick View** window.








Screen Shot

One function is unique to the **Quick View** window. Click the **Screen Shot** button to snap an image of the current desktop. You can access saved images by clicking the **Get File** folder icon in the same **Quick View** window.

Record Desktop

Applies only to machines assigned the WinVNC remote control type. The **Record Desktop** button records the desktop without launching a remote control session.

Agent Badges

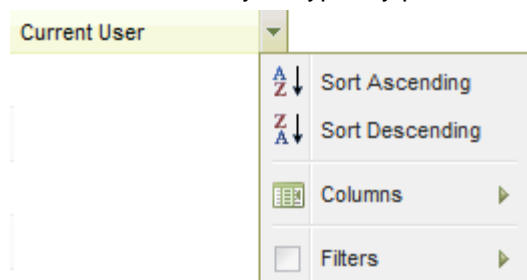
Add *badges* to the lower right corner of agent status icons, such as   . These badges display everywhere the agent icon displays in the user interface. For example, you could mark a machine with a  badge to indicate the customer requires a phone call before anyone works on that machine. Or mark a server with a  badge because you should not do anything to it until after hours.







Select one or more machines on the Agent > **Edit Profile** (page 65) page, then click the **Icon Badge** link at the top of the page and select one of the available badges. You can define a **Special Instructions** text message for each badge. Click the **Update** button to assign the badge to selected machines.

When you hover the cursor over an agent status icon with a badge, the **Quick View** (page 16) window displays the **Special Instructions** text in the bottom of the window.

Data Table Column Options

Data tables in Kaseya 2 typically provide the following column options.



- **Column Selection** - Click any column header drop-down arrow , then **Columns** to select which columns display in the table. Click the Sort Ascending  or Sort Descending  icons to sort the table by the selected column heading.
- **Column Sorting** - Click the Sort Ascending  or Sort Descending  icons to sort the table by the selected column heading.
- **Column Filtering** - Click the column drop-down arrow  to enter a filter value for that column. For example enter NS to find all rows that start with NS in that column. Enter NS%2 to find all rows that start with **NS** and end with 2 in that column. You can filter by multiple column filters if you like.
- **Flexible Column Widths** - Expand or collapse the width of each column by dragging the column header boundaries left or right.

Learning More

PDFs are available to help you quickstart your implementation of **Virtual System Administrator™**. They can be downloaded from the [first topic in the VSA online help](#) (<http://help.kaseya.com/webhelp/EN/VSA/7000000>).

If you're new to **Virtual System Administrator™** we recommend the following quickstart guides:

1. Getting Started
2. User Administration
3. [Agent Configuration and Deployment](#)
4. Remote Control Tools
5. Monitoring Configuration
6. Custom Reports

The following resources are also available.

Kaseya University

See [Kaseya University](#) (<http://university.kaseya.com>) for training options.

Chapter 3


Agent

In This Chapter

Agent Overview	20
Agent Status	28
Agent Logs	31
Log History	32
Event Log Settings	34
Deploy Agents	35
Create	48
Delete	52
Rename	53
Change Group	55
Copy Settings	55
Import / Export	57
Suspend	58
Agent Menu	59
Check-In Control	61
Working Directory	64
Edit Profile	65
Portal Access	67
Set Credential	68
LAN Cache	69
Assign LAN Cache	72
Update Agent	72
File Access	74
Network Access	75
Application Blocker	77

Agent Overview

Agent

Functions in the **Agent** module allow users to create, edit, and delete machine IDs, customize the appearance of the machine's agent icon  in the **system tray** (on page 564), control agent check-in frequency, and update the version of agent software that resides on managed machines.



Note: If you're new to agent installation, see the [Agent Configuration and Deployment](#) quick start guide.

Functions	Description
Agent Status (page 28)	Displays active user accounts, IP addresses and last check-in times.
Agent Logs (page 31)	Displays logs of: <ul style="list-style-type: none"> • Agent system and error messages • Execution of agent procedures, whether successful or failed. • Configuration changes made by a user. • Send/receive data for applications that access the network. • Application, System, and Security event log data collected from managed machine. • Alarm log • Remote control log • Log monitoring
Log History (page 32)	Specifies how long to store log data.
Event Log Settings (page 32)	Specifies event log types and categories included in event logs.
Deploy Agents (page 35)	Creates agent install packages for installing agents on multiple machines.
Create (page 48)	Creates machine ID accounts and/or install packages for installing agents on single machines.
Delete (page 52)	Deletes machine ID accounts.
Rename (page 53)	Renames existing machine ID accounts.
Change Group (page 55)	Reassigns machines to a different machine group or subgroup.
Copy Settings (page 55)	Mass copies settings from one machine account to other machine accounts.
Import / Export (page 57)	Imports and exports agent settings, including scheduled agent procedures, assigned monitor sets, and event sets, as XML files.
Suspend (page 58)	Suspends all agent operations, such as agent procedures, monitoring, and patching, without changing the agent's settings.
Agent Menu (page 59)	Customizes the agent menu on managed machines.
Check-In Control (page 61)	Controls agent check-in frequency on agent machines.
Working Directory (page 64)	Sets the path to a directory used by the agent to store working files.

Edit Profile (page 65)	Edits machine account information.
Portal Access (page 67)	Sets up accounts to allow machine users remote control access to their own machines.
Set Credential (page 68)	Sets a logon credential for the agent to use in Patch Management, the useCredential() procedure command, Endpoint Security, and Desktop Management.
LAN Cache (page 69)	Designates a machine to act as a file source for other machines on the same LAN.
Assign LAN Cache (page 72)	Assigns machines to, and removes machines from, a selected LAN Cache machine.
Update Agent (page 72)	Updates the agent software on managed machines.
File Access (page 74)	Prevents unauthorized access to files on managed machines by rogue applications or users.
Network Access (page 75)	Lets you approve or deny network access on a per application basis.
Application Blocker (page 77)	Application blocker prevents any application from running on a managed machine.

Agents

The VSA manages machines by installing a software client called an **agent** on a managed machine. The agent is a system service that does not require the user to be logged on for the agent to function and does not require a reboot for the agent to be installed. The agent is configurable and can be totally invisible to the user. The sole purpose of the agent is to carry out the tasks requested by the VSA user. Once installed:

- An agent icon—for example the  agent icon—displays in the system tray of the managed machine. [Agent icons](#) (page 21) can be custom images or removed altogether.
- Each installed agent is assigned a unique VSA **machine ID / group ID / organization ID** (page 556). Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available agent licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > [Deploy Agents](#) (page 35) inside the VSA.
- [Multiple agents](#) (page 44) can be installed on the same machine, each pointing to a different server.
- A [check-in icon](#) (page 15) displays next to each machine ID in the VSA, displaying the overall status of the managed machine. For example, the  check-in icon indicates an agent is online and the user is currently logged on.
- Clicking a check-in icon displays a single machine interface for the managed machine called [Live Connect](#) (page 15). [Live Connect](#) provides instant access to comprehensive data and tools you need to work on that one machine.
- Hovering the cursor over a check-in icon displays an [agent quick view window](#) (page 16) immediately. You can launch an agent procedure, view logs or launch [Live Connect](#) from the agent quick view window.

Agent Icons

Once installed on a machine, the agent displays an icon in the computer's system tray. This icon is the machine user's interface to the agent. The icon may be disabled at the discretion of the VSA user using

Agent

the Agent > **Agent Menu** (page 59) page.

Note: You can fully customize agents icon using System > Site Customization. See **Creating Custom Agent Icons** (page 396). This includes unique icons for Apple and Linux machines.

Agent Icon Background is Blue

When the agent is running and **successfully checking into the VSA**, the agent icon's background is **blue**.



Note: Double clicking the agent icon displays the **Portal Access Welcome Page** (page 561).

Agent Icon Background is Grey

A running agent that can **not** check into the VSA displays a **gray icon**. This indicates that either the network connection is down or the agent is pointed at the wrong address for the VSA.



If the agent icon is gray check the following:

1. Verify this machine has internet access.
2. Check to see if there is a firewall blocking the **outbound** port used by the agent to connect to the VSA. The default is port 5721.
3. Verify this machine account's **Check-in Control** (page 61) settings are correct.
4. Manually set the VSA server address in the agent by right clicking the agent menu, selecting **Set Account...**, and filling in the form with the correct address.

A screenshot of a dialog box titled "Set Agent Account Information". The dialog box has a blue title bar with a close button (X) in the top right corner. The main area is white and contains the following text: "Please enter the address of your management server. This Agent automatically connects to the server's IP Address or hostname to manage your system." Below this text are two input fields: "Machine.Group ID" with the value "newmachine.company.company-org" and "Server Address" with the value "help.company.com". At the bottom of the dialog box are two buttons: "OK" and "Cancel".

Agent Icon Background is Red

The agent icon turns **red** when a machine user manually disables remote control. VSA users prevent anyone from remote controlling their machine by selecting **Disable Remote Control** when they right click the agent menu.



Agent Icon Background Flashes between White and Blue

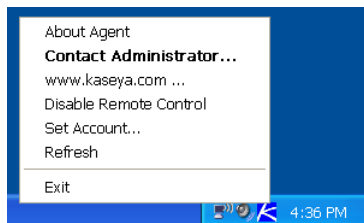
The agent icon **flashes** between a white background and its normal background when a *message is waiting* to be read. Clicking the icon displays the message.



Note: See **Remote Control > Send Message** (page 341) for an explanation of how to set up the sending of messages.

Agent Menu Options

Right clicking the agent icon pops up a menu of options available to the machine user.



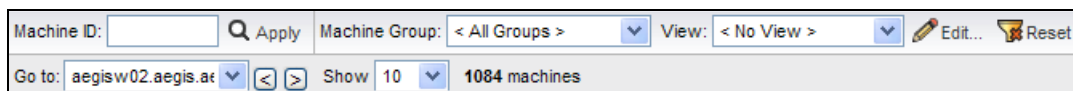
Note: See [Agent > Agent Menu](#) (page 59) for a description of how to turn these options on or off.

Disabling the Agent Menu

VSA users may completely **disable the agent menu** (page 59) and remove the icon from the machine's desktop.



Machine ID / Machine Group Filter





The Machine ID / Machine Group filter is available on all tabs and functions. It allows *you*—rather than an administrator—to limit the machines displayed on *all* function pages. The [View Definitions](#) window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type. Once filter parameters are specified, click the **Apply** button to apply filter settings to *all* function pages. By default, the Machine ID / Group ID filter displays all machine IDs in **<A11 Groups>** managed by the currently logged on VSA user.

Note: Even if a VSA user selects **<A11 Groups>**, only groups the VSA user is granted access to using [System > User Security > Scopes](#) (page 369) are displayed.


- **Machine ID** - Limits the display of data on *all* function pages by machine ID string. Include an asterisk (*) wildcard with the text you enter to match multiple records. For example, entering the string ABC* limits the display of machine IDs on all function pages to machine IDs that start with the letters ABC.
Filters the display of machines by machine ID. Enter the *beginning* of a string to find all machine IDs that match that string. Include an asterisk at the beginning of a string to find all devices that match that string anywhere in the machine ID. For example, entering the string *ABC matches all machine IDs that include ABC anywhere in their machine ID.
- **Apply** - Click the **Apply** button to apply filter settings to all function pages.
- **Machine Group** - Limits the display of data on all function pages by **group ID or organization** (page 556). An organization with only *one machine group* only displays the machine group in the **Machine Group** drop-down list, not the organization. Organizations with *multiple machine groups* display both the organization and all machine groups for that organization. This allows the organization to be optionally selected to include all the machine groups.
- **View** - Change views by selecting a different view definition. The [View Definitions](#) window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type.
- **Edit...** - Click to display the [View Definitions](#) (page 24) page.
- **Reset** - Clears all filtering.

Agent

- **Go to** - When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.
- **Show** - Select the number of machines IDs displayed on each page.
- **(Machine Count)** - Shows the machine count, based on filter settings.

View Definitions

Machine ID / Group ID Filter > Edit...

The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type. You can create and name multiple views. View filtering is applied to *all* function pages by selecting a **View** from the drop-down list on the **machine ID / machine group filter** (page 23) panel and clicking the **Apply**  icon. Options are organized by sections that can be expanded and collapsed as needed. When an option is set the section remains expanded.

Header Options

- **Save** - Save the selected view.
- **Save As** - Save the selected view view to a new name.
- **Delete** - Delete the selected view.
- **Select View** - Select a view.
- **Edit Title** - Edit the title of a view.
- **Share...** - You can **share** (page 370) a view with selected VSA users and user roles or make the view public for all VSA users and user roles.

To Create or Edit a New View

1. Click the **Edit...** button to the right of the **View** drop-down list in the machine ID / group ID filter panel to open the **View Definitions** editor.
2. Click the **Save As** button and enter a name for a new view.
3. Enter the desired filter specifications.
4. Click the **Save** button.

Machine Filter

- **Set machine ID** - Checking this box overrides any value set for the **Machine ID** field on the Machine ID / Group ID filter panel with the value entered here. The Machine ID field on the Machine ID / Group ID filter panel is disabled to prevent inadvertent changes while displaying a view with **Set machine ID** selected.
- **Set group ID** - Checking this box overrides the **Group ID** filter on the Machine ID / Group ID filter panel with the value entered here. The Group ID field on the Machine ID / Group ID filter panel is disabled to prevent inadvertent changes while displaying a view with **Set group ID** selected.
- **Only show selected machine IDs** - Save a view first before selecting machines IDs using this option. Once the view is saved, a **<N> machines selected** link displays to the right of this option. Click this link to display a **Define Collection** window, which allows you to create a view using an arbitrary **collection** (page 552) of machine IDs.

Machine Status

- **Show machines that have / have not / never been online in the last N periods** - Check to list those machines whose agents have checked into the Kaseya Server, or not, within the specified period of time. Use the **never** option to filter **machine ID template** (page 557) accounts, because these accounts never check in.
- **Show machines that are suspended / not suspended** - Check to list machines that are suspended or are not suspended.

- **Show machines that have/have not rebooted in the last N periods** - Check to list machines that have not rebooted in the specified number of periods.
- **Machines with Credential status** - Check to list machines with the selected **credential** (*page 553*) status.
- **Connection gateway filter** - Check to only list machines that have a connection gateway matching the specified filter. Include an asterisk (*) wildcard with the text you enter to match multiple records. For example 66.221.11.* matches all connection gateway addresses from 66.221.11.1 through 66.221.11.254.
- **IP address filter** - Check to only list machines that have an IP address matching the specified filter. Include an asterisk (*) wildcard with the text you enter to match multiple records. For example 66.221.11.* matches all IP addresses from 66.221.11.1 through 66.221.11.254.

OS Info

- **OS Type** - Check to only list machines that match the selected operating system as reported by a Latest Audit.
- **OS Version** - Check to only list machines that match the OS version string as reported by a Latest Audit. Use this filter to identify machines by **service pack**.

Agent Procedure

- **With agent procedure scheduled/not scheduled** - Check to only list machines that have the specified agent procedure either scheduled to run or not.

Note: Click the [select agent procedure](#) link to specify the agent procedure by name.

- **Last execution status success/failed** - Check to only list machines that have already executed the selected agent procedure. Select the appropriate radio button to list machines that successfully executed the agent procedure or failed to execute the agent procedure.
- **Agent procedure has/has not executed in the last N days** - Check to only list machines that have or have not executed the agent procedure in the specified period of time.

Applications

- **Contains/Missing application** - Check to only list machines that have, or don't have, an application installed using the specified filter. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Version string is > < = N** - Check to further refine the application filter with a version number greater than, less than or equal to a specified value.
- **Show Machines with teh following module installed**
 - **Anti-Malware**
 - **Antivirus**

Add-On Modules

- Filter machines based on whether they have had client software installed for selected add-on modules.

Label

- **Show machines with all or any of the following labels** - Filters machines using **all** or **any** of the selected labels.
- A series of keys in a machine's local registry is checked to identify whether the machine can be "labeled" a certain type of machine. Examples of labels include: **DNS Server, Domain Controller, POP3 Server, SMTP Server, and SQL Server**. Labeling is automatic. Each agent machine is checked periodically, typically once an hour, for configuration changes that may affect the labeling of the machine.

Patch Management

- **Show/Hide members of patch policy** - Checking this box works together with the machine ID and group ID filters to only list specific machines belonging (**Show**) or not belonging (**Hide**) to a specific **patch policy** (page 559).
- **Machines that have no patch scan results (unscanned)** - Check to only list machines that have not been scanned for missing patches.
- **Machines missing greater than or equal to N patches** - Check to only list machines *missing* a specified number of Microsoft patches.
- **Use Patch Policy** - Check to only list machines missing a specified number of *approved missing* Microsoft patches.
- **Patch scan schedule / not schedule** - Check to only list machines with either a patch scheduled or not scheduled.
- **Last execution status for patch scan success / failed** - Check to only list machines whose patch scan succeeded or failed.
- **Patch scan has / has not executed in the last <N> <periods>** - Check to only list machines whose patch scan has or has not executed within a specified time period.
- **Machines with Reboot Pending for patch installations** - Check to only list machines with a reboot pending for patch installations.
- **Machines with Patch Test Result** - Check to only list machines with the selected patch test result.
- **Machines with Patch Automatic Update configuration** - Check to only list machines with the selected Automatic Update configuration.
- **Machines with Patch Reboot Action configuration** - Check to only list machines with the selected Reboot Action configuration.
- **Machines with Patch File Source configuration** - Check to only list machines with the selected patch File Source configuration.
- **Machines missing a specific patch (use KB Article ID - digits only)** - Check to only list machines missing a specific patch.
- **Machines with installed patch (use KB Article ID - digits only)** - Check to only list machines with an installed patch identified by KB Article.
- **Machines being used as file share** - Check to only list machines configured as a file share using File Source.
- **Machines with file share located at select a machine** - Check to only list machines using a file share that was configured using File Source.
- **Machines with patch scan source set to online but offline scan ran last** - Check to only list machines with a Default Scan Source set to online but ran an offline scan most recently.
- **Default patch scan source Offline/Online.** - Check to only list machines using an offline or online default patch scan source.
- **Windows Automatic Update Disabled/Not Disabled** - Check to only list machines where Windows Automatic Update is disabled or is not disabled.

Monitoring

- **Only show machines with monitorset assigned <Select a Monitorset>** - Select to list all machines assigned this monitor set.
- **Only show machines with monitorset assigned <Select a SNMPset>** - Select to list all machines assigned this SNMP set.

Advanced Filtering

- **Advanced Agent Data Filter** - Check and click the **Define Filter...** button to further refine the view using the **Filter Aggregate Table** (page 27).

Warning: You must enter a space character to separate the operator from the data in a filter entry. For example, the filter entry `>= 500` includes a space character just after the equal sign.

Filter Aggregate Table

Machine ID / Group ID Filter > Edit... > Define Filter...

The **Filter Aggregate Table** lists over 75 agent and managed machine attributes that can be used to further refine a view definition using **advanced filtering** (page 27).

Note: **Collections** (page 552) provide an alternate method of selecting machine IDs for a view definition (page 24), regardless of whether they share any attributes.

User Defined Attributes

You can add user defined attributes to the **Filter Aggregate Table** using the Audit > **System Information** (page 134) page, then create view definitions that select machine IDs based on these user defined attributes.

Advanced Filtering

Advanced filtering lets you design complex searches to isolate data to just those values you want. Enter filter strings into the same edit fields you enter filter text.

Warning: You must enter a space character to separate the operator from the data in a filter entry. For example, the filter entry `>= 500` includes a space character just after the equal sign.

Advanced filtering supports the following operations:

White Space

To search for white space in a string, enclose the string in double quotes.

For example: `"Microsoft Office*" OR "* Adobe *"`

Nested operators

All equations are processed from left to right. Use parenthesis to override these defaults.

For example: `(("* adobe " OR *a*) AND *c*) OR NOT *d* AND < m`

AND

Use the logical AND operator to search for data that must contain multiple values but can appear in different places in the string.

For example: `Microsoft* AND *Office*` returns all items that contain both Microsoft and Office in any order.

OR

Use the logical OR operator to search for data that may contain multiple values but must contain at least one.

For example: `*Microsoft* OR *MS*` returns all items that contain either Microsoft and MS in any order.

NOT

Search for a string not containing the match data.

For example: `NOT *Microsoft*` returns all non-Microsoft applications.

For example: `NOT *Windows* AND NOT *update*` returns all items that do not contain either the strings Windows or update.

Agent

<, <= (Less than or less than or equal to)

Performs a string comparison to return all data whose value is less than the entered value.

For example: `< G*` returns all applications starting with a letter less than G.

For example: `< 3` returns the values 2, 21 and 287.

Note: Dates may also be tested for but must be in the following format: YYYYMMDD HH:MM:SS where YYYY is a four digit year, MM is a two digit month (01 to 12), DD is a two digit day (01 - 31), HH is a two digit hour (00 - 23), MM is a two digit minute (00 - 59), and SS is a two digit second (00 - 59). HH:MM:SS is optional. Date and time are separated with a space.

For example: `< 20040607 07:00:00` or `< "20040607 07:00:00"` returns all dates earlier than 7:00 on 7 June 2004. *Ensure a space exists after the < operator.*

>, >= (Greater than or greater than or equal to)

Performs a string comparison to return all data whose value is more than the entered value.

For example: `> G*` returns all applications starting with a letter greater than G.

For example: `> 3` returns the value 3, 3abc and 30.129.101.76.

Agent Ver

Returns all machines using a specified [agent version](#) (page 72). For example, agent version 6.2.1.1 is specified as 6020101

Agent Status

Agent > Machine Status > Agent Status

- [Agent status alerts can be defined using Monitoring > Alerts > Agent Status](#) (page 250).

The [Agent Status](#) page provides a summary view of a wide variety of agent data. You may choose all the data columns yourself to fully customize the view. Column and filter selections apply to each VSA user individually. Paging rows can be sorted by clicking column heading links.

- User defined columns of information can be added using the Audit > [System Information](#) (page 134) page. Once added, you can display them on this page and in the [Aggregate Table](#) report.
- You can filter the display of machine IDs on any agent page using the [Show machines that have / have not / never been online in the last N periods](#) option in [View Definitions](#) (page 24).

Select Columns...

Specify which columns of data to display and the order to display them in.

Filter...

Click [Filter...](#) to display a [Filter Aggregate Table](#). Enter strings to filter the display of rows in the paging area. For example, to search for the machine ID that "jsmith" is logged on to, enter `jsmith` in the edit box next to [Current User](#). Include an asterisk (*) wildcard with the text you enter to match multiple records.

Reset Filter

Displays only if an advanced filter is set. Click [Reset Filter](#) to clear all filter strings.

Column Definitions

Columns are described in the default order they display on this page.








- **Machine ID** - Machine ID label used throughout the system.
- **Current User** - Logon name of the machine user currently logged into the machine (if any).
- **Last Reboot Time** - Time of the last known reboot of the machine.
- **Last Checkin Time** - Most recent time when a machine checked into the Kaseya Server.
- **Group ID** - The group ID portion of the machine ID.
- **First Checkin Time** - Time when a machine first checked into the Kaseya Server.
- **Time Zone** - The time zone used by the machine.
- **Computer Name** - Computer name assigned to the machine.
- **Domain/Workgroup** - The workgroup or domain the computer belongs to.
- **Working Directory** - The directory on the managed machine the agent uses to store temporary files.
- **DNS Computer Name** - The fully qualified DNS computer name for the machine, which comprises the computer name plus the domain name. For example: `jsmithxp.acme.com`. Displays only the computer name if the machine is a member of a workgroup.
- **Agent GUID** - A unique identifier for a machine ID.group ID account and its corresponding agent.
- **Operating System** - Operation system type the machine is running.
- **OS Version** - Operation system version string.
- **IP Address** - IP address assigned to the machine, in version 4 format.
- **Subnet Mask** - Networking subnet assigned to the machine.
- **Default Gateway** - Default gateway assigned to the machine.
- **Connection Gateway** - IP address seen by the Kaseya Server when this machine checks in. If the machine is behind a DHCP server, this is the public IP address of the subnet.
- **Country** - The country associated with the Connection Gateway.
- **IPv6 Address** - IP address assigned to the machine, in version 6 format.
- **MAC Address** - MAC address of the LAN card used to communicate with the Kaseya Server.
- **DNS Server 1, 2** - IP address of the DNS servers assigned to the machine.
- **DHCP Server** - The IP address of the DHCP server used by this machine.
- **Primary/Secondary WINS** - WINS settings.
- **CPU Type** - Processor make and model.
- **CPU Speed** - Clock speed of the processor.
- **CPU Count** - The number of CPUs.
- **RAM Size** - MBytes of RAM on the machine.
- **Agent Version** - Version number of the Kaseya agent loaded on the machine.
- **Last Logged In User** - Logon name of the last person to log into the machine.
- **Portal Access Logon** - Logon name given to a machine user for logging into the Kaseya Server.
- **Portal Access Remote Control** - Enabled if this machine user can log in and get remote control access *to their own machine from another machine*. Disabled if access is denied.
- **Portal Access Ticketing** - Enabled if this machine user can log in and enter trouble tickets. Disabled if access is denied.
- **Portal Access Chat** - Enabled if this machine user can *initiate* chat sessions with a VSA user. Disabled if access is denied.
- **Primary/Secondary KServer** - IP address / name the machine uses to communicate with the Kaseya Server.
- **Quick Checkin Period - Quick check in** (*page 552*) time setting in seconds.
- **Contact Name** - Machine user name entered in **Edit Profile** (*page 65*).
- **Contact Email** - Email address entered in Edit Profile.
- **Contact Phone** - Phone number entered in Edit Profile.
- **Contact Notes** - Notes entered in Edit Profile.
- **Manufacturer** - System manufacturer.
- **Product Name** - System product name.

Agent

- **System Version** - Product version number.
- **System Serial Number** - System serial number.
- **Chassis Serial Number** - Serial number on the enclosure.
- **Chassis Asset Tag** - Asset tag number on the enclosure.
- **External Bus Speed** - Motherboard bus speed.
- **Max Memory Size** - Max memory size the motherboard can hold.
- **Max Memory Slots** - Total number of memory module slots available.
- **Chassis Manufacturer** - Manufacturer of the enclosure.
- **Chassis Type** - Enclosure type.
- **Chassis Version** - Enclosure version number.
- **Motherboard Manufacturer** - Motherboard manufacturer.
- **Motherboard Product** - Motherboard product ID.
- **Motherboard Version** - Motherboard version number.
- **Motherboard Serial Num** - Motherboard serial number.
- **Processor Family** - Processor type installed.
- **Processor Manufacturer** - Processor manufacturer.
- **Processor Version** - Processor version ID.
- **CPU Max Speed** - Max processor speed supported.
- **CPU Current Speed** - Speed processor is currently running at.
- **vPro-Host Name** - The name of the vPro-enabled machine set by vPro configuration.
- **vPro-Computer Name** - The name of the vPro-enabled machine set by the operating system.
- **vPro-Model** - The model of the vPro-enabled machine.
- **vPro-Manufacturer** - The manufacturer of the vPro-enabled machine.
- **vPro-Version** - The version of the vPro-enabled machine.
- **vPro-Serial Number** - The serial number of the vPro-enabled machine.
- **vPro-Asset Number** - An asset management identifier assigned to the vPro-enabled machine.
- **vPro-Motherboard Manufacturer** - The manufacturer of the motherboard of the vPro-enabled machine.
- **vPro-Motherboard Product Name** - The product name of the motherboard of the vPro-enabled machine.
- **vPro-Motherboard Version** - The version number of the motherboard of the vPro-enabled machine.
- **vPro-Motherboard Serial Number** - The serial number of the motherboard of the vPro-enabled machine.
- **vPro-Motherboard Asset Tag** - An asset management identifier assigned to the motherboard of the vPro-enabled machine.
- **vPro-Bios Vendor** - The vendor of the BIOS of the vPro-enabled machine.
- **vPro-Bios Version** - The version of the BIOS of the vPro-enabled machine.
- **vPro-Bios Release Date** - The BIOS release date of the vPro-enabled machine.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (*page 16*) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled



The agent has been suspended

Agent Logs

Agent > Machine Status > Agent Logs

The **Agent Logs** page displays log data related to managed machines. There are corresponding **log reports** (page 142) for each type of log provided.

Note: The system automatically limits the number of log entries per log type per machine to 1000. Once the limit has been reached, log entries exceeding the limit are archived, if archiving is enabled, and deleted from the system. The archive option is set in **Log History** (page 32).

Machine ID

Click the hyperlink of a machine ID to list all logs for that machine ID.

Select Log




Select a log from the **Select Log** drop-down list. The types of logs available include:


- **Alarm Log** - Lists all alarms triggered for the selected machine.
- **Monitor Action Log** - The log of **alert conditions** (page 551) that have occurred and the corresponding actions, if any, that have been taken in response to them.

Note: A counter value of -998 in the monitor logs indicates the monitor set is returning no data. Check that the the Performance Logs & Alerts service in Windows is running. This is a pre-requisite for monitoring of performance counters.

- **Agent Log** - Displays a log of agent, system, and error messages.
- **Configuration Changes** - Displays VSA settings changes for the selected machine
- **Network Statistics** - Displays a log of send/receive data for network applications.

Note: This log requires the Audit > **Network Access** (page 75) driver be enabled. This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. The driver is *disabled* by default.

- **Event Logs** - Displays event log data collected by Windows. Not available for Win9x. Only event logs that apply to the selected machine display in the event log drop-down list. A  indicates a log entry classified as a warning. A  indicates a log entry classified as an error. A  indicates a log entry classified as informational.

A monitor wizard  icon displays next to event log entries in the VSA and in **Live Connect**. Clicking the monitor wizard icon of a log entry displays a wizard. The wizard enables you to create a new event set criteria based on that log entry. The new event set criteria can be added to any new or existing event set. The new or changed event set is immediately applied to the machine that served as the source of the log entry. Changing an existing event set affects all machines assigned to use that event set. The monitor wizard icon displays in:

- Agent > Agent Logs
- Live Connect > Event Viewer
- Live Connect > Agent Data > Event Log

See Monitor > **Event Log Alerts** (page 276) for a description of each field shown in the wizard.

- **Agent Procedure Log** - Displays a log of successful/failed agent procedures.

Agent

- [Remote Control Log](#) - Displays a log of successful/failed remote control sessions.
- [Log Monitoring](#) - Displays [Log Monitoring](#) (page 555) entries.

Events per Page

Select the number of rows displayed per page.

Start Date / End Date / Refresh

Select a range of dates to filter log data, then click the [Refresh](#) button.



Filter...

Applies to [Event Logs](#) only. Click [Filter...](#) to restrict the amount of data displayed. You can specify a different advanced filter for each event category and column of data displayed.

Apply event log filter

Applies to [Event Logs](#) only. The event log filter includes options defined using the [Filter...](#) button. If [Applied event log filter](#) is checked, filtering is applied.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Log History

Agent > Machine Status > Log History

The [Log History](#) page determines the number of days to store log data in the database on a per log basis for each machine ID. Log data is displayed using [Agent Logs](#) (page 31) or printed to a report using [Info Center > Reporting > Logs](#). This page also determines whether agent log data is subsequently archived to text files located on a network directory. The directory is specified using [System > Server Management > Configure](#) (page 377). Changes made using this page take effect at the next agent check-in and display **in red text** until then.

- [Log Settings](#) can also be maintained using the [Agent Settings](#) tab of [Live Connect](#) (page 344) > Agent Data or the [Machine Summary](#) (page 131) page.
- [System > System Preferences > Check-in Policy](#) (page 356) can restrict the number of days users can keep log entries, to avoid placing undue stress on servers running the Kaseya Server service.
- These settings default from the agent install package. Agent install packages are created using Agent > [Deploy Agent](#) (page 35).

Estimating Database Sizing Requirements

The more data you log, the larger your database grows. Database sizing requirements can vary, depending on the number of agents deployed and the level of logging enabled. To estimate database sizing requirements for log data, create a dump of your database's `nteventlog` table. Determine how much data is being logged per day, then use that to predict the amount of extra space required to extend the log retention period.

Set days to keep log entries, check to archive to file

Set the number of days to keep log data for each type of log. Check the checkbox for each log to archive log files past their cutoff date.

- [Configuration Changes](#) - The log of configuration changes made by each user.

- **Network Statistics** - The log of incoming and outgoing packet count information and the application or process transmitting and/or receiving such packets. This information can be viewed in detail using Agent > **Agent Logs** (page 31) > Network Statistics.
- **Agent Procedure Log** - Displays a log of successful/failed agent procedures.
- **Remote Control Log** - Displays a log of remote control events.
- **Alarm Log** - The log of all alarms issued.
- **Monitor Action** - The log of alert conditions that have occurred and the corresponding actions, if any, that have been taken in response to them.
- **SYS log** - The 'log monitoring' log.
- **Agent Uptime Log** - Logs the uptime history of agents. Number of days must be set to 1 or greater for accurate last reboot time collection. See **Collecting last reboot times for the agent** (<https://helpdesk.kaseya.com/entries/35994418>) and **Reboot Now button remains and/or end user reports ongoing patch reboot nag after reboot** <https://helpdesk.kaseya.com/entries/33901207>.

Note: All agent log archives listed above are stored in the directory specified by the System > Server Management > **Configure** (page 377) > **Log file archive path** field.

Set days to keep monitoring logs for all machines

The following monitoring log settings are applied system-wide.

- **Event Log** - The log of all events. The events collected are specified in more detail using Agent > **Event Log Settings** (page 34).
- **Monitor Log** - The log of data collected by monitoring sets.
- **SNMP Log** - The log of all data collected by SNMP sets.
- **Agent Log** - The log of agent, system, and error messages

Note: Monitoring data log archives—identified on the Agent > **Log History** (page 32) page—are stored in the <KaseyaRoot>\UserProfiles\@dbBackup directory. This is to improve performance on systems where the database is on a different server. All other agent log archives are stored in the directory specified by the System > **Configure** (page 377) > **Log file archive path** field.

Set All Days

Click **Set All Days** to set all "day" fields to the same setting.

Select All Archive / Unselect All Archive

Click the **Select All Archive** link to check all archive checkboxes on the page. Click the **Unselect All Archive** link to uncheck all archive checkboxes on the page.

Update




Click **Update** to update selected machine IDs with agent log settings.

Select All/Unselect All






Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.

Agent

-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Event Log Settings

Agent > Machine Status > Event Log Settings

The **Event Log Settings** page specifies the combination of **event log** (page 554) types and categories that are collected by the VSA.

Note: Alerts can be separately specified for events using **Monitoring > Event Log Alerts** (page 276). **Event log alerts are still generated even if event logs are not collected by the VSA.**

To specify **Event Log Settings**:

1. Click an event log type in the **Event Log Types** list box. Hold down the [Ctrl] key to click multiple event log types.
2. Click **Add >** to add event log types to the **Assigned Event Types** list box. Click **<< Remove** or **<< Remove all** to remove event log types from the **Assigned Event Types** list box.
3. Check one or more event categories: **Error, Warning, Information, Success Audit, Failure Audit, Critical, Verbose**.
4. Select one or more machine IDs.
5. Click **Update** or **Replace** to apply these settings to selected machine IDs.

Global Event Log Black Lists

Each agent processes all events, however events listed on a "black list" are *not* uploaded to the VSA server. There are two black lists. One is updated periodically by Kaseya and is named `EvLogBlkList.xml`. The second one, named `EvLogBlkListEx.xml`, can be maintained by the service provider and is not updated by Kaseya. Both are located in the `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles` directory. Alarm detection and processing operates regardless of whether entries are on the collection blacklist.

Flood Detection

If 1000 events—not counting **black list events** (page 555)—are uploaded to the Kaseya Server by an agent *within one hour*, further collection of events of that log type are stopped for the remainder of that hour. A new event is inserted into the event log to record that collection was suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your Kaseya Server. Alarm detection and processing operates regardless of whether collection is suspended.

Update

Adds event log types listed in the **Assigned Event Types** list box to the set of event log types already assigned to selected machine IDs.

Replace

Replaces all event log types assigned to selected machine IDs with the event log types listed in the

[Assigned Event Types](#) list.

Clear All









Clears all event log types assigned to selected machine IDs.

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended


Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Delete Icon

Click the delete icon  to delete this record.

Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

Assigned Categories

The event categories stored by the VSA for this machine ID and event log:

- [Error](#)
- [Warning](#)
- [Information](#)
- [Success Audit](#)
- [Failure Audit](#)
- [Critical](#) - Applies only to Vista, Windows 7 and Windows Server 2008
- [Verbose](#) - Applies only to Vista, Windows 7 and Windows Server 2008

Deploy Agents

[Agent](#) > [Install Agents](#) > [Deploy Agents](#)

The [Deploy Agent](#) page creates and distributes an agent install package to *multiple* machines.

Agent Install Packages

Agents are installed on managed machines using an [agent install package](#). An agent install package contains all the settings you prefer an agent to work with on a target machine.

Agent

The Agent > **Deploy Agents** page displays the agent install packages that are available in your VSA. A **Default Install** package is provided with the VSA. You might see other agent install packages already created and listed on this page.

An agent install package is created using the **Configure Automatic Account Creation** wizard. The wizard copies agent settings from an *existing* machine ID or machine ID template and generates an install package called **KcsSetup**. All settings and pending agent procedures from the machine ID you copy from—except the machine ID, group ID, and organization ID—are applied to every new machine ID created with the package.

Note: See the PDF quick start guide, [Agent Configuration and Deployment](#).



Additional Topics

- **Creating an Agent Install Package** (page 37)
- **Manually Installing the Agent** (page 37)
- **Automating the Installation of the Agent** (page 38)
- **Maintaining Agent Install Packages** (page 39)
- **Configuring Agent Settings** (page 40)
- **Agent Install Command Line Switches** (page 42)
- **Install Issues and Failures** (page 44)
- **Installing Multiple Agents** (page 44)
- **Installing Linux Agents** (page 46)
- **Supported Linux Functions** (page 47)
- **Supported Apple Functions** (page 48)

Actions

- **Click to download default Agent** - Click this link to download the current VSA user's default package directly from this page.
- **Users can download agents from** - Paste this hyperlink into an email message. The *unique ID number* ensures that when the link is clicked in the email message, the default install package is selected and downloaded. Set a different install package as the default to display the link for that install package.
- **Manage packages from all administrators** - Check to display all packages created by all VSA users. Once a hidden package is displayed, you can use the package or make the package public. This option only displays for **master role users** (page 564).

Table Columns

- **Set Default** - Specify your own default install package by selecting the radio button to the left of the package name in the **Set Default** column.
- **Delete Icon** - Click the delete icon  to remove a package from the paging area. If you created the package, then this also deletes the package from the system and removes it for all VSA users.
- **Edit Icon** - Click the edit icon  next to a package to change parameters for that package using the **Configure Automatic Account Creation** wizard.
- **Package Name** - Lists the name of the package.
- **Public Package** - Public package rows display with a brown background. Private package rows display with a gray background.
- **Share** - Click **Share** to **share** (page 370) a private package with other users, user roles or to make the package public.
- **List on dl.asp** - Click the **dl.asp** link in the column header to display the web page machine users see when they install an agent on their machine. Check a box in this column to include its package in the list of available download packages on the **dl.asp** page.
- **Description** - Displays the description of the package.

Creating an Agent Install Package

On the Agent > [Deploy Agents](#) (page 35) page, click [Create Package](#) to start the [Configure Automatic Account Creation](#) wizard. The wizard is a 7 step process.

1. Define rules for naming the machine ID.
 - Prompt the user to enter a machine ID.
 - Use the computer name as the machine ID.
 - Set the user name of the currently logged on user as the machine ID.
 - Specify a fixed machine ID for this install package.
2. Define rules for naming the group ID.
 - **Existing Group** - Select an existing group ID from a drop-down list.
 - **Domain Name** - Uses the user's domain name.
 - **New Group** - Specify a new group ID. This option only displays for **master role users** (page 564).
 - **Prompt User** - Asks user to enter a group ID. This option only displays for **master role users** (page 564).
3. Specify agent install package **command line switches** (page 42) including the ability to install **silently without any task bars or dialog boxes** (page 562).
4. Specify the machine ID to copy settings and pending agent procedures from. All copied settings and pending agent procedures—except the organization ID, machine ID, and group ID—are applied to every new machine ID created with the package.

Note: The statement Copy settings from unknown.root.unnamed if nothing selected is based on the machine ID or template selected by the Default Install package.

5. Select the operating system you are creating the install package for: **Automatically choose OS of downloading computer: Windows, Macintosh, or Linux.**
6. Optionally bind a user logon credential to the install package. Fill in the **Administrator Credential** form to securely bind user rights to the install package.
 - Users without administrator rights can install the package successfully without having to enter an administrator credential.
 - If the administrator credential is left blank and the user does not have administrator rights to install software, the install package prompts the user to enter an administrator credential during the install. **If the package is also silent KcsSetup will fail without any dialog messages explaining this.**

Administrator Credentials - If necessary, an agent install package can be created that includes an administrator credential to access a customer network. Credentials are only necessary if users are installing packages on machines and do not have administrator access to their network. The administrator credential is encrypted, never available in clear text form, and bound to the install package.

7. Name the install package for easy reference later. This name displays on the [Deploy Agents](#) page and the `d1.asp` download page.

Manually Installing the Agent

Manually Downloading Install Packages from the Deploy Agent Page

The [Deploy Agent](#) page provides three types of links for downloading agent install packages:

Agent

- **Click the "download default agent" link** - Each user has his or her own default agent install package. Click this link to download your own user default agent.
- **Click a "package" link** - The complete list of available agent install packages displays on the **Deploy Agents** page. Click any of these links to download the agent install package.
- **Click the "dl.asp" link** - The `dl.asp` web page lists all publicly available agent install packages. Click any package listed on the `dl.asp` web page to download it.

Any of these methods downloads the same `KcsSetup` file used to install the agent.

Installing an Agent Using the `dl.asp` Page

The following is the fastest way to install an agent manually.

1. Log on to any machine you want to install an agent on.
2. Enter the following URL in the browser of that machine:
`http://<YourVSAaddress>/dl.asp`
3. Click the **Default Install** package to begin installation of the agent on that machine.
 - If other install packages are listed, select your preferred install package.
 - Once the install starts you may have to confirm the installation to ensure it completes.
4. Log on to your VSA:
`http://<YourVSAaddress>`
5. Within the VSA, select the Agent > **Agent Status**
(<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#250.htm>) page.

You should see a new machine account listed on this page for the agent you just created.

Executing the Agent Install Package on the Endpoint Machine

Users can execute the `KcsSetup` installer on the endpoint machine using any of the following methods:

- **Windows**
 - Double-click the `KcsSetup` to launch it.
 - Open a **command line window** and type `KcsSetup` followed by any desired **command line switches** (page 42).
 - Select **Run...** from the **Windows Start** menu and type `KcsSetup` followed by any desired command line switches.
- **Apple and Linux**
 - Double-click `KcsSetup` to launch it.
 - The full filename for a Macintosh agent install package is `KcsSetup.app`. `KcsSetup.app` is downloaded as a `KcsSetup.zip` which contains `KcsSetup.app` inside a folder titled **Agent**. Click the `KcsSetup.zip` file to expand it, click the **Agent** folder, then click the `KcsSetup.app` file to execute it.

Note: For Apple, **command line switches** (page 42) can only be used when creating the agent install package.

Note: For Linux, see **Installing Linux Agents** (page 46) for more detailed instructions.

Reinstalling Agents

The **Create** (page 48) page enables you to re-install an agent for an existing machine ID account.

Automating the Installation of the Agent

You can use the following methods to automate the installation of agent install packages:

Logon

- **Windows** - Set up an **NT logon** procedure to run the install package every time a user logs into the network. See system requirements.
- **Apple** - Set up an **Apple OS X Login Hook Procedure** to run the install package every time a user logs into the network. See Apple KB Article **HT2420** (<http://support.apple.com/kb/HT2420>).

Procedure

1. Create the deployment package using the Agent > **Deploy Agents** wizard.
 - The **KcsSetup** installer skips installation if it detects an agent is already on a machine if the `/e` switch is present in the installer package.
 - You will probably want to select the silent install option.
 - It may be necessary to bind an administrator credential if users running the logon procedure don't have user rights.
2. Download the appropriate **KcsSetup** installer package using the `d1.asp` page and copy it to a network share which users can execute programs from.
3. Add **KcsSetup** with its network path to the logon procedure.

Email

Email **KcsSetup** to all users on the network. Download the appropriate install package from the **Deploy Agents** page, then attach it to an email on your local machine. You can also copy and paste the link of the default install package into an email message. Include instructions for launching the package, as described in the **Manual** bullet below.

Discovery by Network or Domain

Use the **Discovery** module to discover machines on **Networks** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) and **Domains** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#10750.htm>), then install the agents on discovered machines, either manually or automatically.

Automatic Account Creation

You should be aware that *automatic account creation* is enabled using System > **Check-in Policy** to automatically create a machine ID account when an agent install package is installed. This option is enabled by default when the VSA is installed.

Assigning New Machine IDs to Machine Group by IP Address

You may choose to create a "generic" install package that adds all new machine accounts to the unnamed group ID. When the agent checks in the first time, the System > **Naming Policy** assigns it to the correct group ID and/or sub-group ID using the IP address of the managed machine. Agent settings can be configured afterward by policy or template. See:

- **Configuring Agent Settings Using Policies** (page 41)
- **Configuring Agent Settings Using Templates** (page 41)


Maintaining Agent Install Packages

Updating the Agent Software

An agent install package always downloads a **KcsSetup.exe** that uses the latest version of the agent software available. Once the **KcsSetup.exe** file is created, its version of the agent software remains fixed within the exe. Consider replacing **KcsSetup.exe** files that were created a while ago, then stored in network locations or added to CDs for ease of distribution. Similarly, the version of agent software installed on machines always remains fixed, until you update them using the **Update Agent** (page 72) page.

Editing the Default Install Package

The **Default Install** package sets the default values displayed when you create a new package. Normally the **Default Install** package cannot be modified. The **Save** button is disabled. To enable the **Save** button for the **Default Install** package, do the following as a *master role user*:

1. Click the **Share** button next to the **Default Install** package in Agent > **Deploy Agents**.
2. Check **Allow other users to modify**.
3. Click **Save**.
4. Click the edit icon  next to the **Default Install** package.

The **Save** button will be enabled when you edit the **Default Install** package.

Note: If you delete the **Default Install** package, it is re-created immediately.

Configuring Agent Settings

Agent Settings

Agent settings determine the behavior of the agent on the managed machine. Although each agent can be configured individually, it's easier to manage machines if you adopt similar settings for each type of machine you manage. For example, laptops, desktops and servers could all have settings that are unique to that type of machine. Similarly, machines for one customer may have unique characteristics that differ from the machines used by other customers. Type of agent settings include:

- **Credential** (page 68)
- **Agent Menu** (page 59)
- **Check-in Control** (page 61)
- **Working Directory** (page 64)
- **Logs** (page 32)
- **Edit Profile** (page 65)
- **View Collections** (page 552)
- **Portal Access** (page 67)
- Remote Control Policy
- **Patch Settings** (page 559)
- Patch File Source
- Patch Policy Memberships
- **Alerts** (page 248)
- **Event Log Alerts** (page 276)
- **Monitor Sets** (page 234)
- **Distribute Files** (page 118)
- **Scheduled Agent Procedures** (page 80)

Policies vs Templates

There are two general methods of maintaining agent settings on multiple machines.

- **Configuring Agent Settings Using Policies** (page 41) - This is the preferred, *dynamic* method of managing agent settings on hundreds, even thousands, of machines. Once a policy is applied to a target machine, propagation is automatic.
- **Configuring Agent Settings Using Templates** (page 41) - This is the legacy, *static* method of maintaining agent settings on multiple machines. Agent settings must be manually copied to each target machines each time you make a change.

Configuring Agent Settings Using Policies

The **Policy Management** (KPM) module in the VSA manages *agent settings by policy*. Once policies are assigned to machines, machine groups or organizations, *policies are propagated automatically*, without further user intervention.

The System Management Wizard

A policy setup wizard is located on System > Orgs/Groups/Depts/Staff > Manage > Systems Management tab.

The setup wizard enables you to quickly *configure and apply machine management policies for a specific organization*. Once configured, these policies are assigned to each machine you manage on behalf of that organization. Policies govern many different aspects of machine management:

- Audit scheduling
- Monitoring
- Alerts
- Patch Management
- Routine machine maintenance using agent procedures

With policies you no longer have to manage each machine individually. You only have to assign or change the policy. A policy assignment or a change within an assigned policy is propagated within 30 minutes to all member machines without you having to schedule anything. Once applied, you can quickly determine whether managed machines are in compliance or out of compliance with their assigned policies. Compliance tracking by individual policy provides you with the information you need to deliver IT services consistently throughout the organizations you manage.

Note: See the **Standard Solution Package** for a detailed explanation of each option in the setup wizard (<http://help.kaseya.com/webhelp/EN/SSP/7000000/index.asp#11220.htm>).

Configuring Agent Settings Using Templates

Machine ID Templates

A machine ID template is *a machine ID record without an agent*. Since an agent never checks into a machine ID template account, it is not counted against your total license count. You can create as many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are typically copied from a selected machine ID template. Machine ID templates are usually created and configured for certain types of machine. Machine type examples include desktops, Autocad, QuickBooks, small business servers, Exchange servers, SQL Servers, etc. **A corresponding install package can be created based on each machine ID template you define.**

- Create machine ID templates using Agent > **Create** (page 48).
- Import a machine ID template using Agent > **Import/Export** (page 57).
- Base an agent install package on a machine ID template using Agent > **Deploy Agents** (page 35).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > **Copy Settings** (page 55).
- Identify the total number of machine ID template accounts in your VSA using System > **Statistics** (page 389).
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.
- Separate machine ID templates are recommended for Windows, Apple and Linux machines. Alternatively you can create a package that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

To apply a machine ID template to a package:

Agent

1. Use the **Create Package** wizard in **Deploy Agent** to use the template as the source machine ID to copy settings from when creating the package to install.
2. Add additional attributes to the package using this same wizard. These additional attributes usually differ from one customer to the next and therefore cannot be usefully stored in the template.

Copying Agent Settings

Machine ID templates (page 557) are initially used to create an agent install package using the template as the source to copy settings from. But even after agents are installed on managed machines, you'll need to update settings on existing machine ID accounts as your customer requirements change and your knowledge of the VSA grows. In this case use Agent > **Copy Settings** to copy these changes to any number of machines IDs you are authorized to access. Be sure to select **Do Not Copy** for any settings you do not want to overwrite. Use **Add** to copy settings without removing existing settings. Kaseya recommends making changes to a selected template first, then using that template as the source machine ID to copy changes from. This ensures that your machine ID templates remain the "master repositories" of all your agent settings and are ready to serve as the source of agent install packages and existing machine ID accounts.

Templates and Filtered Views

There is a corresponding relationship between machine ID templates and filtering your view of selected machines using the **Only show selected machine IDs** view definition option. For example, if you define a machine ID template called "laptops", then it's easier to apply settings to all the "laptops" you're responsible for if you have a filtered view called "laptops". Simply select the view for "laptops" and only laptops are displayed on any function page, regardless of the machine group they belong to. The same idea applies to "desktops", "workstations", "Exchange servers", etc.

Filtered views of selected machines are particularly useful when you're getting ready to copy settings from a machine ID template to existing agents using the **Copy Settings** function described above.

Base Templates and Audits

Since you can never be sure what settings should be applied to a machine until you perform an audit on the machine, consider installing an agent package created from a "base" template that has most of the agent settings *turned off*. Once you have the audit, then you can decide which settings should go on which machine. Use the **Copy Settings** function to copy settings from the appropriate template to the new agent.

Agent Install Command Line Switches

Agent install command line switches for `KcsSetup` are case insensitive and order independent. Separate switches with an empty space. For example: `KcsSetup /e /g=root.unnamed /c`


Note: For Apple agents, command line switches can only be used when creating the agent install package.

`/b` - Reboot the system after installation completes. Agent installation requires a reboot in order to load its drivers. Use this switch on packages given to users that do not have rights to shut down the computer.

`/c` - Use the computer name as the machine ID for the new account. If the computer name cannot be determined programmatically, the machine user is prompted to enter a machine ID. The exception is silent mode, `/s`, in which case the installation stops and an error is logged to the installation log.

`/d` - Use the current domain name as the group ID for the new account. If the domain name cannot be determined programmatically, the machine user is prompted to enter the group ID. The exception is silent mode, `/s`, in which case the installation stops and an error is logged to the installation log.

`/e` - Exit immediately if the installer detects that an agent is already installed. Use `/e` at the end of logon procedures. `/k` or `/r` overrides `/e`.

- /f "Publisher"** - Specifies the full name of the service provider or tenant. Windows only.
- /g=xxx** - Specifies the group ID to use for the new account. **xxx** must be an alpha-numeric string and can not contain spaces or punctuation marks.
- /h** - Display the help dialog box listing all the command line switches, unless the **/s** switch is set, in which case the application exits.
- /i** - Ignore non-critical errors such as incorrect or indeterminate versions of WinSock2, or indeterminate versions of the OS, and force the installation to proceed.
- /j** - Does not install an agent shortcut to the **Start > All Programs** menu. Windows only.
- /k** - Displays a dialog box asking the user if it is OK to re-install when the agent is already detected on the machine. Without this switch, the installer exits if an agent is already present.
- /m=xxx** - Specifies the machine ID to use for the new account. **xxx** must be an alpha-numeric string and can not contain spaces or any punctuation marks except period(.).
- /n = partitionId** - Specifies the partition ID of the **tenant partition** (*page 564*) the installed agent/machine ID account is a member of.
- /o "Company Title"** - Specifies the company title of the service provider or tenant. Windows only.
- /p "install_path"** - Overrides the default installation path by specifying the full directory path, including drive letter, in which to install the agent.
- On Windows, by default, the agent installation creates a directory using the **%ProgramFiles%** variable path as **\<company>\<Agent-Instance-Guid>**.
 - On Linux, by default, the agent installation creates a directory named **/opt/Kaseya/<Agent-Instance-Guid>**
 - On Apple, the **/p** switch is not supported & ignored.
- /r** - Executes the installation program and re-installs the agent even if an agent is already on the machine.
- /s** - Runs in silent mode. Suppresses all dialog boxes.
- /t "Title"** - Specifies the title of any dialog windows shown to the machine user during installation. The default title is: "Kaseya Agent".
- /u** - Uses the current machine user name as the machine ID for the new account. If the machine user name cannot be determined programmatically, the user is prompted to enter a machine ID. The exception is silent mode, **/s**, in which case the installation stops and an error is logged to the installation log.
- /v** - Associates this agent with an existing agent account in the VSA when the machine name, agent name and organization are the same for the same partition. Ignores creating a new agent account when a new MAC address is detected. Suitable for re-using existing agent accounts created for reverted VDI resources.
- /w** - Overwrites the existing configuration file with a configuration file included in the agent installation. Use with the **/r** switch to re-install an agent with new server settings. Intended for an existing agent that is attempting to connect to a server that no longer exists.
- /x** - Disables remote control after successfully installing the agent. This option is ignored when updating or re-installing. Remote control of this machine can only occur after the user selects **Enable Remote Control** by right clicking the K icon  on the system tray.
- /z "Message"** - Specifies the message shown to the user when installation completes. The exception is silent mode, **/s**, in which case the installation completes and the status message is written to the installation log. The default message is: "The Agent has been installed successfully on your computer."
- /?** = Display the help dialog box listing all the command line switches, unless the **/s** switch is set, in which case the application exits. Windows only.

Linux Only Install Switches

See [Installing Linux Agents](#) (page 46).

Install Issues and Failures

The following issues and failures can occur when installing agents:

- **Invalid Credential** - The [credential](#) (page 553) bound to the package must have administrator rights on the local machine. The agent installs as a system service requiring full administrator privileges to install successfully. The administrator name may be a domain user of the form `domain\administrator` or `administrator@domain`. On Vista, 7, and 2008 machines, ensure User Account Control (UAC) is disabled for the administrator rights credential being used.
- **Domain Specified for a Machine Not in the Domain** - If, in step 2 of package creation in [Deploy Agent](#), the [Domain Name](#) option is selected and the computer is not part of a domain, an installation package will peg the CPU at 100% during install, but eventually install.
- **Blocked by Anti-Virus Program** - Some anti-virus programs may classify the agent installation as a security threat and block its execution.
- **Blocked by Security Policy** - Local or domain security policies may prevent access to the installation directory, typically by default the `Program Files` directory.
- **Insufficient Licenses** - The agent may be prevented from checking in the first time and creating an account if there are insufficient VSA licenses available. When this happens a gray K icon appears in the system tray just after the agent is installed on the machine and never turns blue. A tooltip displays when the cursor is placed over the gray agent icon and reports "'Machine ID.Group ID' not recognized by the Kaseya Server".

Apple

- Macintosh agents cannot be deployed silently without a valid username and password.

Installing Multiple Agents

Multiple agents can be installed on the same managed machine, each checking in to different Kaseya Servers. *Run the v6 agent installer from a different Kaseya Server* and you will get an additional agent.

- Applies to Windows and Linux agents. Installing multiple Macintosh agents is not supported.
- A v6 agent can co-exist with other v6 agents.
- For Windows only:
 - A v6 agent can co-exist with v5.1 or older agents.
 - Any managed machine with a domain controller login procedure that runs the agent installer automatically *must* update the v5.1 or older `KcsSetup` file with the v6 agent. The v5.1 or older installer does not know about the newer v6 agent and will re-install even if the v6 agent is present.

Driver Usage - Windows Agents Only

If multiple agents are installed on a machine, only one agent at a time controls the drivers required to use [File Access](#) (page 74), [Network Access](#) (page 75), [Application Blocker](#) (page 77). These functions can only be performed by the agent controlling these drivers.

- Originally the first agent installed controls the drivers.
- If the first agent controlling the drivers is uninstalled, then these drivers are uninstalled as well and these three functions cannot be performed by any agent.
- These drivers are re-installed by either of the following events:
 - Any of the existing agents on the machine are updated. The updated agent takes control of the drivers and can perform these three functions.

- A new agent is installed. The newly installed agent takes control of these drivers and can perform these three functions.
- To determine which agent has control of the drivers, see *Registry* below.

Identifying Agents on Managed Machines

When a Kaseya agent is installed, a *unique identifier* is created for the agent comprising the Kaseya Server's 6 character customer ID and a randomly generated 14 digit number. This unique agent identifier, called the agent GUID, is used to create separate sub-folders to store agent program files, and as a sub-key for agent registry values.

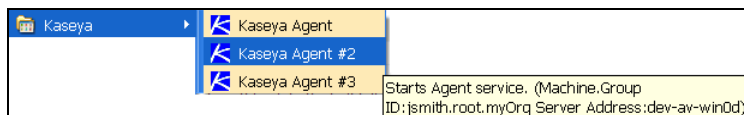
In the examples below, agents display specific information for the following placeholders:

- <GUID> - The agent instance GUID.
- <company> - The agent's install directory.
- <serveraddress> - The Kaseya Server address the agent checks into.
- <machineID.groupID.orgID> - The machine ID, group ID, and organization ID of the agent on the Kaseya Server.
- <shortcutname> - The name of the shortcut. Example: Kaseya Agent #2.


Shortcuts

When you move the mouse cursor over a Kaseya Agent shortcut—for example, a shortcut on the Windows Start Menu—a tool tip displays as:

- Start Agent service. (machine.GroupID:<machineID.groupID.orgID> Address:<serveraddress>)
- If you right click a shortcut, you'll also see this text in the comment field of the shortcut property page.



About Agent

Right click the K icon  in the system tray of a managed machine and select the **About Agent** option to display the following information:

- Agent Version
- Server Address - <serveraddress>
- Product ID - <GUID>
- Program Title - <shortcutname>

Windows Agents

Add/Remove

Agents display as follows:

- Kaseya Agent (<machineID.groupID.orgID> - <serveraddress>)
- Kaseya Agent #2 (<machineID.groupID.orgID> - <serveraddress>)
- Kaseya Agent #3 (<machineID.groupID.orgID> - <serveraddress>)

Services

The description field of the service displays the same text shown above in the agent shortcut.

Registry

Agent registry settings displays as follows:

```
HKLM\Software\Kaseya\Agent
  DriverControl - The agent that controls driver usage.
  KES_Owned_By - The agent that manages the KES client.

HKLM\Software\Kaseya\Agent\<GUID>
  Title - <shortcutname>
  Path - C:\Program Files\<company>\<GUID>
  ServAddr - <serveraddress>
  machineID - <machineID.groupID.orgID>
  DriverControl - The agent that controls driver usage.
  KES_Owned - The agent that manages the KES client.
```

Default Agent Installation Folders

- See the `/p` switch in [Agent Install Command Line Switches](#) (page 42).

Installing Linux Agents

Note: See [System Requirements](http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm) (<http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm>) for supported Linux operating systems and browsers.

Installing Linux Agents Manually

1. From a Linux machine open a Firefox or Chrome browser in a Gnome session and log into the VSA.
2. Display the Agent > Install Agents > [Deploy Agents](#) (page 35) page.
3. Click the [Click to download default Agent](#) hyperlink to begin downloading the the default agent install package. A Linux agent install package will download.

Note: Alternately, you can create your own Linux package by pressing [Create Package](#) and stepping through the wizard.

4. Once the download is complete, locate the `KcsSetup.sh` file in the download directory of the Linux machine.

Note: If you have downloaded `KcsSetup.exe` or `KcsSetup.zip`, you have downloaded the wrong install file because the selected install package is dedicated to Windows or Macintosh installs.

5. Issue the following commands as root:

```
# chmod +x KcsSetup.sh
# ./KcsSetup.sh
```

The agent installs and starts. Log into your VSA and view the status of the agent.

For further information see the install log file, located at:

```
/tmp/KASetup_<pid>.log
```

where `<pid>` is the process id of the `./KcsSetup.sh` execution.

Note: Run `KcsSetup.sh -V -D` for verbose terminal output.

Note: Run `KcsSetup.sh -X` to save the temp files created in the `/tmp` file. Saving these files is useful when troubleshooting a failed install.

6. After the Linux agent is installed, log in and log out to see the Kaseya agent icon in a Gnome panel.

Installing Linux Agents Using LAN Watch and Install Agents

1. Schedule a Discovery > **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) scan using an existing Linux agent as the discovery machine.
2. Install a Linux agent on a discovered Linux machine using one of the Discovery > Discovered Devices pages.
 - Enter `root` in the **Admin Logon** field.
 - Enter the password for the `root` user of the targeted Linux machines in the **Password** field.
 - Select an agent install package in the **Select an Agent Package to install** field.
 - Check the checkboxes next to one or more targeted Linux machines, or enter the IP address or name of a targeted Linux machine in the **undiscovered machine** field.
 - Click the **Submit** button.

Note: The **Install Agents** page does not currently distinguish between Linux and other systems. It is the installer's responsibility to select only Linux systems.

Uninstalling a Linux Agent Manually

A `<install-dir>/bin/KcsUninstaller` always gets installed with the agent and will remove the agent. Agents are typically installed to the `/opt` directory.

Issue the following commands as root:

```
# ./KcsUninstaller
```

Note: Run the command `./KcsUninstaller -D -V` to uninstall the agent with verbose terminal output.

Troubleshooting Linux Agents Installs

- See the **Troubleshooting Linux Agent Installs** (<https://helpdesk.kaseya.com/entries/36223968>) community page.

Supported Linux Functions

Linux agents support the following functions:

- Agent procedures
- Latest audits, baselines audits and system audits
- Remote control and FTP with VNC
- SSH
- Reset Password
- LAN Watch and Install Agents - See **Installing Linux Agents** (page 46).
- Alerts
- Monitoring of Processes
- Monitoring of SNMP
- Log Parser
- Site Customization - The **Agent Icons** tab now includes a set of icons for Linux agents you can customize.
- Only non-plug-in specific items are accessible via a Linux-based Browser or when browsing to Linux agent machine. This is the following:
- Live Connect - Only non-plug-in specific items are accessible via a Linux-based browser or when browsing to a Linux agent machine. Supported menu options include:
 - Home
 - Agent Data
 - Audit Information

Agent

- Ticketing (or Service Desk Ticketing)
- Chat
- Video Chat

See [System Requirements](http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm) (<http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm>).

Supported Apple Functions

Apple agents support the following functions:

- Audits - selected hardware and software attributes
- Agent procedures
- Remote Control
- FTP
- SSH
- Reset Password
- Task Manager
- Live Connect including Desktop Access.
 - On Apple Leopard (Intel) and above, including Lion and Mountain Lion, you can use Desktop Access in Live Connect to remote control a Windows system using Firefox or Safari.
 - On Windows using any of our supported browsers you can use Desktop Access to remote control a Apple Leopard (Intel) and above, including Lion and Mountain Lion.
- Desktop session recording via Remote Control and Quick View, for Snow Leopard and above, including Lion and Mountain Lion
- LAN Watch via Discovery
- Supported monitoring:
 - SNMP monitoring
 - Process monitoring in monitor sets
 - System Check
 - Log Parser

See [System Requirements](http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm) (<http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm>).

Create

Agent > Install Agents > Create

The **Create** page creates a machine ID account and agent install package for a *single* machine. You create the machine ID account first, then create an install package for this single machine. Typically the **Create** page applies to:

- **Machine ID templates** - In this case, no install package need be created, since **machine ID templates** ([page 557](#)) are not intended for installation to a machine.
- **Reinstalling Agents for an Existing Account** - Because the **Create** install packages does *not* automatically create a new machine ID account, you can use the **Create** page to *re-install* agents on managed machines for *existing* accounts.
- **Secured environments** - Secured environments may require each machine be setup manually. For example, you might be required to name a new machine ID account manually and/or create an agent install package with a unique credential for a single machine. A user must be logged into a target machine locally to install the package.

Note: Use **Agent > Deploy Agents** (page 35) to create and distribute agent install packages to *multiple* machines. The **Deploy Agents** install package *automatically creates a machine ID account* when it is installed provided automatic account creation is enabled using **System > Check-in Policy** (page 356).

Note: Use **Discovery** to install agents *on remote systems*.

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the **machine ID / group ID / organization ID** (page 556) and the **agent** (page 547). The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

Agent License Counts

The following events affect agent license counts:

- An "unused" agent license is changed to "used" if a machine ID account is created and the agent installed.
- If the agent is deleted but not the account, the agent license is still considered "used".
- If the account is deleted, regardless of what happens to the agent, the agent license goes back to "unused".
- If an account is created, but the agent is not yet installed the first time, the account is called a **machine ID template** (page 557). Machine ID template accounts are not counted as "used" until you install the agent.

Including Credentials in Agent Install Packages

If necessary, an agent install package can be created that includes an administrator **credential** (page 553) to access a customer network. Credentials are only necessary if users are installing packages on machines and *do not have administrator access* to their network. The administrator credential is encrypted, never available in clear text form, and bound to the install package.

Operating System Selection

Agent packages can be created to install agents on machines running either Windows, Apple, or Linux operating systems, or to automatically choose the type of operating system of the downloading computer.

Machine ID Templates

A machine ID template is *a machine ID record without an agent*. Since an agent never checks into a machine ID template account, it is not counted against your total license count. You can create as many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are typically copied from a selected machine ID template. Machine ID templates are usually created and configured for certain types of machine. Machine type examples include desktops, Autocad, QuickBooks, small business servers, Exchange servers, SQL Servers, etc.

A corresponding install package can be created based on each machine ID template you define.

- Create machine ID templates using **Agent > Create** (page 48).
- Import a machine ID template using **Agent > Import/Export** (page 57).
- Base an agent install package on a machine ID template using **Agent > Deploy Agents** (page 35).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using **Agent > Copy Settings** (page 55).
- Identify the total number of machine ID template accounts in your VSA using **System > Statistics** (page 389).

Agent

- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.
- Separate machine ID templates are recommended for Windows, Apple and Linux machines. Alternatively you can create a package that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

Predefined Alerts

If you create a machine ID account using Agent > **Create** and do not copy settings from any other machine, then several typical alerts are created for the machine ID account by default.

Copy new account settings from

Click a radio button next to any machine ID listed in the paging area. Agent settings are copied from this machine ID.

Note: If you don't include a machine ID to copy from and click **Create**, a new, usable machine ID account is created using Kaseya Server defaults.

New Machine ID

Enter a unique name for the new machine ID you are creating.

Group ID

Select an existing group ID for the new machine ID you are creating. The default is `root.unnamed`. Group IDs are created by a VSA user using System > Orgs / Groups / Depts > **Manage** (page 372).

Create

Click **Create** to create the new machine ID for the selected group ID.

Set/Clear New accounts created in group ID <Group ID> copy settings from <Machine ID>

For each group ID you can specify a different default machine ID to copy settings from.

1. Select a machine ID to copy settings from by clicking the radio button next to any machine ID listed in the paging area.
2. Select a group ID from the group ID drop-down list.
3. Click the **Set** to ensure that new machine IDs you create for the selected group ID will copy settings from the selected default machine ID.
4. Click the **Clear** link to remove this assignment.

Set/Clear Accounts created in unassigned group IDs copy settings from <Machine ID>

This option specifies the default machine ID to copy settings from if no default machine ID is set for a group ID. This option only displays for **master role users** (page 564).

1. Select a machine ID to copy settings from by clicking the radio button next to any machine ID listed in the paging area. Initially this value is set to *unassigned*.
2. Click the **Set** to ensure that new machine IDs created without a group default machine ID copy settings from the master role user's default machine ID. Initially this value is set to *unassigned*.
3. Click the **Clear** link to remove this assignment.

Entering Contact Information









When you enter contact information on this page for a new machine ID account, then create the new machine ID account by clicking the **Create** button, these same contact information fields populate the Agent > **Edit Profile** (page 65) page. Contact information includes:

- **Contact Email** - Enter the email address of the individual using the managed machine.

- **Auto** - Check **Auto** to automatically populate the **Contact Email** field with an email address that uses the following format: `machineid@groupid.com`. This feature assumes you are creating machine IDs and group IDs that conform to user email addresses.
- **Contact Name** - Enter the name of the individual using the managed machine.
- **Contact Phone** - Enter the phone number of the individual using the managed machine.
- **Admin Email** - Enter the email address of the individual responsible for providing IT support for the managed machine.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (*page 16*) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Copy Settings

Click a radio button next to any machine ID listed in the paging area. Machine ID settings are copied from this machine ID.

Download / Email Agent Installation

Click a machine ID link to create and distribute an install package for an existing machine ID account using the **Download Agent** wizard.

Note: An install package created using this page is for a specific machine ID account. Use **Deploy Agent** (*page 35*) to create install packages for *multiple* machines.

1. Select the operating system you are creating the install package for: **Windows**, **Macintosh**, or **Linux**.
2. Optionally bind a user logon credential to the install package. Fill in the Administrator Credential form to securely bind user rights to the install package.
 - Users without user rights can install the package successfully without having to enter an administrator credential.
 - If the administrator credential is left blank and the user does not have user rights to install software, the install package prompts the user to enter a administrator credential during the install.
3. Select the method of distribution.
 - **Download** - Download the install package immediately to the machine you are currently using. The install package is always called **KcsSetup**.
 - **Email** - Email a text message that contains a link to download the install package.

Type

The type of operating system used by the managed machine:

- Windows
- Macintosh
- Linux

First Checkin

Lists the time that each agent checked into the Kaseya Server for the first time.

Delete

[Agent](#) > [Install Agents](#) > [Delete](#)

The [Delete](#) page deletes three different combinations of *machine ID accounts* and *agents*.

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the [machine ID / group ID / organization ID](#) ([page 556](#)) and the [agent](#) ([page 547](#)). The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

Agent License Counts

The following events affect agent license counts:

- An "unused" agent license is changed to "used" if a machine ID account is created and the agent installed.
- If the agent is deleted but not the account, the agent license is still considered "used".
- If the account is deleted, regardless of what happens to the agent, the agent license goes back to "unused".
- If an account is created, but the agent is not yet installed the first time, the account is called a [machine ID template](#) ([page 557](#)). Machine ID template accounts are not counted as "used" until you install the agent.

Deleting Agents with Tickets

Deleting a machine account reassociates any **Service Desk** tickets or **Ticketing** tickets with the machine group or organization that machine account was a member of.

Procedure

1. Select one or more machine IDs in the paging area.
2. Click one of the following radio buttons:
 - **Uninstall agent first at next check-in** - Uninstall the agent from the machine **and** remove the machine ID account from the Kaseya Server. The account is not deleted until the next time the agent successfully checks in.
 - **Delete account now without uninstalling the agent** - Leave the agent installed **and** remove the machine ID account from the Kaseya Server.
 - **Uninstall the agent and keep the account** - Uninstall the agent from the machine **without** removing the machine ID account from the Kaseya Server.
3. Click the **Delete Accounts** button.

Note: Uninstalling an agent does not remove K-VNC or the KBU client, KES client, or KDPM client. Before you delete the agent, use [Remote Control > Uninstall RC](#) ([page 332](#)) to uninstall K-VNC on the managed machine. Uninstall all add-on module clients as well.

Select old accounts that have not checked in since <date>.

Click the **Select old** hyperlink to check all machine IDs in the paging area that have not checked in since

the specified date. This is an easy way to identify and remove obsolete machine IDs.

Clean Database









Removing a machine account using this [Delete](#) page marks the machine account for deletion. Actual deletion usually occurs during off hours to reserve resources during working hours. There are some cases where it is useful to purge machine accounts immediately. For example, your Kaseya Server may exceed the agent license count. Click [Clean Database](#) to immediately purge machine accounts that are already marked for deletion.

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Last Check-In

Displays the time the machine's agent last checked in to the Kaseya Server. Agents that have not checked-in recently display this information **in red text**.

Rename

Agent > Install Agents > Rename

The [Rename](#) page renames any existing machine ID account. You can change the machine ID and/or re-assign it to a different group ID.

Agents are identified by a unique GUID number. Renaming the agent only changes the name the agent displays, both on the Kaseya Server and in the [Set Account...](#) option on the agent menu of the managed machine.

Note: See [Agent > Change Group](#) (page 55) to assign multiple machines to a different group ID.

Procedure

1. Select a machine ID in the paging area.
2. Click one of the following radio buttons:
 - [Rename account](#) - Select this option to rename a selected machine ID account.
 - [Merge offline account <Offline Machine ID> into <Select Machine ID> Delete <Offline Machine ID> after merge](#) - Use merge to combine log data from two different accounts into the same machine.

Agent

This could be necessary if an agent was uninstalled and then re-installed with a different account name. Merge combines the accounts as follows:

- ✓ Log data from both accounts are combined.
- ✓ **Baseline Audit** (page 551) data from the old offline account replaces any baseline data in the selected account.
- ✓ Alert settings from the selected account are kept.
- ✓ Pending agent procedures from the selected account are kept. Pending agent procedures from the old offline account are discarded.
- ✓ The old account is deleted after the merge.

Note: Since the machine can only be active on a single account, only offline accounts are provided in the drop-down list to merge with.

3. Optionally enter in a **New Name** for the machine ID account.
4. Optionally select a different **Group ID** for the machine ID account.
5. Click the **Rename** button.

Rename

Click **Rename** to change the name of a selected machine ID account, using the options previously selected.

New Name









Enter the **New Name** for the selected machine ID.

Group ID

Select the **Group ID** to assign to the selected machine ID account. The default leaves the group ID unchanged.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369). Click the radio button to the left of the machine account you wish to rename.

New Name at Next Check-in

Lists the new name the account will be renamed to the next time that agent checks in. Only pending renames are displayed here.

Change Group

[Agent](#) > [Install Agents](#) > [Change Group](#)

The [Change Group](#) page assigns multiple machines IDs to a different group ID. Machines currently offline are assigned the next time they check in.

Moving a Machine ID to a Different Group

1. Select one or more machine IDs in the paging area.
2. Select a group ID from the [Select new group ID](#) drop-down menu.
3. Click the [Move](#) button.

Move

Assigns selected machine IDs to the selected group ID.

Select new group ID

Specify the new group ID to assign to each selected machine ID.









Note: Create a new machine group ID or sub group ID using [System > User Security > Scopes](#) (page 369).

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using [System > User Security > Scopes](#) (page 369).

Copy Settings

[Agent](#) > [Configure Agent](#) > [Copy Settings](#)

The [Copy Settings](#) page copies selected settings from a single source machine ID to multiple machine IDs. You can copy settings *from only one source* machine ID or template at a time. But you can copy different types of settings from different source machine IDs or templates in succession.

Copy Settings and Templates

[Machine ID templates](#) (page 557) are initially used to create an agent install package using the template as the source to copy settings from. But even after agents are installed on managed machines, you'll need

Agent

to update settings on existing machine ID accounts as your customer requirements change and your knowledge of the VSA grows. In this case use Agent > **Copy Settings** to copy these changes to any number of machines IDs you are authorized to access. Be sure to select **Do Not Copy** for any settings you do not want to overwrite. Use **Add** to copy settings without removing existing settings. Kaseya recommends making changes to a selected template first, then using that template as the source machine ID to copy changes from. This ensures that your machine ID templates remain the "master repositories" of all your agent settings and are ready to serve as the source of agent install packages and existing machine ID accounts.

Copy

Click **Copy** to select a source machine. Once you select the source machine a second window displays the types of settings you can copy.

By selecting only certain types of settings to copy, you can avoid overwriting customer specific settings you want to keep, such as the **Patch File Source**, which is different for each customer.

Select the **Add** option to add settings to target machines without replacing existing settings.

The types of agent settings you can copy include:

- Credential
- Agent Menu
- Checkin Control
- Working Directory
- Logs
- Machine Profile - Refers to settings in Audit > **Edit Profile** (page 65).
- View Collections
- Portal Access
- Remote Control Policy
- Patch Settings
- Patch File Source
- Patch Policy Memberships
- Fixed Alerts - These are all the alert types on the Monitor > **Alerts** (page 248) page except for **Event Log alerts** and **System alerts**.
- Event Log Alerts
- Monitor Sets
- Distribute Files
- Protection
- Agent Procedure Schedules

Select Machine ID

Click the **Select Machine ID** link to specify which machine ID to copy settings from.

Spread agent procedure schedules when copying to multiple machines









You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10,

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Status

Shows the machine name that settings were copied from and the time they were copied.

Import / Export

Agent > Configure Agent > Import / Export

The **Import / Export** page imports and exports machine ID account settings as XML files, including scheduled agent procedures, assigned monitor sets and event sets. Log data is not included in the import or export. You can use **Import / Export** to migrate machine ID account settings, including **machine ID templates** (page 557), from one Kaseya Server to the next.

- When importing an XML file ensure the encoding of the file is ISO-8859-1.
- See **Copy Settings** (page 55) for a list of the types of settings associated with a machine ID account.
- For the latest instructions on migrating an existing Kaseya Server to a new machine see *Moving the Kaseya Server* section in the latest **Kaseya Server installation instructions** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/Install/index.asp#home.htm>).
- Sample templates for specific types of machines can be imported and are available on the Kaseya forum in our **Kaseya Connections** website at <http://community.kaseya.com> (<http://community.kaseya.com>).

To Export Machine ID Settings

1. Click the **select the machine** link. A machine selection dialog box displays.
2. Optionally filter the display of the machine IDs listed using the **machine ID / group ID filter** (page 556).
3. Click a machine ID link to export. The machine ID you selected now displays on the **Import / Export** page.
4. Click **Export**. The page displays an XML statement of the agent settings being exported.
5. Export the XML statement by:
 - Copying the XML text to the clipboard.
 - Right-clicking the **Download** link and selecting the **Save Target As** option to save the XML text as an XML file on your local computer.

To Import Machine ID Settings



1. When importing an XML file ensure the encoding of the file is ISO-8859-1.
2. Click **Browse** to select an XML file representing the settings of a machine ID account. Typically these XML files are created by exporting them from another Kaseya Server.
3. Click **Import**. A set of additional options displays.

Agent

4. Accept or specify the name of the machine ID. A new one is created if this name doesn't already exist in the Kaseya Server.
5. Accept or select a different group ID.
6. Optionally check the box next to **Replace existing data if this machine ID already exists**.
7. Optionally change the email notification address for all alerts defined for this machine ID account.
8. Click **Finish** to complete the import.

Suspend

Agent > Configure Agent > Suspend

The **Suspend** page suspends all agent operations, such as agent procedures, monitoring, and patching, without changing the agent's settings. When suspended, a machine ID displays a suspended icon  next to it. While a machine ID account is suspended the managed machine displays a gray agent icon  in the **system tray** (on page 564).

You can filter the display of machine IDs on any agent page using the **Show machines that are suspended/not suspended** option in **View Definitions** (page 24).

Suspend

Click **Suspend** to suspend agent operations on selected machine IDs.

Resume









Click **Resume** to resume agent operations on selected machine IDs.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID



The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Suspended

Displays **Suspended** if the machine ID is suspended.

Agent Menu

Agent > Configure Agent > Agent Menu

The **Agent Menu** page specifies the options that display in the agent menu of a user's machine. The user displays the agent menu by right-clicking the agent icon  in the **system tray** (on page 564) of the managed machine. This page can also *prevent* the agent icon  from displaying on the user's machine. Changes made using this page take effect at the next agent check-in and display **in red text** until then.

Note: See [Agent Icons](#) (page 21) for a general explanation of how agent icons display on the user's machine.

Hiding the Agent Icon on the User's Machine

To hide the agent icon altogether:

1. Select one or more machine IDs.
2. Uncheck the **Enable Agent Icon** checkbox.
3. Click **Update**.

All of the other checkbox settings will become dimmed, indicating that all agent menu options have been disabled.

Preventing the User from Terminating the Agent Service on the User's Machine

If the **Exit** option is enabled on a user's managed machine, the user can terminate the agent service on the managed machine by selecting this option. When the agent service is stopped, the managed machine displays as offline to VSA users and can no longer receive commands from the Kaseya Server.

To remove the **Exit** option from agent menus on managed machines:

1. Select one or more machine IDs.
2. Uncheck the **Exit** checkbox.
3. Click **Update**.

Checkboxes

- **Enable Agent Icon** - Check to display the agent icon in the system tray of the managed machine. Uncheck to hide the agent icon and prevent the use of agent menu options.
- **About <Agent>** - Check to enable the machine user to click this option to display the About box for the installed agent. The default option label Agent can be customized.
- **<Contact Administrator...>** - Check to enable the machine user to click this option to display either the user's **Portal Access** (page 561) page or a different contact URL. The default option label Contact Administrator... can be customized.
- **<Your Company URL...>** - Check to enable the machine user to click this option to display the URL specified in the corresponding URL field.
- **Disable Remote Control** - Check to enable the machine user click this option to *disable* remote control on the user's managed machine.
- **Set Account...** - Check to enable the machine user to click this option to display their machine ID.group ID.organization ID and to change the Kaseya Server address the agent checks into. The new IP address you enter must point to a working VSA, or else the IP address change will not take effect.
- **Refresh** - Check to enable the machine user to initiate an immediate **full check-in** (page 552).
- **Exit** - Check to enable the machine user to terminate the agent service on the managed machine.

Update

Click **Update** to apply agent menu settings to selected machine IDs.









Agent

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

ACObSRx

This column summarizes the agent menu options enabled for a machine ID. [ACObSRx](#) applies to the keyboard shortcuts that are used to access each option in the agent menu.

A letter indicates that option displays in the agent menu. A "-" indicates that menu option does not display in the agent menu.

A = [About Agent](#)

C = [Contact User](#)

O = Launches the URL specified in the URL field. The agent displays the text listed in the field to the left of the URL field.

b = [Disable Remote Control](#)

S = [Set Account...](#)

R = [Refresh](#)

x = [Exit](#)

About Title

The text appended to the label for the [About](#) option on the agent menu. For example, if the About Title is Agent then the label of the [About](#) option displays as About Agent.

Contact Title

The text displayed on the agent menu for contacting a VSA user.

Custom Title

The text displayed on the agent menu for contacting a custom URL.

Contact URL

The URL to display when the [Contact Administrator...](#) option is selected by the machine user. The default URL is the [Portal Access](#) (page 67) page. A different URL can be entered.

Custom URL

The URL to display when this agent menu option is selected by the user.

Check-In Control

Agent > Configure Agent > Check-In Control

The **Check-In Control** page specifies when and where each agent should check in with a Kaseya Server. You can specify the primary and secondary Kaseya Server names/IP addresses used by the agent to check in, the bandwidth consumed by an agent to perform tasks and the check-in period.

- The agent only checks into the primary server but not the secondary server, unless the primary server goes offline.
- The primary and secondary Kaseya Server values and the minimum and maximum check-in periods are subject to the policies set using System > **Check-in Policy** (page 356). This prevents users from selecting settings that place undue stress on servers running the Kaseya Server service.
- Changes made using this page take effect at the next agent check-in and display **in red text** until then.
- **Check-in Control** information can also be maintained using the **Agent Settings** tab of the **Live Connect** (page 53) and **Machine Summary** (page 131) pages.

Secondary Server Limitations

Legacy remote control functions are relayed through the primary Kaseya Server address. When an agent checks into the secondary Kaseya Server address, legacy remote control sessions do not connect because they are directed to the wrong VSA relay server address. All other functions, including Kaseya Remote Control functions, are supported and scheduled by the secondary Kaseya Server in the same manner as the primary Kaseya Server address.

Migrating Agents from one Kaseya Server to Another

You may decide for performance or logistical reasons to migrate managed machines to a new Kaseya Server. This can be done at any time, whether or not the agents are currently checking in.


1. At the **original** Kaseya Server, set the **primary** Kaseya Server setting to point to the **new** Kaseya Server address.
2. At the **original** Kaseya Server, point the **secondary** Kaseya Server setting to the **original** Kaseya Server.
3. At the **new** Kaseya Server, set both the **primary** and **secondary** Kaseya Server to point to the **new** Kaseya Server.
4. Wait for all the agents to successfully check into the **new** Kaseya Server. At that time, the **original** Kaseya Server can be taken off-line.

Note: For the latest instructions on migrating an existing Kaseya Server to a new machine see *Moving the Kaseya Server* section in the latest Kaseya Server installation instructions (<http://help.kaseya.com/webhelp/EN/VSA/7000000/Install/index.asp#home.htm>).

Changing the Port used by Agents to Check into the Kaseya Server

1. Set the **Primary** Port to the **new** port.
2. Set the **Secondary** Port to the **old** port.
3. Wait for the new settings to take effect on all the agents.
4. Display the System > **Configure** (page 377) page. Enter the new port number in the **Specify port Agents check into server with** edit box and click the **Change Port** button.

Agent

Note: If any agents have not migrated to the new port before you switch the Kaseya Server, you will have to manually change the port at the managed machine. Right click the agent icon  in the system tray to display the agent menu on the managed machine and select the **Set Account...** option. Enter the server address and port. For example, 192.168.1.7:1234.

Primary KServer

Enter the IP address or fully qualified **host name** (*on page 555*) of the machine ID's primary Kaseya Server. This setting is displayed in the **Primary Kaseya Server** column.

Kaseya agents initiate all communication with the Kaseya Server. For this reason the agents must always be able to reach the domain name or IP (Internet Protocol) address assigned to the Kaseya Server. Choose an IP address or domain name which can be resolved from all desired network(s), both on the local LAN and across the internet.

Best Practices: Although a public IP address may be used, Kaseya recommends using a **domain name server (DNS)** name for the Kaseya Server. This practice is recommended as a precaution should the IP address need to change. It is easier to modify the DNS entry than redirecting orphaned agents.

Primary Port

Enter the port number of either the primary Kaseya Server or a virtual system server. This setting is displayed in the **Primary KServer** column.

Warning: Do NOT use a *computer name* for your server. The agent uses standard WinSock calls to resolve a fully qualified **host name** (*on page 555*) into an IP address, which is used for all agent connections. Resolving a computer name into an IP address is done by NETBIOS, which may or may not be enabled on each computer. NETBIOS is an optional last choice that the Windows will attempt to use to resolve a name. Therefore, only fully qualified names or IP addresses are supported.

Secondary KServer

Enter the IP address or fully qualified host name of the machine ID's secondary Kaseya Server. This setting is displayed in the **Secondary KServer** column. The agent only checks into the primary server but not the secondary server, unless the primary server goes offline.

Secondary Port



Enter the port number of either the secondary Kaseya Server or a virtual system server. This setting is displayed in the **Secondary KServer** column.

Check-In Period

Enter the time interval for an agent to wait before performing a **quick check-in** (*page 552*) with the Kaseya Server. A check-in consists of a check for a recent update to the machine ID account. If a recent update has been set by a VSA user, the agent starts working on the task at the next check-in. This setting is displayed in the **Check-In Period** column. The minimum and maximum check-in periods allowed are set using System > **Check-in Policy** (*page 356*).

Best Practices: The agent maintains a persistent connection to the Kaseya Server. As a result, quick check-in times do not effect response times from the agent. The quick check-in time sets the maximum time to wait before re-establishing a dropped connection. Setting all your machine's quick check-in time to 30 seconds guarantees each agent recovers from a dropped connection within 30 seconds, assuming connectivity is successful.

Bind to Kserver

If checked, the agent is bound to a **unique Kaseya Server ID**. Bound agents cannot check-in successfully unless the unique Kaseya Server ID they are bound to using the Agent > **Check-in Control** (page 61) page matches the unique ID assigned to the Kaseya Server using the System > **Configure** (page 377) > **Change ID** option. Prevents IP address spoofing from redirecting agent check-ins. A lock  icon in the paging areas shows the agent is bound. To *unbind* agents, select machine IDs, ensure **Bind to Kserver** is unchecked and click **Update**. The lock  icon no longer displays for selected machines.

Bandwidth Throttle

Limit the agent to consuming a maximum amount of bandwidth on the system with this control. By default the agent shares bandwidth with all other running applications so you typically do not need bandwidth throttle enabled. Disable bandwidth throttle by entering a 0.

Warn if multiple agents use same account

The Kaseya Server can detect if more than one agent is connecting to the Kaseya Server and using the same machine ID.group ID.Organization ID. This problem could be caused by installing an agent install package pre-configured with the machine ID on more than one machine. Check this box to receive notifications of more than one agent using the same account each time you log into the Kaseya Server as a user.

Warn if agent on same LAN as KServer connects through gateway

If you are managing machines that share the same LAN as your Kaseya Server then you may get this alert. By default all agents connect back to the Kaseya Server using the **external name/IP address** (page 377). TCP/IP messages from these agents travel through your internal LAN to your router, and then back to the Kaseya Server. Some routers do a poor job of routing internal traffic back through themselves. Check this box to receive a notification when the Kaseya Server detects an agent may be on the same LAN but connecting through the router.









Note: Agents on the same LAN as the Kaseya Server should specify the internal IP address shared by both the agent and the Kaseya Server on the **Check-In Control** (page 61) page.

Update

Click **Update** to update all selected machine IDs with the options previously selected.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and

the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Working Directory

[Agent](#) > [Configure Agent](#) > [Working Directory](#)

The [Working Directory](#) page sets the path to a directory on the managed machine used by the agent to store working files.

Depending on the task at hand, the agent uses several additional files. The server transfers these files to a working directory used by the agent on the managed machine. For selected machine IDs you can change the default working directory from C:\kworking to any other location.

Warning: Do not delete files and folders in the working directory. The agent uses the data stored in the working directory to perform various tasks.

You can approve this directory in security programs, such as virus checkers, to allow operations such as remote control from being blocked.

Note: A working directory can also be maintained using the [Agent Settings](#) tab of the [Live Connect](#) (page 344) and [Machine Summary](#) (page 131) pages. A working directory can be written to using a `getVariable()` command in agent procedures.

Set

Click [Set](#) to set selected machine IDs use the working directory previously entered.

Set a path to a directory used by the agent to store working files

Enter the path of the working directory used by the agent on the managed machine.

Set as System Default









Click [Set as System Default](#) to set a system-wide default for the agent working directory. This option only displays for [master role users](#) (page 564).

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Working Path

The path of the working directory assigned to this machine ID. On a Apple OS X system, if the path name contains a space, then it must be preceded with a backslash. For example: `/tmp/name\ with\ three\ spaces`

Edit Profile

Agent > Configure Agent > Edit Profile

The **Edit Profile** page maintains contact information, the language preference for the agent menu on the user's machine and notes about each machine ID/group ID account. Profile information can be maintained in three other places:

- The contact information in the **Edit Profile** page can be automatically populated when a new account is created using the Agent > **Create** (page 48) page.
- VSA users and machine users can both maintain contact information using the Home > **Change Profile** tab in the **Live Connect** (page 344) or **Portal Access** (page 67) window.
- VSA users only can maintain notes and contact information using the **Agent Settings** tab of the **Live Connect** (page 344) and **Machine Summary** (page 131) pages.






To change user accounts settings:

1. Select a machine ID in the paging area.
2. Enter **Notes**, **Admin Email**, **Contact Name**, **Contact Email** and **Contact Phone** information.
3. Press **Update**.

Special Instructions

Enter any notes about a machine ID account. Helpful information can include the machine's location, the type of machine, the company, or any other identifying information about the managed machine. These special instructions display when you hover the cursor over an agent status icon with a badge. The **Quick View** (page 16) window displays the **Special Instructions** text in the bottom of the window.

Icon Badge

Add *badges* to the lower right corner of agent status icons, such as   . These badges display everywhere the agent icon displays in the user interface. For example, you could mark a machine with a  badge to indicate the customer requires a phone call before anyone works on that machine. Or mark a server with a  badge because you should not do anything to it until after hours.

Select one or more machines on the Agent > **Edit Profile** (page 65) page, then click the **Icon Badge** link at the top of the page and select one of the available badges. You can define a **Special Instructions** text message for each badge. Click the **Update** button to assign the badge to selected machines.

When you hover the cursor over an agent status icon with a badge, the **Quick View** (page 16) window displays the **Special Instructions** text in the bottom of the window.

Auto assign tickets

Auto assign a ticket to this machine ID if the **Ticketing email reader** (page 414) or a **Service Desk** email reader receives an email from the same email address as the **Contact Email** field of **Edit Profile**. Applies when new emails come into the **Ticketing** email reader that do not map into any of the **email mappings** (page 416) or as described for **Service Desk** in the Ticket Associations section of the **Readers tab** (<http://help.kaseya.com/webhelp/EN/KSD/7000000/index.asp#7560.htm>) topic in online help.

Note: if multiple machine IDs have the same **Contact Email** value, then only one machine ID can have this checkbox checked.

Agent

Contact Name

Enter the name of the individual using the managed machine. This setting is displayed in the **Contact Name** column.

Contact Email

Enter the email address of the individual using the managed machine. This setting is displayed in the **Contact Email** column.

Contact Phone

Enter the phone number of the individual using the managed machine. This setting is displayed in the **Contact Phone** column.

Admin Email

Enter the email address providing administrator support for this managed machine. This setting is displayed in the **Admin Email** column.

Language Preference

The language selected in the **Language Preference** drop-down list determines the language displayed by an **agent menu** (page 59) on a managed machine. The languages available are determined by the language packages installed using System > **Preferences** (page 353).

Machine Role

The machine role to apply to selected machine IDs. **Machine roles** (page 367) determine the **Portal Access** (page 67) functions available to the machine user.

Update









Click **Update** to update selected machine IDs with the profile information previously entered.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Portal Access

Agent > Configure Agent > Portal Access

The **Portal Access** page defines the logon name and password, by machine ID, required to use **Live Connect** (page 344) as a machine user *remotely*. A **Live Connect** session run by a machine user is called **Portal Access**. The functions displayed using **Portal Access** are determined by the System > Machine Roles > **Access Rights** (page 368) tab.

Note: You can download a Live Connect PDF from the first topic of online help.

Note: See **Enabling Ticketing for Portal Access Users on Unsupported Browsers** (page 68).

Accessing Portal Access Locally

Machine users do not have to logon to **Portal Access** locally. Clicking the agent icon in the system tray of their machine initiates the **Portal Access** session without having to logon.

Accessing the Portal Access Logon Page Remotely

A machine user can display the **Portal Access** logon page for their own machine from another machine as follows:

1. Browse to the `http://your_KServer_address/access/` page, substituting the appropriate target Kaseya Server name for `your_KServer_address` in the URL text.

Note: This is the same page that VSA users use to logon to the VSA.

2. Logon by entering the user name and password assigned to the machine ID. The user name and password is specified using the Agent > **Portal Access** page.

The **Portal Access** page displays. The machine user can click any menu option as though he or she were logged in from their own managed machine. The machine user can click the **Desktop** or **File Transfer** menu options to initiate a remote connection to their own machine, create or view ticket, or initiate a chat, if these options are enabled by machine role.

Re-Enabling User Logons

Machine user logons follow the same **Logon Policy** (page 391) as VSA user logons. If a user attempts to logon too many times with the wrong password their account will automatically be disabled. You can re-enable the logon by setting a new password or waiting for the disable account time to lapse.

Customizing Portal Access

Portal Access sessions can be customized using System > Customize > **Live Connect** (page 398), including adding a logo, welcome page and links to other URLs.

Logon Name

Enter the **Logon Name** the user must use to log into the VSA to initiate chat sessions, enter or view tickets and/or get remote access to their machine. Logon names and passwords are case sensitive. Passwords must be at least six characters long. The **Logon Name** defaults to the `machineID.groupID` name.

Create Password, Confirm Password

Define a password for the machine user logon. Passwords must be at least 6 characters long. The machine user can change the password after the VSA user assigns one.

Apply

Click **Apply** to apply the **Portal Access** logon name and password to the selected machine ID.

Agent

Clear

Permanently remove the **Portal Access** logon **credential** (page 553) from the selected machine ID.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Logon Name

The **Portal Access** logon name assigned to this machine ID.

User Web Logon

Displays **Enabled** if a **Portal Access** logon name and password has been assigned to this machine ID. Indicates that a machine user can log into the **Portal Access** page for their own machine *remotely* using a web browser on any other machine.

Enabling Ticketing for Portal Access Users on Unsupported Browsers

Live Connect and **Portal Access** are not supported on certain browsers, such as browsers older than IE8 or Firefox 3.5. Machine users required to work with unsupported browsers can be enabled to create and view **Ticketing** (page 400) tickets as follows:

1. Create a separate machine role for unsupported browser users in System > **Machine Roles** (page 367). For example, create a **Tickets Only** machine role.
2. For the new machine role you just created, uncheck the **Live Connect** checkbox in the System > Machine Roles > **Access Rights** (page 368) tab.
3. Assign machines with unsupported browsers to this new machine role.
4. When machine users click their agent icon, a single **Ticketing** window displays instead of the **Portal Access** window.

Note: Enabling this option applies to all users using the same managed machine.

Set Credential

Agent > Configure Agent > Set Credential

The **Set Credential** page registers the credential required by an agent to perform user level tasks on a managed machine. A credential is the logon name and password used to authenticate a user or process's access to a machine or network or some other resource. Most agent tasks do not require a credential. Credentials are specifically required or referenced by the following:

- **Patch Management** - If a credential is defined for a machine ID, then **Patch Management** installs all new patches using this credential. Therefore, **Set Credential** (page 68) should always be *a user with administrator rights*.
- **Patch Status** - Patch Status resets test results every time a machine ID's **Set Credential** changes.
- **File Source** - File Source may require a set credential be defined for the machine ID acting as the file share.
- **Patch Alert** - Set up an alert to notify you if a machine ID's credential is missing or invalid.
- **Office Source** - The agent must have a credential to access the alternate Office source location, in case a patch is being installed when no user is logged into the machine.
- **If-Then-Else** (page 84) - The `useCredential()` command in the agent procedure editor requires a credential be defined in **Set Credential** to run successfully.

- **Backup > Image Location** (<http://help.kaseya.com/webhelp/EN/KSD/7000000/index.asp#7948.htm>) - If a UNC path is specified in **Image Location**, a credential must be defined using **Set Credential** that provides access to this UNC path. Without the credential, the machine will *not* have access to the image location and the backup will fail. When specifying a UNC path to a share accessed by an agent machine—for example `\\machinename\share`—ensure the share's permissions allow read/write access using the credential specified for that agent machine in Agent > **Set Credential** (*page 68*).
- **View Definitions** (*page 24*) - Includes a **Machines with Credential status** option that allows you to filter the display of machine IDs on any agent page by their credential status.
- Desktop Management - Installing the client for this module requires a credential be defined.

Blank Passwords

Blank passwords can be used if the managed machine's **Local Security Policy** allows blank passwords. On the managed machine, open the Local Security Policy tool in Administrative Tools. Navigate to **Local Policies - Security Options**. Look for a policy named **Accounts: Limit local account use of blank passwords to console logon only**. The default setting is enabled. Change it to disabled and a credential with a blank password will work.

Username

Enter the username for the credential. Typically this a user account.

Password

Enter the password associated with the username above.

Domain

Local user account - Select this option to use a credential that logs into this machine locally, without reference to a domain.

Use machine's current domain - Create a credential using the domain name this machine is a member of, as determined by the **latest audit** (*page 551*). This makes it easier to **Select All** and rapidly set a common username/password on multiple machines, even if selected machines are members of different domains.

Specify domain - Manually specify the domain name to use for this credential.

Apply

Assign the credential to all checked machine IDs. Machine IDs with assigned credentials display the username and domain in the associated table columns.

Clear

Remove the credential from all checked machine IDs.

Test

Click **Test** to verify whether a username/password/domain credential will work before assigning it to a machine ID.

Cancel

Click **Cancel** to cancel the testing of a username/password/domain credential.

LAN Cache

Agent > Configure Agent > LAN Cache

The **LAN Cache** page designates a machine to act as a file source for other machines on the same LAN. When a LAN cache is enabled and a machine on the same LAN requests a download from the Kaseya

Agent

Server for the first time, files are downloaded to the LAN cache machine, then copied to the requesting machine. From then on the file does not need to be downloaded from the Kaseya Server. Other machines—on the same LAN and using the same LAN cache—copy the file from the LAN cache machine. Doing so speeds delivery to multiple machines throughout the same LAN and reduces network bandwidth issues.

Background

LAN Cache configures a file source as follows:

- Automatically creates a local administrator or domain administrator account, or allows you to manually specify the credential for an existing domain administrator. Created accounts are given a unique name (FSAdminxxxxxxxxx where x is a digit) with an automatically generated strong password. The generated password contains 15 randomly selected characters and contains at least one the following characters:
 - uppercase letters
 - lowercase letters
 - numbers (0 - 9)
 - non-alphanumeric characters
- Once the password is generated, it is compared against the admin name to ensure that no 2 character combinations in the password match any 2 character combination in the admin name. This logic ensures that the generated passwords will meet any Windows password complexity logic.
- The credentials for the account are associated with this LAN cache within Kaseya and are used when necessary instead of any assigned agent credential. *LAN Cache does not require nor support using the credential specified on the Set Credential page.*
- Creation of the specified customer share directory on the specified fixed disk drive configured as a Windows administrative share. The directory and share are created for you without leaving the **LAN Cache** page. The directory specified for LAN cache is strictly for customer use. *Kaseya never uses this customer-specified directory/share.*
- Creation of a special Kaseya directory—always `VSAFileShare` as a sub-directory under the customer directory—on the specified fixed disk drive configured as a Windows administrative share.

Procedure - General

1. Select a LAN cache machine.
2. Assign machines to the LAN cache using the **Assign LAN Cache** (page 72) page.

Procedure - For writeFile() and getURL() Steps in Agent Procedures

These commands can download files from a **LAN Cache** instead of the VSA or from a URL. Files have to be larger than 4k bytes.









1. Select a LAN cache machine.
2. Assign machines to the LAN cache using the **Assign LAN Cache** (page 72) page.
3. *For the writeFile() command only*, upload the files you intend to download to assigned machines to the Kaseya Server using Agent Procedures > Manage Procedures > Schedule / Create > **Manage Files** (page 108) > *Shared* folder. Files have to be larger than 4k bytes.
4. Create and run an agent procedure that includes a **writeFile()** (page 102) or **getURL()** (page 95) step.
 - When an agent executes the **writeFile()** or **getURL()** step of an agent procedure for the first time, it downloads the file from the KServer or the URL, then updates the assigned LAN cache with the file.
 - For subsequent requests for the same file by any agent, the file is downloaded from the LAN cache instead of from its original source.

- To take full advantage of the caching mechanism, execute the agent procedure referencing the file on one agent first. After that agent has uploaded the file to the assigned LAN cache, execute the procedure on other agents assigned to the same LAN cache.

Actions

- **Add LAN Cache** - Specifies a LAN cache on a selected machine.
 - **1. LAN Cache Name** - Enter a name of the LAN cache as it will be displayed in **Assign LAN Cache**.
 - **2. Directory Name** - Enter the name of the directory only, without specifying the name of the machine or the drive letter. The directory does not have to already exist. LAN Cache will create the directory and the required share settings for you.
 - **3. Select the UNC server name resolution - Use Computer Name or Use Computer IP Address.** Specifies the UNC name resolution format used to access the share. Example:
 \\computername\sharename\$ or \\10.10.10.118\sharename\$.
- Note:** The next step—selecting the type of credential—does not display if the **System > Default Setting (page 384) > LAN Cache - Use auto-generated administrator credentials** option is set to yes.
- **4. Select the type of LAN Cache administrator credentials to use**
 - ✓ **Use auto-generated administrator credentials** - If selected, an administrator credential is created for you when the LAN Cache is created. A local administrator credential is created unless the machine is a domain controller. If the machine is a domain controller, a domain administrator credential is created.
 - ✓ **Use an existing domain administrator credential** - If selected, enter the domain, username and password of an existing domain credential. The domain credential will not be created for you.
 - **5. Select a fixed drive on which to create the LAN Cache** - Select the drive to create the share on.
- **Remove LAN Cache** - Removes the LAN cache from a selected machine.
 - **Clear Pending** - Cancels the pending creation of a LAN cache on a selected machine.
 - **Test Generated Cache Credential** - Click to test the credentials used by a selected machine. The result is shown in the **Credential Test Status** column.

Columns

- **(Check-in Icon)** - These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window (page 16)**.
 -  Online but waiting for first audit to complete
 -  Agent online
 -  Agent online and user currently logged on.
 -  Agent online and user currently logged on, but user not active for 10 minutes
 -  Agent is currently offline
 -  Agent has never checked in
 -  Agent is online but remote control has been disabled
 -  The agent has been suspended
- **Machine.Group ID** - A unique **machine ID / group ID / organization ID (page 556)** name for a machine in the VSA.
- **Cache Name** - The name of the LAN cache as displayed with the VSA.
- **Cache Path** - The path specified for the LAN cache.
- **Cache UNC** - The UNC used to locate the LAN cache on the network.
- **Cache Created** - Date/time the LAN cache was created.
- **Cache Administrator** - The administrator account used to access the LAN Cache.

Agent

- **Credential Test Status** - Displays the results of testing the administrator account credentials used to access the LAN Cache. Credentials can be tested using the **Test Generated Cache Credential** button at the top of the page.

Assign LAN Cache

[Agent](#) > [Configure Agent](#) > [Assign LAN Cache](#)

The **Assign LAN Cache** page assigns machines to, and removes machines from, a selected **LAN Cache** ([page 69](#)) machine. When a machine is assigned to a LAN cache, the LAN cache autogenerated credential is created on that machine. If the machine is a domain controller, the autogenerated credential is a domain credential. If a domain account is specified on the **LAN Cache** page instead of the autogenerated credential, no credential is created on machines assigned to the LAN cache using this page.

Actions

- **Assign** - Assigns a LAN cache selected from the drop-down list to selected machines.
- **Unassign** - Unassigns a LAN cache from selected machines.
- **Clear Pending** - Cancels the pending assignment of a selected machine to a LAN cache.
- **Test Generated Cache Credential** - Click to test the credentials used by a selected machine. The result is shown in the **Credential Test Status** column.

Columns

- **Select All / Unselect All** - Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.
- **Machine.Group ID** - A unique **machine ID / group ID / organization ID** ([page 556](#)) name for a machine in the VSA.
- **Assigned LAN Cache** - Displays the LAN cache a machine is assigned to.
- **Assigned** - The date/time a machine was assigned to a LAN cache.
- **Test Status - Credential Test Status** - Displays the results of testing the administrator account credentials used to access the LAN Cache. Credentials can be tested using the **Test Generated Cache Credential** button at the top of the page.

Update Agent

[Agent](#) > [Upgrade Version](#) > [Update Agent](#)

The **Update Agent** page schedules managed machines to be updated with the latest version of the agent software at the agent's next check-in. Updating the agent software makes no changes to the **agent settings** ([page 547](#)) you have defined for each agent.

Note: Any agent used for monitoring must be updated using the [Agent > Update Agent](#) page.

Update Agent

Click **Update Agent** to schedule selected machines to be updated.

Remind me at logon when agents need an update

If checked, a popup window displays when VSA users logon if managed machines under their control need to be updated with the latest version of the agent software. The reminder only displays if at least one agent within the VSA user's **scope** ([page 369](#)) requires updating. Users can disable this feature at logon time and can re-activate it by selecting this checkbox.

Force update even if agent is at version x.x.x.x

If checked, machines selected for update are updated with new files to replace the agent files on the managed machine, even if the agent version is currently up to date. This performs a "clean" installation of the agent files.

After update run agent procedure <select agent procedure>

Select an agent procedure to run immediately after an agent update completes. This capability lets you re-apply customizations to an agent that may be lost after an agent update. Typically these customizations involve hiding or renaming agent identifiers on managed machines so as to prevent users from recognizing the agent is even installed.

Cancel Update

Click [Cancel Update](#) to cancel a pending update on selected managed machines.

Download Live Connect plugin installer for Windows browsers









For all versions of Windows supported by Live Connect, clicking this link downloads a standalone installer to the VSA user's local machine. The installer installs the Live Connect Plugin Manager and all Live Connect plugins for Chrome, Firefox and Internet Explorer.

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Agent Version

The version of the agent software running on the managed machine. **Version numbers in red** indicate that the version on the agent machine is not the same as the latest version available.

Update Agent Procedure

The agent procedure assigned to run when the agent is updated.

Last Update

The date the agent was last updated on the managed machine. Since the server must wait for the managed machine to check-in, according to the check-in schedule as specified in Agent > [Check-In Control](#) (page 61), **Pending** displays in the [Last Update](#) column until the next check-in occurs.

File Access

Agent > Protection > File Access

The **File Access** page prevents unauthorized access to files on managed machines by rogue applications or users. Any application can be approved or denied access to the file.

Note: You may also block operating system access to the protected file by blocking access to `explorer.exe` and/or `cmd.exe`. This prevents the file from being renamed, moved, or deleted therefore completely locking down the file from tampering.

Multiple Agents

If **multiple agents** (page 44) are installed on a machine, only one agent at a time controls the drivers required to use **File Access** (page 74), **Network Access** (page 75), **Application Blocker** (page 77). These functions can only be performed by the agent controlling these drivers.

Block

To protect a file from access by rogue applications, enter the filename and click the **Block** button. This displays the **File Access** popup window.

The dialog presents the user with one of the following options:

- **Filename to access control** - Enter the **file name and/or a portion of the full path**. For example, adding a file named `protectme.doc` to the list, protects occurrences of `protectme.doc` in any directory on any drive. Adding `myfolder\protectme.doc` protects all occurrences of the file in any directory named `myfolder`.
- **New** - Add in a new application to the access list. You can manually enter the application or use the **Search...** button to select an application name.
- **Remove** - Removes an application from the approved access list
- **Search** - Select a machine ID to search the list of applications installed on that machine ID and select an application name. This list is based on the latest audit performed on that machine ID. You are not actually browsing the managed machine.
- **Ask user to approve unlisted** - Lets users approve/deny access to the file on a per application basis each time a new application tries to access that file. Use this feature to build up an access control list based on normal usage.
- **Deny all unlisted** - Blocks an application from accessing the file. Select this option if you are already sure of which files need access and which do not.

Unblock





Remove an application from the protection list by clicking the **Unblock** button. This opens a new dialog box listing all protected files for the selected machine IDs. You can remove files from just the selected machine or from all machines containing that file path.





Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.


-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes

-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Filename

Filename of the file to be blocked. Click the edit icon  next to any filename to change file access permissions for that filename.

Approved Apps

Lists applications approved to access the file on the machine ID.

Ask User Approval

If checked, the user of a machine ID is asked to approve file access if an unapproved application attempts to access the file.

Network Access

[Agent](#) > [Protection](#) > [Network Access](#)

The **Network Access** page lets you approve or deny **TCP/IP-protocol-based network access** on a per application basis. Users can also be notified when an unlisted application accesses the network, permitting or denying that application network access. Typically this function is used to control access to internal and external *internet* sites, but can include internal LAN traffic that also uses the TCP/IP protocol.

Driver

This function requires the driver be *enabled* to block network access and monitor network bandwidth statistics. *The driver is disabled by default.* This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. *For Windows machines earlier than Vista, an enabled driver only takes effect after a reboot of the machine.*

Note: To determine which applications should be approved or denied network access, use the **Network Statistics** (page 181) report to view network bandwidth utilization versus time. Drill down and identify peak bandwidth consumers by clicking the graph's data points. See which application and which machine use bandwidth at any point in time.

Warning: Applications that do not use the Windows TCP/IP stack in the standard way may conflict with the driver used to collect information and block access, especially older legacy applications.

Multiple Agents

If **multiple agents** (page 44) are installed on a machine, only one agent at a time controls the drivers required to use **File Access** (page 74), **Network Access** (page 75), **Application Blocker** (page 77). These functions can only be performed by the agent controlling these drivers.

To approve or deny network access to one or more applications

1. Check the checkbox next to one or more machine IDs in the **Machine.Group ID** column.

Agent

2. Click the link of *any* machine ID in the **Machine.Group ID** column. It does not have to be the machine ID you checked. This displays the **Application List** popup window, listing all applications installed on that machine ID. The list is based on the latest audit that was performed for that machine ID.
3. Since the list in the **Application List** window may be large, you can control the applications displayed by clicking **Filter** to filter the list.
4. Check the checkboxes next to the application name you wish to approve or deny network access to.
5. You can also enter application names in the **Add applications not found by audit here** edit field, to identify applications not listed.
6. Click the **Select** button to confirm your selections and close the **Application List** window. The selected applications now display at the top of the page.
7. Click **Approve Apps** or **Deny Apps**. The applications selected in the **Application List** window are added from the **Approved Apps/Denied Apps** column.

To remove approve and deny settings for one or more machine IDs

1. Check the checkbox next to one or more machine IDs in the **Machine.Group ID** column.
2. Click the **Remove Apps** button.

Network Access Options









- **Notify user when app blocked** - Notify the user when a blocked application attempts to access the network. Use this function to build up the access list based on normal usage. This lets you see which applications on your system are accessing the network and when. The machine user is prompted to select one of four responses when an application is blocked:
 - **Always** - Allows the application access to the network indefinitely. Users will not be prompted again.
 - **Yes** - Allows the application access to the network for the duration of the session. Users will be prompted again.
 - **No** - Denies the application access to the network for the duration of the session. Users will be prompted again.
 - **Never** - Denies the application access to the network indefinitely. Users will not be prompted again.
- **Enable/Disable driver at next reboot** - **Enable/Disable** the network access protection driver for an agent. Applications that do not use the Windows TCP/IP stack in the standard way may conflict with this driver, especially older legacy applications. **The agent can not monitor network statistics or block network access if this driver is disabled.** *For Windows machines earlier than Vista, an enabled driver only takes effect after a reboot of the machine.*
- **Apply Unlisted Action** - An unlisted application is one that has not been explicitly approved or denied access to the network. Select the action to take when an unlisted application attempts to access the network.
 - **Ask user to approve unlisted** - A confirmation dialog box displays if an unlisted application attempts to access the network.
 - **Approve all unlisted** - The unlisted application is granted access to the network.
 - **Deny all unlisted** - The unlisted application is denied access to the network and the application is closed on the managed machine.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status


These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (*page 16*) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).


Notify User

A green checkmark  in the **Notify User** column indicates that the managed machine user is notified when an application attempts to access the network that has been denied network access.

To notify the user when a application has been denied:

1. Select machine IDs.
2. Click the **Enable** button for **Notify user when app is blocked**.

To remove this notification:

1. Select machine IDs that display a green checkmark  in the **Notify** column.
2. Click the **Disable** button for **Notify user when app is blocked**.

Enable Driver

Identifies on a per machine ID basis, which machines have the network protection driver enabled or not. *For Windows machines earlier than Vista, an enabled driver only takes effect after a reboot of the machine.*

Unlisted Action

Displays the **Unlisted Action** to take when an unlisted application attempts to access the network. See **Apply Unlisted Action** above.

Approved Apps / Denies Apps / Remove Apps / Remove All

These settings can only be applied once the driver is enabled.

- Approved applications are listed in the first row.
- Denied applications are listed in the second row.
- If the **Approve all unlisted** radio option is selected and applied to a machine ID, then the approved application list is replaced by the phrase Approve All Unlisted.
- If **Deny all unlisted** radio option is selected and applied to a machine ID, then the denied application list is replaced by the phrase Deny All Unlisted.
- Click **Remove Apps** to remove a selected applications from selected machines.
- Click **Remove All** to remove all applications from selected machines.

Application Blocker

Agent > Protection > Application Blocker

The **Application Blocker** page prevents any application from running on a machine ID. Blocked applications cannot be renamed, moved, or deleted from the system. **File Access** (page 74) can also block applications, but **Application Blocker** is faster to configure if you simply want to block and unblock

Agent

applications.

Multiple Agents

If **multiple agents** (page 44) are installed on a machine, only one agent at a time controls the drivers required to use **File Access** (page 74), **Network Access** (page 75), **Application Blocker** (page 77). These functions can only be performed by the agent controlling these drivers.

Block

To block an application from running on a machine:

1. Select one or more machine IDs. Only machine IDs currently matching the **Machine ID / Group ID filter** (page 23) are displayed.
2. Enter the application's filename in the edit box.
The application can be **referenced by file name and/or a portion of the full path**. For example, adding an application named `blockme.exe` to the list, prevents all occurrences of `blockme.exe`, on any directory or on any drive, from running. Adding `myfolder\blockme.exe` prevents occurrences of the application in any directory named `myfolder` from running.
3. Click the **Block** button.
4. The blocked application displays in the **Application** column beside the selected machine IDs.









Unblock

To unblock an application from the blocked list:

1. Select one or more machine IDs that show blocked applications in the **Application** column.
2. Click the **Unblock** button. This opens a **File Access** popup window listing all blocked applications for the selected machine IDs.
3. Click one or more blocked applications.
4. Click the **Unblock** button. The window closes.
5. The blocked application no longer displays in the **Application** column beside the selected machine IDs.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Application

Filename of the application being blocked.

Chapter 4

Agent Procedures

In This Chapter

Agent Procedures Overview.....	80
Schedule / Create.....	80
Distribution.....	109
Agent Procedure Status	110
Pending Approvals	111
Patch Deploy	112
Application Deploy.....	113
Packager	116
Get File	116
Distribute File.....	118
Application Logging	119

Agent Procedures Overview

Agent Procedures

The **Agent Procedures** module **creates and schedules agent procedures** (page 80) on managed machines. You can view the status of all procedures run on a managed machine using **Agent Procedure Status** (page 110). You can also spread out the impact agent procedures have on network traffic and server loading using **Distribution** (page 109).

The **Agent Procedures** module also provides:

- **File Transfers** - Transfer files to and from managed machines using **Get File** (page 116) and **Distribute File** (page 118).
- **Customized Installations** - When a pre-defined install solution cannot be used, use **Packager** (page 116) to create a self-extracting file ready for automated distribution.
- **Patch and Application Deployment** - You can schedule the installation of Microsoft and non-Microsoft applications and patches using **Patch Deploy** (page 112) and **Application Deploy** (page 113).

Note: See Patch Management to install Microsoft patches on managed machines.

Functions	Description
Schedule / Create (page 80)	Automates user-defined tasks on managed machines by creating and scheduling agent procedures.
Distribution (page 109)	Minimizes network traffic and server loading by executing agent procedures evenly throughout the day.
Agent Procedure Status (page 110)	Shows the status of agent procedures executed on managed machines.
Patch Deploy (page 112)	Use this wizard tool to create procedures to deploy Microsoft patches to managed machines.
Application Deploy (page 113)	Use this wizard tool to create procedures to deploy non-Microsoft install packages (setup.exe) to managed machines.
Packager (page 116)	An external application that allows users to create customized installation packages deployable on managed machines.
Get File (page 116)	View and manage files uploaded to the Kaseya Server from managed machines using the getFile() agent procedure command.
Distribute File (page 118)	Write files to all selected managed machines and maintain them.

Schedule / Create

Agent Procedures > Manage Procedures > Schedule / Create

The **Schedule / Create** page automates user-defined tasks on managed machines by creating and scheduling *agent procedures*. See the following topics for details:

- **Action Buttons** (page 81)
- **Scheduling Agent Procedures** (page 82)
- **Creating / Editing Agent Procedures** (page 83)
- **IF-ELSE-STEP Commands** (page 84)
- **64-Bit Commands** (page 103)

- [Using Variables](#) (page 104)
- [Variable Manager](#) (page 107)
- [Manage Files Stored on Server](#) (page 108)
- [Folder Rights](#) (page 108)

Related Topics

- [Agent Procedure Failure Alerts](#) - The [Alerts - Agent Procedure Failure](#) (page 262) page triggers an alert when an agent procedure fails to execute on a managed machine. For example, if you specify a file name, directory path or registry key in an agent procedure, then run the agent procedure on a machine ID for which these values are invalid, you can be notified about the agent procedure failure using this alerts page.
- [Logging Failed Steps in Procedures](#) - The System > [Configure](#) (page 377) page includes the following option - [Enable logging of procedure errors marked "Continue procedure if step fail"](#) - If checked, failed steps in procedures are logged. If blank, failed steps in procedures are *not* logged.
- [Preventing the Logging of Successful Child Script Execution](#) - The System > [Configure](#) (page 377) page includes the following option - [Enable logging of successful child script execution in agent procedure log](#) - If unchecked, child script success entries are not included in the [agent procedure log](#) (page 31). This can reduce the size of the agent procedure log tremendously. It takes up to 5 minutes for the KServer to read this setting change.
- [View Definitions](#) - You can filter the display of machine IDs on any agent page using the following agent procedure options in [View Definitions](#) (page 24).
 - [With procedure scheduled/not scheduled](#)
 - [Last execution status success/failed](#)
 - [Procedure has/has not executed in the last N days](#)


Action Buttons

Agent procedures are organized using two folder trees in the middle pane, underneath [Private](#) and [Shared](#) cabinets. The following action buttons display, depending on the object selected in the folder tree.

When a Cabinet is Selected

- [Collapse All](#) - Collapses all branches of the folder tree.
- [Expand All](#) - Expands all branches of the folder tree.

Always Available

- [Manage Files](#) - See [Manage Files Stored on Server](#) (page 108) for more information.
- [Manage Variables](#) - See [Variable Manager](#) (page 107) for more information.
- [\(Apply Filter\)](#) - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

When a Folder is Selected

- [Share Folder](#) - Shares a folder with user roles and individual users. *Applies to shared cabinet folders only.*

Note: See guidelines for share rights to objects within folder trees in the [Folder Rights](#) (page 108) topic.

- [New Procedure](#) - Opens the agent procedure editor to create a new procedure in the selected folder of the folder tree. See [Creating / Editing Agent Procedures](#) (page 83).
- [New Folder](#) - Creates a new folder underneath the selected cabinet or folder.

Agent Procedures

- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **Import Folder/Procedure** - Imports a folder or procedure as children to the selected folder in the folder tree. *Applies to private cabinet folders only.*
- **Export Folder** - Exports the selected folder and all its procedures as an XML file. The XML file can be re-imported.

Additional Actions When a Procedure is Selected

- **Edit Procedure** - Opens the agent procedure editor to edit the selected procedure. See [Creating / Editing Agent Procedures](#) (page 83).
- **Rename Procedure** - Renames the selected procedure.
- **Delete Procedure** - Deletes the selected procedure. Agent procedures that are used by other agent procedures cannot be deleted.
- **Export Procedure** - Exports the selected procedure.

Scheduling Agent Procedures

Manage the scheduling of agent procedures using tabs in the right hand pane. When a procedure is selected in the middle pane, the following tabs display in the right-hand pane.

- **Schedule** - Select one or more machine IDs in this tab's table, then click one of the following action buttons:
 - **Schedule Procedure** - Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:
 - ✓ **Schedule will be based on the timezone of the agent (rather than server)** - If checked, time settings set in the Scheduler dialog reference the local time on the agent machine to determine when to run this task. If blank, time settings reference server time, based on the server time option selected in System > [Preferences](#) (page 353). Defaults from the System > [Default Settings](#) (page 384) page.
 - ✓ **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
 - ✓ **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
 - ✓ **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
 - ✓ **Exclude the following time range - Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.

Note: You can stagger the running of scheduled agent procedures using [Agent Procedures > Distribution](#) (page 109).

- **Run Now** - Run this agent procedure on each selected machine ID immediately.
- **Cancel** - Cancel the scheduled agent procedure on each selected machine ID.
- **View Procedure** - Provides a display only view of the procedure. A user can execute an agent procedure and view it without necessarily being able to edit it. See [Folder Rights](#) (page 108) for more information.

- **Used by** - Displays a list of other procedures that execute this procedure. Agent procedures that are used by other agent procedures cannot be deleted.

Creating / Editing Agent Procedures

Creating / Editing Agent Procedures

To create a new procedure, select a cabinet or folder in the middle pane, then click the **New Procedure** button to open the **Creating / Editing Agent Procedures** (page 83).

To edit an existing procedure, select the procedure, then click the **Edit Procedure** button to open the **Creating / Editing Agent Procedures** (page 83). You can also double-click a procedure to edit it.

Note: Access to creating or editing a procedure depends on your **Folder Rights** (page 108).

The Agent Procedure Editor

All statements you can add to an agent procedure display in the left-hand pane. Agent procedures display in the middle pane of the editor on one more tabs. The parameters for each statement display in the right-hand pane.

Note: See **IF-ELSE-STEP Statements** (page 84) for a detailed explanation of each statement's parameters.

Action Buttons

These buttons display in the middle pane of the procedure editor.

- **Procedure**
 - **New** - Creates an empty tab for a new procedure.
 - **Open** - Edits an existing procedure.
 - **Save** - Saves the currently selected procedure.
 - **Save As** - Saves the procedure to a different name. A dialog enables you to select the folder used to save the procedure.
- **Edit** - The following buttons are only enabled when one or more statements are selected.
 - **Undo** - Undoes the last edit.
 - **Redo** - Redoes the last edit.
 - **Cut** - Cuts selected lines.
 - **Copy** - Copies selected lines.
 - **Paste** - Pastes copied lines.
 - **Remove** - Removes selected lines.
 - **Goto Line** - Selects the line number you specify.
 - **Search** - Searches for matching text in commands, parameters and values.
 - **Insert Lines** - Inserts a blank line that you can then begin typing into. This displays a drop-down list of commands that you can select a command from and insert into the procedure.
 - **Indent Lines** - Indents selected lines
 - **Outdent Lines** - Outdents selected lines.
- **Help**
 - **Help Tips** - Display tooltips on how to use the procedure editor.
 - **Online Help** - Displays online help.




Drag and Drop

- Drag and drop any statement above or below any other statement.

Agent Procedures

- Drag and drop any comment above or below any statement.
- A statement is automatically indented when dropped below an IF statement, except for an ELSE statement.
- You can nest steps within multiple IF or ELSE statements. Just drag-and-drop an IF or ELSE statement below an IF statement to insert it as a child statement.

Guidelines

- Click any STEP, IF or ELSE statement in the middle pane to see its settings in the right-hand pane. You can edit these settings in the right hand pane or click any value in a statement directly to edit it.
- Multiple lines can be selected and acted on at one time.
- Right click selected lines to get additional options.
- Enter a value at the top of the left pane to filter the list of statements you can select.
- Hovering the cursor over any statement in the left or middle pane displays a tooltip description of that statement. The same description displays at the top of the third pane.
- Hovering the cursor to the left of selected statements displays    icons. Click these icons to remove, indent or outdent selected statements.
- When entering a value for a variable into a parameter:
 - Enter a < to select from a list of system variables.
 - Enter a # to select from a list of **user defined variables** (page 104).
- Open and work on multiple procedures simultaneously. Each procedure you open displays in a separate tab. Copy and paste selected statements between tabs.
- You can set a STEP to **Continue on Fail**. This allows a procedure to continue running even if that particular STEP fails.
- Click the blank line at the bottom of the procedure to edit the description for the entire procedure.

IF-ELSE-STEP Commands

The following is a summary of standard IF-ELSE-STEP commands used in VSA agent procedures.

IF Definitions

checkVar() (page 87)	Evaluates the given agent variable. See Using Variables (page 104).
else (page 88)	Adds an Else branch to run steps when an If branch returns a False result.
eval() (page 88)	Compares a variable with a supplied value.
getOS() (page 88)	Determines if the current Windows OS is 32 or 64-bit.
getRAM() (page 89)	Evaluates the total amount of memory reported by the latest audit of the agent.
getRegistryValue() (page 89)	Evaluates the given registry value.
hasRegistryKey() (page 89)	Tests for the existence of the given registry key.
isAppRunning() (page 89)	Checks to see if a specified application is currently running on the managed machine.
isServiceRunning() (page 89)	Determines if a service is running on the managed machine.
isUserActive() (page 90)	Determines whether the user is either: <ul style="list-style-type: none">• Idle or not logged on, or• Active
isUserLoggedIn() (page 90)	Tests whether a specific user, or any user, is logged in or not.
isYesFromUser() (page 90)	Presents a Yes/No dialog box to the user.

testFile() (page 90)	Tests for the existence of a file.
testFileInDirectoryPath() (page 90)	Tests for the existence of a file in the current directory path returned by getDirectoryPathFromRegistry() .
true (page 91)	Always returns True, executing If branch.
STEP Definitions	
alarmsSuspend() (page 91)	Suppresses alarms on a machine for a specified number of minutes.
alarmsUnsuspendAll() (page 91)	Stops the suppression of alarms on a machine.
captureDesktopScreenshot() (page 91)	Captures a desktop screenshot of the agent machine and uploads it to the Kaseya Server.
changeDomainUserGroup() (page 91)	Changes a domain user's membership in a domain user group.
changeLocalUserGroup() (page 91)	Changes a local user's membership in a local user group.
closeApplication() (page 91)	Closes a running application.
comment() (page 91)	Adds a one-line comment to the procedure.
copyFile() (page 92)	Copies a file from one directory to another.
copyUseCredentials() (page 92)	Copies a file from one directory to another using a user credential.
createDomainUser() (page 92)	Adds a new user to an Active Directory domain when run on a domain controller.
createEventLogEntry() (page 92)	Creates an event log entry in either the Application, Security or System event log types. You can create a Warning, Error or Informational event with your own description.
createLocalUser() (page 92)	Adds a new local user account to a machine.
createWindowsFileShare() (page 92)	Creates a new file share on a Windows machine.
deleteDirectory() (page 92)	Deletes a directory from the agent machine.
deleteFile() (page 92)	Deletes a file from the managed machine.
deleteFileInDirectoryPath() (page 93)	Deletes file in directory returned by getDirectoryPathFromRegistry() .
deleteRegistryKey() (page 93)	Deletes a key from the registry.
delete64BitRegistryKey() (page 93)	Deletes a 64-bit (page 103) key from the registry.
deleteRegistryValue() (page 93)	Deletes a value from the registry.
delete64BitRegistryValue() (page 93)	Deletes a 64-bit (page 103) value from the registry.
deleteUser() (page 93)	Deletes a user from the agent machine.
disableUser() (page 93)	Disables a user, preventing logon to the agent machine.
disableWindowsService() (page 93)	Disables a Windows service.
enableUser() (page 93)	Enables a previously disabled user, allowing the user to logon to the OS.
executeFile() (page 93)	Executes any file as if it was run from the Run item in the Windows Start menu.
executeFileInDirectoryPath() (page 94)	Same as execute file. File location is relative to the directory returned by getDirectoryPathFromRegistry() .
executePowershell() (page 94)	Executes a powershell file, or command with arguments or both.
executePowerShell32BitSystem (page 94)	Executes a powershell file, or command with arguments or both, as a 32 bit system command.
executePowerShell32BitUser (page 94)	Executes a powershell file, or command with arguments or both, as a 32 bit user command.
executePowerShell64BitSystem (page 94)	Executes a powershell file, or command with arguments or both, as a 64 bit system command.

Agent Procedures

executePowerShell64BitUser (page 94)	Executes a powershell file, or command with arguments or both, as a 64 bit user command.
executeProcedure() (page 94)	Starts another VSA agent procedure on the current machine.
executeShellCommand() (page 94)	Runs any command from a command shell.
executeShellCommandToVariable() (page 95)	Executes a shell command and returns output created during and after its execution to a variable.
executeVBScript() (page 95)	Runs a Vbscript, with or without command line arguments.
getDirectoryPathFromRegistry() (page 95)	Returns the directory path stored in the registry at the specified location. Result used in subsequent steps.
getFile() (page 95)	Gets a file from the managed machine and saves it to the Kaseya Server.
getFileInDirectoryPath() (page 95)	Gets a file from the managed machine located relative to the directory returned by getDirectoryPathFromRegistry() and saves it to the Kaseya Server.
getRelativePathFile()	Uploads a file from a managed machine to an approved path on the Kaseya Server.
getURL() (page 95)	Returns the text and HTML contents of a URL and stores it to a file on the managed machine.
getURLUsePatchFileSource() (page 96)	Downloads a file from a given URL to a target folder and file for that agent. Uses the Patch Management > File Source settings.
getVariable() (page 96)	Gets a value from the agent on the managed machine and assigns it to a variable. See Using Variables (page 104).
getVariableRandomNumber() (page 96)	Generates a random number.
getVariableUniversalCreate() (page 96)	Gets a variable that persists outside of the immediate procedure's execution.
getVariableUniversalRead() (page 96)	Reads up to three variables you have previously created using the getVariableUniversalCreate() step.
giveCurrentUserAdminRights() (page 96)	Adds the current user to the local administrator's group on the agent machine, either permanently or for a temporary period of time.
impersonateUser() (page 96)	Specifies the user account to use when executing a file or shell when Execute as the logged on user is specified in a subsequent command.
installAptGetPackage() (page 97)	Silently installs a package using the <code>apt-get</code> command in Linux.
installDebPackage() (page 97)	Silently installs a Debian package on any Linux OS that supports <code>.deb</code> packages.
installDMG() (page 97)	Silently installs a <code>.DMG</code> package in OS X.
installMSI() (page 97)	Installs an MSI file for Windows.
installPKG() (page 97)	Silently installs a <code>.PKG</code> package in OS X.
installRPM() (page 97)	Silently installs an RPM package on any Linux OS that supports installing RPMs.
logoffCurrentUser() (page 97)	Automatically logs off the current user.
pauseProcedure() (page 97)	Pauses the procedure for N seconds.
reboot() (page 97)	Reboots the managed machine.
rebootWithWarning() (page 97)	Reboots a machine, displaying a warning message to the end-user before the reboot process occurs.
removeWindowsFileShare() (page 97)	Removes a file share from a Windows agent.
renameLockedFile() (page 98)	Renames a file that is currently in use.

renameLockedFileInDirectoryPath() (page 98)	Renames a file currently in use in directory returned by getDirectoryPathFromRegistry() .
scheduleProcedure() (page 98)	Schedules an agent procedure to run on a specified machine.
sendAlert() (page 98)	Creates an alert based on a previous getVariable() command.
sendEmail() (page 99)	Sends an email to one or more recipients.
sendMessage() (page 99)	Displays a message in a dialog box on the managed machine.
sendURL() (page 100)	Opens a browser to the specified URL on the managed machine.
setRegistryValue() (page 100)	Sets the registry value to a specific value.
set64BitRegistryValue() (page 100)	Sets the 64-bit (page 103) registry value to a specific value.
sqlRead() (page 100)	Returns a value from the database and stores it to a named variable by running a selected SQL "read" statement.
sqlWrite() (page 101)	Updates the database by running a selected SQL "write" statement.
startWindowsService() (page 101)	Runs a Start command for a Windows service, if it exists.
stopWindowsService() (page 101)	Runs a Start command for a Windows service if it exists.
transferFile() (page 101)	Transfers a file from the agent machine running this step to another agent machine.
uninstallbyProductGUID() (page 101)	Silently uninstalls a product based on its MSI GUID.
unzipFile() (page 101)	Extracts the contents of a specified zip file to a target folder.
updateSystemInfo() (page 102)	Updates the selected System Info field with the specified value.
useCredential() (page 102)	Specifies that Set Credential should be used when Execute as the logged on user is specified in a subsequent command.
windowsServiceRecoverySettings() (page 102)	Sets the Service Recovery Settings for any given service in Windows.
writeDirectory() (page 102)	Writes a directory from the server to the managed machine.
writeFile() (page 102)	Writes a file stored on the Kaseya Server to the managed machine.
writeFileFromAgent() (page 102)	Transfers a file from another agent machine to the agent machine running this step.
writeFileInDirectoryPath() (page 103)	Writes a file stored on the Kaseya Server to the managed machine using the directory returned by getDirectoryPathFromRegistry() .
writeProcedureLogEntry() (page 103)	Writes a string to the Agent Procedure Log.
writeTextToFile() (page 103)	Writes text to a file on the agent machine.
zipDirectory() (page 103)	Compresses a directory and any subdirectories or files it contains into a zip file on the agent machine.
zipFiles() (page 103)	Compresses a single file or files into a zip file on the agent machine.

IF Commands

checkVar()

Enter a variable name, in the form #var_name#, in the space provided. [checkVar\(\)](#) evaluates the current

Agent Procedures

values assigned `#var_name#` and compares it with the supplied value. The supplied value may also be another variable name in the form of `#var_name2#`. If the check is true, **IF** commands are executed. If the check is false, **ELSE** steps are executed. See [Using Variables](#) (page 104). The available tests are:

- **Exists** : true if the variable exists.
- **Does Not Exist** : true if the variable does *not* exist.
- **=** : true if value of the variable equals the test value.
- **Not =** : true if value of the variable does *not* equal the test value.
- **>** : true if value of the variable is greater than the test value.
- **>=** : true if value of the variable is greater than or equal to the test value.
- **<** : true if value of the variable is less than the test value.
- **<=** : true if value of the variable is less than or equal to the test value.
- **Contains** : true if the test value is a sub string of the variable value.
- **Not Contains** : true if the test value is *not* a sub string of the variable value.
- **Begins With** : true if the variable value begins with the test value.
- **Ends With** : true if the variable value ends with the test value.

For the tests **=**, **Not =**, **>**, **>=**, **<**, and **<=** the variables compared may be a string, a number, a date in the format of `yyyy/mm/dd` or `yyyy/mm/dd hh:mm` or `yyyy/mm/dd hh:mm:ss`, or a version number containing dots or commas such as `1.2.3` or `4,5,6,7`. Values in variables are stored as strings, so compared numbers must be of equal string length. If a date format is specified, it may be offset using **+** `dd:hh:mm:ss` or **-** `dd:hh:mm:ss`. Only `dd` days are required; `hh` hours, `mm` minutes, and `ss` seconds may be omitted and are assumed to be zero when absent. `CURRENT_TIMESTAMP` may be specified to indicate that the current time be substituted in the comparison at the time the procedure is executed. e.g. `CURRENT_TIMESTAMP - 7:12:00:00` will be evaluated as 7 days and 12 hours subtracted from the time that the procedure is executed.

else

Adds an **Else** command underneath a corresponding **If** command. Any steps listed under the **Else** command are executed when the corresponding **If** command returns a **False** result.

eval()

Enter an expression containing one or more variable names, in the form `#var_name#`, in the space provided. **eval()** uses the current value assigned to each `#var_name#`, evaluates the mathematical expression, and compares it with the supplied value. The supplied value may also be another expression. The mathematical expression may contain **+**, **-**, *****, **/**, **(**, and **)**. e.g. `(3.7 + (200 * #countA#)) / (#countB# - #countC#)`. If the check is true, **IF** steps are executed. If the check is false, **ELSE** steps are executed. The available tests are:

- **=** : true if value of the variable equals the test value.
- **Not =** : true if value of the variable does not equal the test value.
- **>** : true if value of the variable is greater than the test value.
- **>=** : true if value of the variable is greater than or equal to the test value.
- **<** : true if value of the variable is less than the test value.
- **<=** : true if value of the variable is less than or equal to the test value.

Note: Cannot be used with **Exists**, **Does Not Exist**, **Contains**, or **Not Contains** operators.

getOS()

Determines if the current Windows OS is 32 or 64-bit.
Operating systems supported: Windows

getRAM()

Evaluates the total amount of memory reported by the latest audit of the agent. This could come in helpful in ensuring a system meets the resource requirements of an application before an installation is attempted.

Operating systems supported: Windows, OS X, Linux

getRegistryValue() / get64BitRegistryValue() (page 103)

After entering the registry path, the value contained in the key is returned. A check can be made for existence, absence, equality, or size differences. For example, `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\AppPaths\AgentMon.exe\path` contains the directory path identifying where the agent is installed on the target machine. The test determines if the value stored for this key exists, thereby verifying the agent is installed.

The available tests are:

- `Exists` : true if the registry key exists in the hive.
- `Does Not Exist` : true if the registry key does *not* exist in the hive.
- `=` : true if value of the registry key equals the test value.
- `Not =` : true if value of the registry key does *not* equal the test value.
- `>` : true if value of the registry key is greater than the test value (value must be a number).
- `>=` : true if value of the registry key is greater than or equal to the test value (value must be a number).
- `<` : true if value of the registry key is less than the test value (value must be a number).
- `<=` : true if value of the registry key is less than or equal to the test value (value must be a number).
- `Contains` : true if the test value is a sub string of the registry key value (value must be a string).
- `Not Contains` : true if the test value is *not* a sub string of the registry key value (value must be a string).

Using the Backslash Character (\)

A backslash character `\` at the end of the key returns the default value of that key.

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\WORDPAD.EXE\` returns a default value, such as `%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE`

The *last single backslash* in a string is used to delimit the registry key from the registry value. To include backslashes as part of the value string, specify *double slashes* for each slash character. For example, the string `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey\Value\Name` is interpreted as the key `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey` with a value of `Value\Name`.

hasRegistryKey() / has64bitRegisterKey() (page 103)

Tests for the existence of a registry key. `hasRegistryKey()` differs from `getRegistryValue()` since it can check for a directory level registry entry that only contains more registry keys (no values).

isAppRunning()

Checks to see if a specified application is currently running on the managed machine. If the application is running, the **IF** command is executed; otherwise, the **ELSE** command is executed. When this option is selected from the drop-down list, the **Enter the application name** field appears. Specify the process name for the application you want to test. For example, to test the `Calculator` application, specify `calc.exe`, which is the process name that displays in the **Processes** tab of the Windows **Task Manager**.

isServiceRunning()

Determines if a service is running on the managed machine. Specify the *service name*.

- True if the service name is running.

Agent Procedures

- False if the service name is stopped or does not exist.

Note: Be sure to use the *service name* of the service, not the *display name* of the service. For example, the *display name* of the service for Microsoft SQL Server is SQL Server (MSSQLSERVER), but the *service name* of the service is MSSQLSERVER. For Windows machines, right click any service in the Services window and click the Properties option to see the *service name* of that service.

isUserActive()

Determines whether the user is either:

- Idle or not logged on, or
- Active

Operating systems supported: Windows, OS X, Linux

isUserLoggedin()

Tests to see if a specific user or any user is logged on the managed machine. Enter the machine user's logon name or leave the field blank to check for any user logged on. The **IF** commands are executed if a user is logged on. The **ELSE** steps are executed if the user is not logged on.

isYesFromUser()

Displays a dialog box on the managed machine with **Yes** and **No** buttons. Also carries out the **ELSE** command if a specified amount of time has timed out. If **Yes** is selected by the machine user, the **IF** command is executed. If the selection times out or the machine user selects **No**, the **ELSE** command is executed. This function requests the machine user's permission to proceed with the agent procedure. This query is useful for agent procedures that require a reboot of the managed machine before completion.

Procedure variables, for example #varName#, may be used inside **isYesFromUser()** fields to dynamically generate messages based on procedure data.

testFile()

Determines if a file exists on a managed machine. Enter the full path and file name. **testFile()** compares the full path and file name with the supplied value. If the check is true, **IF** commands are executed. If the check is false, **ELSE** steps are executed.

Note: Environment variables such as %windir%\notepad.exe are acceptable.

The available tests are:

- **Exists** : true if the full path and file name exists.
- **Does not Exist** : true if the full path and file name does *not* exist.
- **Contains** : true if the test value is a sub string of the file content.
- **Not Contains** : true if the test value is *not* a sub string of the file content.
- **Begins With** : true if the test value begins with the variable value.
- **Ends With** : true if the test value ends with the variable value.

testFileInDirectoryPath()

Tests the specified file located at the path returned using the **getDirectoryPathFromRegistry()** step. The available tests are:

- **Exists** : true if the file name exists.
- **Does not Exist** : true if the file name does *not* exist.
- **Contains** : true if the test value is a sub string of the file content.

- **Not Contains** : true if the test value is *not* a sub string of the file content.
- **Begins With** : true if the test value begins with the variable value.
- **Ends With** : true if the test value ends with the variable value.

true

Selecting **True** directs the **IF** commands to execute. Use **True** to directly execute a series of steps that do not require any decision points, such as determining whether a file exists using **testFile()**.

STEP Commands**alarmsSuspend()**

Suppresses alarms on a machine for a specified number of minutes. Updates the status of machines on the Monitor > Status > **Suspend Alarm** (page 229) page.

alarmsUnsuspendAll()

Stops the suppression of alarms on a machine. Updates the status of machines on the Monitor > Status > **Suspend Alarm** (page 229) page.

captureDesktopScreenshot()

Captures a desktop screenshot of the agent machine and uploads it to the Kaseya Server. The screenshot is saved as a PNG file with a unique name in a folder dedicated to that agent. You can access these files from the Audit > **Documents** (page 138) page or from **Live Connect** (page 344). End-user notification options must be selected based on the level of user notification desired, silently capturing a screenshot, notifying the user that the capture will take place, or asking to approve the capture. A custom message can be entered if end-user notification or permission requesting is selected. Otherwise a standard message displays.

Operating systems supported: Windows, OS X

changeDomainUserGroup()

Changes a domain user's membership in a domain user group. This **STEP** must be run on a domain controller. Enter the domain username of the member being added or removed from the domain user group. Then select whether to add or remove membership. Then select the domain user group.

Operating systems supported: Windows

changeLocalUserGroup()

Changes a local user's membership in a local user group. Enter the local username of the member being added or removed from the local user group. Then select whether to add or remove membership. Then select the group.

Operating systems supported: Windows

closeApplication()

If the specified application is running on the managed machine, then that application is closed down. Specify the process name for the application you want to close. For example, to close the Calculator application, specify `calc.exe`, which is the process name that displays in the **Processes** tab of the Windows **Task Manager**.

comment()

Adds a one line comment to the procedure.

copyFile()

Copies a file from one directory to another on the agent machine. If the target file exists, you must check a box to overwrite an existing file. Be sure to keep in mind folder syntax when running this **STEP** across different operating systems, for example, `c:\temp\tempfile.txt` for Windows and `/tmp/tempfile.txt` for OS X and Linux.

Operating systems supported: Windows, OS X, Linux

copyUseCredentials()

Copies a file from a directory on a machine and attempts to copy the file to a target directory and filename. The copy process uses either:

- The user credential specified for an agent using Agent > **Set Credentials** (page 68), or
- The user credential specified by an **impersonateUser()** step before this step.

This **STEP** is mostly used for accessing files across network UNC shares. If the target file exists, you must check a box to overwrite an existing file. Be sure to keep in mind folder syntax when running this **STEP** across different operating systems, for example, `c:\temp\tempfile.txt` for Windows and `/tmp/tempfile.txt` for OS X and Linux.

Operating systems supported: Windows, OS X, Linux

createDomainUser()

Adds a new user to an Active Directory domain when run on a domain controller. Enter a domain user name to create, then a password that meets the domain's complexity requirements for user accounts, then select the domain group the user will be added to, either `Domain Users` or `Domain Admins`.

Operating systems supported: Windows

createEventLogEntry()

Creates an event log entry in either the Application, Security or System event log types. You can create a Warning, Error or Informational event with your own description. The created event is hard-coded to use an Event ID of 607.

Operating systems supported: Windows

createLocalUser()

Adds a new local user account to a machine. Enter a local user name to create, then a password that meets local user account complexity requirements, then select the group the user will be added to.

Operating systems supported: Windows, OS X, Linux

createWindowsFileShare()

Creates a new file share on a Windows machine. You must type in the name of the file share as it will be accessed over the network, and enter the source folder on the agent for the file share. This folder will be created if it does not yet exist.

Operating systems supported: Windows

deleteDirectory()

Deletes a directory from an agent machine. Ensure you have your directory syntax correct for Windows vs. OS X/ Linux. To ensure all sub-directories and files are also removed, check the **Recursively delete subdirectories and files** checkbox.

Operating systems supported: Windows, OS X, Linux

deleteFile()

Deletes a file on a managed machine. Enter the full path and filename.

Note: Environment variables are acceptable if they are set on a user's machine. For example, using a path `%windir%\notepad.exe` would be similar to `C:\windows\notepad.exe`.

Note: You can delete a file that is currently in use using the `renameLockedFile()` command.

deleteFileInDirectoryPath()

Deletes the specified file located at the path returned using the `getDirectoryPathFromRegistry()` command.

deleteRegistryKey() / delete64BitRegistryKey() (page 103)

Deletes the specified registry key and all its sub-keys.

deleteRegistryValue() / delete64BitRegistryValue() (page 103)

Deletes the value stored at the specified registry key. The *last single backslash* in a string is used to delimit the registry key from the registry value. To include backslashes as part of the value string, specify *double slashes* for each slash character. For example, the string `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey\Va1ue\Name` is interpreted as the key `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey` with a value of `Va1ue\Name`.

deleteUser()

Deletes a user from the agent machine.

Operating systems supported: Windows, OS X, Linux

disableUser()

Disables a user, preventing logon to the agent machine.

Operating systems supported: Windows, OS X, Linux

disableWindowsService()

Disables a Windows service.

Operating systems supported: Windows

enableUser()

Enables a previously disabled user, allowing the user to logon to the OS.

Operating systems supported: Windows, OS X

executeFile()

Executes the specified file on the managed machine. This function replicates launching an application using the `Run...` command located in the Microsoft Windows `Start` menu. This function takes three parameters:

- Full path filename to the `.exe` file.
- Argument list to pass to the `.exe` file
- Option for the procedure to wait until the `.exe` completes or not.

Note: Environment variables are acceptable, if they are set on a user's machine. For example, using a path `%windir%\notepad.exe`, would be similar to `C:\windows\notepad.exe`.

If **Execute as the logged on user** is selected, then a credential must be specified by running either the `impersonateUser()` (page 96) or `useCredential()` (page 102) command before this command. If run **Execute as the system account** is selected, execution is restricted to the agent's system level access.

executeFileInDirectoryPath()

Same as **Execute File** except the location of the .exe file is located at the path returned from a **getDirectoryPathFromRegistry()** command.

If **Execute as the logged on user** is selected, then a credential must be specified by running either the **impersonateUser()** (page 96) or **useCredential()** (page 102) command before this command. If run **Execute as the system account** is selected, execution is restricted to the agent's system level access.

executePowershell()

Executes a powershell script, including:

- a Powershell .PS1 file
- a Powershell command with special arguments
- a combination of both

Operating systems supported: Windows XP SP3+/Server 2008 with Powershell add-on, Windows 7, Windows Server 2008

There are *five variants* of this command available.

- **executePowershell()** - Executes a powershell file, or command with arguments, or both. When running this command on either a 32bit or 64bit machine, no system credential or user credential is provided.
- **executePowerShell32BitSystem** - Executes a powershell file, or command with arguments, or both, as a *32 bit system* command.
- **executePowerShell32BitUser** - Executes a powershell file, or command with arguments, or both, as a *32 bit user* command.
- **executePowerShell64BitSystem** - Executes a powershell file, or command with arguments, or both, as a *64 bit system* command.
- **executePowerShell64BitUser** - Executes a powershell file, or command with arguments, or both, as a *64 bit user* command.

System and user commands:

- **System** - If a *system* command is run, execution is restricted to the agent's system level access.
- **User** - If a *user* command is selected, then a credential must be specified by running either the **impersonateUser()** (page 96) or **useCredential()** (page 102) command before this command.

executeProcedure()

Causes another named procedure to execute. Use this capability to string multiple **IF-ELSE-STEP** procedures together. If the procedure no longer exists on the Kaseya Server, an error message displays next to the procedure drop-down list. You can use this command to run a **system procedure** (page 564). You can nest procedures to 10 levels.

executeShellCommand()

Allows the procedure to pass commands to the command interpreter on the managed machine. When this command is selected, the field **Enter the command to execute in a command shell** is displayed. Enter a command in the field. The command must be syntactically correct and executable with the OS version on the managed machine. *Commands and parameters containing spaces should be surrounded by quotes*. Since the command is executed relative to the agent directory, absolute paths should be used when entering commands.

Note: **executeShellCommand()** opens a command prompt window on a managed Windows machine to execute in. If you do not want a window opening on a managed Windows machine, because it might confuse users, put all the commands in a batch file. Send that file to the managed Windows machine using the **writeFile()** command. Then run the batch file with the **executeFile()** command. **executeFile()** does not open a window on a managed Windows machine.

If **Execute as the logged on user** is selected, then a credential must be specified by running either the **impersonateUser()** (page 96) or **useCredential()** (page 102) command before this command. If run **Execute as the system account** is selected, execution is restricted to the agent's system level access.

executeShellCommandToVariable()

Executes a shell command and returns output created during and after its execution to a variable. The variable must be referred to in subsequent steps as `#global:cmdresults#`.

Operating systems supported: Windows, Linux, OS X

executeVBScript()

Runs a Vbscript, with or without command line arguments. If the Vbscript displays a popup window or notifies the end user, check the box for **Use Wscript instead of Cscript**.

Operating systems supported: Windows

getDirectoryPathFromRegistry()

Returns a file path stored in the specified registry key. Use this command to fetch the file location. For instance, use this command to find the directory where an application has been installed. The result can be used in subsequent steps by:

- **deleteFileInDirectoryPath()**
- **executeFileInDirectoryPath()**
- **getFileInDirectoryPath()**
- **renameLockedFileInDirectoryPath()**
- **testFileInDirectoryPath()** (an IF command)
- **writeFileInDirectoryPath()**

getFile()

Upload the file at the specified path from the managed machine. Be sure to enter a full path filename that you want to upload. Example: `news\info.txt`. Folders are created when the **getFile()** command is run, if they don't already exist. The file is stored on the Kaseya Server in a private directory for each managed machine. View or run the uploaded file using Agent Procedures > **Get File** (page 116).

- Optionally, existing copies of uploaded files are renamed with a `.bak` extension prior to the next upload of the file. This allows you to examine both the latest version of the file and the previous version.
- Optionally create a **Get File** alert if the uploaded file *differs* or is the *same* from the file that was uploaded previously. *You must create a Get File alert for a machine ID* using the Monitor > **Alerts - Get File** (page 255) page to enable the sending of an alert using the **getFile()** command. Once defined for a machine ID, the same **Get File** alert is *active for any agent procedure* that uses a **getFile()** command and is run on that machine ID. Turn off alerts for specific files in the agent procedure editor by selecting one of the without alerts options.

getFileInDirectoryPath()

Just like the **getFile()** command but it adds the path returned from the **getDirectoryPathFromRegistry()** command to the beginning of the remote file path. Access the uploaded file using the Agent Procedures > **getFile()** (page 116) function.

getURL()

Returns the text and HTML contents of a URL and stores it to a file on the managed machine. To demonstrate this to yourself, try specifying `www.kaseya.com` as the URL and `c:\temp\test.htm` as the file to store the contents of this URL. A copy of the web page is created on the managed machine that contains all of the text and HTML content of this webpage. You can search the contents of the file on the managed machine in a subsequent command.

Agent Procedures

Another use is to download an executable file that is available from a web server, so that you don't need to upload the file to the VSA server nor use the VSA's bandwidth to write the file down to each agent. You can use a subsequent command to run the downloaded executable on the managed machine.

Note: This command can download files from a LAN file source instead of the URL using [Agent > Configure Agents > LAN Cache](#) (page 69). Files have to be larger than 4k bytes.

getURLUsePatchFileSource()

Downloads a file from a given URL to a target folder and file for that agent. Uses the Patch Management > File Source settings.

Operating systems supported: Windows

getVariable()

Defines a new agent variable. When the procedure step executes, the system defines a new variable and assigns it a value based on data fetched from the managed machine's agent.

Note: See [Using Variables](#) (page 104) for the types of variable values supported by the `getVariable()` command.

getVariableRandomNumber()

Generates a random number which can then be accessed as the variable `#global:rand#` in a subsequent step.

Operating systems supported: Windows, OS X, Linux

getVariableUniversalCreate()

Gets a variable that persists outside of the immediate procedure's execution. This can be useful for passing a variable to another agent procedure using the [scheduleProcedure\(\)](#) step. You can create up to three variables. You can enter either string data or variables created in an earlier step. Variables created using this step can only be read using the [Get Variable – Universal – Read](#) step in any subsequent step.

Operating systems supported: Windows, OS X, Linux

getVariableUniversalRead()

Reads up to three variables you have previously created using the [Get Variable – Universal – Create](#) step. These variables must be referred to as `#global:universal1#`, `#global:universal2#`, and `#global:universal3#`. Please see the initial [Get Variable – Universal – Create](#) step for more detail.

Operating systems supported: Windows, OS X, Linux

giveCurrentUserAdminRights()

Adds the current user to the local administrator's group on the agent machine, either permanently or for a temporary period of time. This change does *not* take effect until the user logs off. It is recommended you leverage the [logoffCurrentUser\(\)](#) step.

Operating systems supported: Windows

impersonateUser()

Enter a username, password, and domain for the agent to logon with. This command is used in a procedure before an [executeFile\(\)](#), [executeFileInDirectoryPath\(\)](#) or [executeShellCommand\(\)](#) that specifies the [Execute as the logged on user](#) option. Leave the domain blank to log into an account on the local machine. Use [impersonateUser\(\)](#) to run an agent procedure using a credential specified *by agent procedure*. Use

[useCredential\(\)](#) to run an agent procedure using a credential specified *by managed machine*.

installAptGetPackage()

Silently installs a package using the `apt-get` command in Linux.

Operating systems supported: Linux

installDebPackage()

Silently installs a Debian package on any Linux OS that supports `.deb` packages.

Operating systems supported: Linux

installDMG()

Silently installs a `.DMG` package in OS X. If the package is formatted as an `Application`, it is copied to the `/Applications` folder. If the `.DMG` contains a `.PKG` installer within it, Kaseya attempts to install it.

Operating systems supported: OS X

installMSI()

Installs an MSI file for Windows. Options can be selected to either run a quiet installation or to avoid automatically restarting the computer after installation if it is requested.

Operating systems supported: Windows

installPKG()

Silently installs a `.PKG` package in OS X.

Operating systems supported: OS X

installRPM()

Silently installs an RPM package on any Linux OS that supports installing RPMs.

Operating systems supported: Linux

logoffCurrentUser()

Automatically logs off the current user. An optional warning that the log-off process is about to begin can be entered and displayed to the end-user.

Operating systems supported: Windows, OS X

pauseProcedure()

Pause the procedure for N seconds. Use this command to give Windows time to complete an asynchronous task, like starting or stopping a service.

reboot()

Unconditionally reboots the managed machine. To warn the user first, use the [isYesFromUser\(\)](#) command before this command. A [isYesFromUser\(\)](#) command prompts the user before rebooting their machine.

rebootWithWarning()

Reboots a machine, displaying a warning message to the end-user before the reboot process occurs.

Operating systems supported: Windows, OS X

removeWindowsFileShare()

Removes a file share from a Windows agent.

Agent Procedures

Operating systems supported: Windows

renameLockedFile()

Renames a file that is currently in use. The file is renamed the next time the system is rebooted. The specified filename is a complete file path name. Can be used to delete a file that is currently in use if the "new file name" is left blank. The file is deleted when the system is rebooted.

renameLockedFileInDirectoryPath()

Renames a file that is currently in use that is located in the path returned from a [getDirectoryPathFromRegistry\(\)](#) command. The file is renamed the next time the system is rebooted. Can be used to delete a file that is currently in use if the "new file name" is left blank. The file is deleted when the system is rebooted.

scheduleProcedure()

Schedules a procedure to run on a specified machine. Optionally specifies the time to wait after executing this step before running the procedure and the specified machine ID to run the procedure on. If no machine is specified, then the procedure is run on the same machine running the agent procedure. Enter the complete name of the machine, for example, `machine.unnamed.org`. *This command allows an agent procedure running on one machine to schedule the running of an agent procedure on a second machine.* You can use this command to run a [system](#) (page 564) procedure. You can nest procedures to 10 levels.

sendAlert()

This step command takes no parameters. Instead one or more [getVariable\(\)](#) (page 96) steps—*run prior to the sendAlert() step*—specify *alert action variables* that determine the actions triggered by the [sendAlert\(\)](#) step. All alert action variables are optional. If no alert action variables are defined, an alarm will be created with a system default message. An alert action variable can be used to disable the default alarm action. Alert action variables, if used, must use the specific names corresponding to their actions:

- `alertSubject` - Subject for alert message. A system default message is used if you do not define one in the agent procedure. See *System Parameters* below.
- `alertBody` - Body for alert message. A system default message is used if you do not define one in the agent procedure. See *System Parameters* below.
- `alertDisableAlarm` - When a default alarm enabled, enter any value to disable.
- `alertGenerateTicket` - Enter any value to generate.
- `alertScriptName` - Valid agent procedure name to execute on current machine.
- `alertEmailAddressList` - Comma-separated email addresses. Required to send email.
- `alertAdminNameList` - Comma-separated list of VSA user names. Required to send messages to the Info Center > [Inbox](#) (page 140).
- `alertNotificationBarList` - Comma-separated list of VSA user names. Required to send messages to the [Notification Bar](#) (page 10).
- `alertNotificationBarMasterAdmins` - Enter any value to send notifications to the [Notification Bar](#) for all [master users](#) (page 361).

System Parameters

You can override the default `alertSubject` and `alertBody` text sent by the [sendAlert\(\)](#) command. If you do you can embed the following *system parameters* in the `alertSubject` and `alertBody` variables you create using [getVariable\(\)](#) commands. *Double* angle brackets are required when embedding them in text. You do not create these embedded system parameters using a [getVariable\(\)](#) command. They are always available.

- `<<id>>` - Machine display name on which the agent procedure is being executed.

- `<<gr>>` - Machine group name on which the agent procedure is being executed.
- `<<at>>` - Alert date/time (server time).
- `<<ata>>` - Alert date/time (agent time).
- `<<apn>>` - Agent procedure name being executed.

Custom Parameters

You can embed *custom parameters* in `alertSubject` and `alertBody` `getVariable()` commands. First, create another variable using the `getVariable()` command. The value stored with this first variable can be dynamic, determined when the agent procedure is run. Second, insert the name of this first variable—surrounded by # and # brackets—into the text value specified by the `alertSubject` and `alertBody` `getVariable()` commands. Examples include:

- `#filename#`
- `#logentry#`
- `#registrykey#`
- `#registryvalue#`

Specifying `getVariable()` Commands before `sendAlert()` in an Agent Procedure

For example, assume an agent procedure:

1. Creates a variable called `runTimeVar` using the `getVariable()` command. The values entered are:
 - Constant Value
 - Procedure terminated. Could not access 'File Server 123'.
 - `runTimeVar`
 - All Operating Systems
 - Continue on Fail
2. Then a second `getVariable()` command is created in the same agent procedure. This second `getVariable()` command specifies the *body* of a `sendAlert()` message. This body message embeds both system and custom parameters. The values entered for this second `getVariable()` command are:
 - Constant Value
 - This alert was generated by `<<apn>>` on machine `<<id>>` at `<<ata>>`:
`#runTimeVar#`.
 - `alertBody`
 - All Operating Systems
 - Continue on Fail
3. Finally the `sendAlert()` command is run and the alert message is created.

Note: The sequence of parameter variables and alert action variables does not matter. *But all of them have to run before the `sendAlert()` command that makes use of them.*

`sendEmail()`

Sends an email to one or more recipients. Specifies the subject and body text of the email.

`sendMessage()`

Sends the entered message to a managed machine. An additional checkbox, if checked, sends the message immediately. If unchecked, sends the message after the user clicks the flashing agent system tray icon.

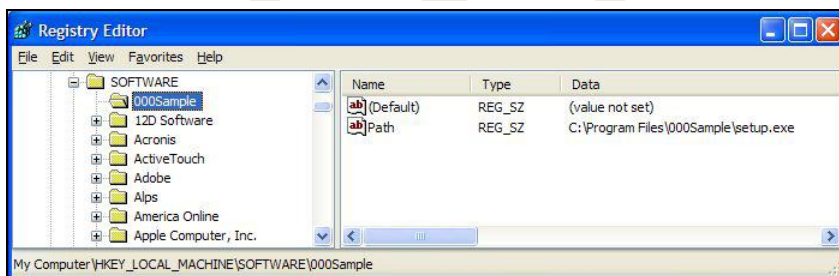
sendURL()

Displays the entered URL in a web browser window on the managed machine. An additional checkbox, if checked, displays the URL immediately. If unchecked, the URL is displayed after the user clicks the flashing agent system tray icon.

setRegistryValue() / set64BitRegistryValue() (page 103)

Writes data to the specified registry value. This function takes three parameters:

- **Enter the full path to a registry key containing a value**
 - Specify the (Default) value for a registry key by adding a trailing backslash \. Otherwise specify a name for an existing value or to create a new value. See the Name column in image below.
Example of setting the (Default) value: HKEY_LOCAL_MACHINE\SOFTWARE\000Sample\
 - The *last single backslash* in a string is used to delimit the registry key from the registry value. To include backslashes as part of the value string, specify *double slashes* for each slash character. For example, the string HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey\Value\\Name is interpreted as the key HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey with a value of Value\Name.
- **Enter the data to write to the registry value**
- **Select the data type**
 - REG_SZ - String value.
 - REG_BINARY - Binary data displayed in hexadecimal format.
 - DWORD - Binary data limited to 32 bits. Can be entered in hexadecimal or decimal format.
 - REG_EXPAND_SZ - An "expandable" string value holding a variable. Example: %SystemRoot%.
 - REG_MULTI_SZ - A multiple string array. Used for entering more than one value, each one separated by a \0 string. Use \\0 to include \0 within a string array value.



sqlRead()

Returns a value from the database and stores it to a named variable by running a selected SQL "read" statement. Global "read" statements are specified in the following location:

<KaseyaInstallationDirectory>\xml\Procedures\AgentProcSQL\0\SQLRead\<filename.xml>
> Filenames can be any name with an .xml extension so long as they are formatted correctly internally. Multiple statements specified using one or more XML files display as a single combined combo box list in the user interface. Each SQL statement in the XML file has a unique label, and only the labels are shown in the combo box. If no SQL statements are defined, then *No Approved SQL* displays in the combo box.

Partition-Specific Statements

Partition-specific folders can contain partition-specific SQL statements. For example:

<KaseyaInstallationDirectory>\xml\Procedures\AgentProcSQL\123456789\SQLRead\<filename.xml>. Users can select and run all 0 folder SQL "read" statements and all SQL "read" statements located in the partition path that matches the partition they are using.

Example Format

```
<?xml version="1.0" encoding="utf-8" ?>
<queryList>
  <queryDef label="Agent Machine Name" sql="SELECT machName FROM dbo.machNameTab WHERE agentGuid = #vMachine.agentGuid#" />
</queryList>
```

sqlWrite()

Updates the database—such as updating the value in a column or inserting a row—by running a selected SQL "write" statement. Global "write" statements are specified in the following location: `<KaseyaInstallationDirectory>\xml\Procedures\AgentProcSQL\0\SQLWrite\<filename.xml>` Filenames can be any name with an `.xml` extension so long as they are formatted correctly internally. Multiple statements specified using one or more XML files display as a single combined combo box list in the user interface. Each SQL statement in the XML file has a unique label, and only the labels are shown in the combo box. If no SQL statements are defined, then `*No Approved SQL*` displays in the combo box.

Partition-Specific Statements

Partition-specific folders can contain partition-specific SQL statements. For example: `<KaseyaInstallationDirectory>\xml\Procedures\AgentProcSQL\123456789\SQLWrite\<filename.xml>`. Users can select and run all `0` folder SQL "write" statements and all SQL "write" statements located in the partition path that matches the partition they are using.

Example Format

```
<?xml version="1.0" encoding="utf-8" ?>
<queryList>
  <queryDef label="Update Table" sql="UPDATE table1 SET column2 = value2 WHERE column1 = value1" />
</queryList>
```

startWindowsService()

Runs a Start command for a Windows service, if it exists.
Operating systems supported: Windows

stopWindowsService()

Runs a Stop command for a Windows service if it exists.
Operating systems supported: Windows

transferFile()

Transfers a file from the agent machine running this step to another agent machine. Enter the fully qualified machine ID of the *target machine*, for example, `mymachine.root.kaseya`. Then enter the full path and file name of the source file you wish to send *from the currently selected agent*. Then enter the full path and file name of the target file on the target machine.
Operating systems supported: Windows

uninstallbyProductGUID()

Silently uninstalls a product based on its MSI GUID.
Operating systems supported: Windows

unzipFile()

Extracts the contents of a specified zip file to a target folder, with an option to automatically overwrite any previously existing target files or folders.
Operating systems supported: Windows, OS X, Linux

updateSystemInfo()

Updates the selected **System Info** field with the specified value for the machine ID this procedure runs on. The **System Info** fields you can update include all columns in **vSystemInfo** (page 462) except **agentGuid**, **emailAddr**, **Machine_GroupID**, **machName**, and **groupName**. **vSystemInfo** column information is used by Audit > **System Info** (page 134), Agent > **System Status** (page 28), the **Filter Aggregate Table** (page 27) in **View Definitions**, and the **Aggregate Table** (page 179) report. You can update a **System Info** field using any string value, including the value of any previously defined agent procedure variable.

useCredential()

Uses the credentials set for the machine ID in **Set Credential** (page 68). This command is used in a procedure before an **executeFile()**, **executeFileInDirectoryPath()** or **executeShellCommand()** that specifies the **Execute as the logged on user** option. Also used to access a network resource requiring a credential from a machine when a user is not logged on. Use **impersonateUser()** to run an agent procedure using a credential specified *by agent procedure*. Use **useCredential()** to run an agent procedure using a credential specified *by managed machine*.

Note: A procedure execution error is logged if a **Set Credential** procedure command encounters an empty username.

Note: Patch Management > Patch Alert can alert you—or run an agent procedure—if a machine ID's credential is missing or invalid.

windowsServiceRecoverySettings()

Sets the Service Recovery Settings for any given service in Windows. Specify the name of the service you wish to modify, then set both the first and second restart failure options and any subsequent restart failure options.

Operating systems supported: Windows

writeDirectory()

Writes a selected directory, including subdirectories and files, from **Manage Files Stored on Server** (page 108) to the full path directory name specified on the managed machine.

writeFile()

Writes a file selected from **Manage Files Stored on Server** (page 108) to the full path filename specified on the managed machine. Enter a new filename if you want the file to be renamed.

Each time a procedure executes the **writeFile()** command, the agent checks to see if the file is already there or not by hashing the file to verify integrity. If not, the file is written. If the file is already there, the procedure moves to the next step. You can repeatedly run a procedure with **writeFile()** that sends a large file to a managed machine and know that the VSA only downloads that file once.

Note: Environment variables are acceptable if they are set on a user's machine. For example, using the path `%windir%\notepad.exe` would be equivalent to `C:\windows\notepad.exe`.

Note: This command can download files from a LAN file source instead of the VSA using Agent > Configure Agents > **LAN Cache** (page 69). Files have to be larger than 4k bytes.

writeFileFromAgent()

Transfers a file from another agent machine to the agent machine running this step. Transfers a file between agents. Similar to the previous **transferFile()** step, though in this case you enter the fully qualified machine ID of the *source machine* that has the file you wish to send *to the currently selected*

agent. First enter the full path and file name of the file you wish to send from the source machine. You then enter the full path and the file name to be created on the target machine.

Operating systems supported: Windows

writeFileInDirectoryPath()

Writes the specified filename to the path returned from a [getDirectoryPathFromRegistry\(\)](#) command.

writeProcedureLogEntry()

Writes the supplied string to the Agent Procedure Log for the machine ID executing this agent procedure.

writeTextToFile()

Writes text to a file on the agent machine, either by appending text to an existing file or by creating a new file if none exists. You enter the text to write to the file, then enter the full path and file name on the agent machine the text will be written to. You can optionally overwrite the entire file with the text you have entered if the file already exists.

Operating systems supported: Windows, OS X, Linux

zipDirectory()

Compresses a directory and any subdirectories or files it contains into a zip file on the agent machine. Enter the full path to be compressed, which can contain wildcards. Then enter the full path and file name of the zip file to be created or updated. If the target zip file already exists, optionally check a box to overwrite it.

Operating systems supported: Windows, OS X, Linux

zipFiles()

Compresses a single file or files into a zip file on the agent machine. Enter the full path of the file or files to be compressed. Then enter the full path and filename of the zip file to be created or updated. If the target zip already exists, optionally check a box to overwrite it.

Operating systems supported: Windows, OS X, Linux

64-Bit Commands

Accessing 64-bit Registry Values

Five 64-bit registry commands and one 64-bit parameter are available in agent procedures. 64-bit Windows isolates registry usage by 32-bit applications by providing a separate logical view of the registry. The redirection to the separate logical view is enabled automatically and is transparent for the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE
- HKEY_USERS*\SOFTWARE\Classes
- HKEY_USERS*_Classes

Since the Kaseya agent is a 32-bit application, you must use the following commands and parameter to access the registry data that are stored in the above keys by the 64-bit applications.

IF Commands

- get64BitRegistryValue()
- has64bitRegistryKey()

Agent Procedures

STEP Commands

- delete64BitRegistryValue()
- delete64BitRegistryKey()
- set64BitRegistryValue()
- 64-bit Registry Value parameter in the getVariable() command

Specifying 64-bit Paths in File Commands

The following commands...

- deleteFile()
- writeFile()
- executeFile()
- renameLockedFile()
- getFile()
- get-variable() File Content parameter

... can specify 64-bit directories using the following variables:

Use This Environment Variable	To Target This Directory
%windir%\sysnative	<drive>:\Windows\System32
%ProgramW6432%	<drive>:\Program Files
%CommonProgramW6432%	<drive>:\Program Files\Common Files

For compatibility reasons, Microsoft has placed 64-bit system files in the \Windows\system32 directory and 32-bit system files in the \Windows\SysWOW64 directory. Similarly, 64-bit application files are installed to the \Program Files and 32-bit application files are installed to the \Program Files (x86) folder. Since the Kaseya agent is a 32-bit application, when a file path containing \Windows\system32 or \Program Files is specified on a 64-bit machine, the file access is automatically redirected to the \Windows\SysWOW64 or \Program Files (x86) folders. To access files in \Windows\system32 and \Program Files folders, use these environment variables when specifying parameters for these file commands.

In Directory Path Commands

The getDirectoryPathFromRegistry() command—and any subsequent ...In Directory Path command—cannot be used to access files in the \Program Files and \Windows\System32 directories on a target 64-bit machine. These commands can still access 32-bit or 64-bit files in any other folder.

Identifying 64-bit Machines

64-bit machine IDs typically display a x64 in the Version column of audit pages.

Using Variables

Use variables to store values that can be referenced in multiple procedure steps. Variables are passed automatically to nested procedures.

- **Three Methods for Creating Variables:**
 - **Procedure Variables** - Use the getVariable() command within a procedure to create a new variable name without any special characters. Example: VariableName. In subsequent steps, including steps in nested procedures, reference the variable by bracketing the variable name with the # character. Example: #VariableName#.

Note: Procedures variables cannot be referenced outside of the procedure or nested procedures that use them except for GLOBAL variables. A procedure variable is only visible to the section of the procedure it was created in and any child procedures. Once a procedure leaves the THEN clause or ELSE clause the variable was created in, the variable is out of scope and no longer valid. Use GLOBAL Variables, described below, to maintain visibility of a variable after leaving the THEN clause or ELSE clause the variable was created in.

- **Managed Variables** - Use the **Variable Manager** (page 107) to define variables that can be used repeatedly in different procedures. You can maintain multiple values for each managed variable, with each value applied to one or more group IDs. Managed variables cannot be re-assigned new values within a procedure. Within a procedure, reference a managed variable by bracketing the variable name with the < and > character. Example: <VariableName>.
- **GLOBAL Variables** - Non-GLOBAL variables cannot return a changed value of a procedure variable defined by its parent procedure. Non-GLOBAL variables initialized in the child procedure also cannot be passed back to the parent. Variables named with the prefix GLOBAL: (case-insensitive followed by a colon) can pass changed values from the child to the parent, whether the variable is initialized in the parent or the child procedure. Subsequent child procedures can make use of any GLOBAL variable initialized in any earlier step, regardless of whether that global variable is initialized in a parent procedure or another child procedure.
- **Variable Names** - Variable names cannot include the following characters: ; % ' " / \ : * ? < > | and the space character.
- **Where Used** - Once variables are created you can include them, in their bracketed format, in any text entry field displayed by an IF-ELSE-STEP dialog box.
- **Case Sensitivity** - Variable names are case sensitive.
- **Reserved Characters** - Because the <, > and # characters are used to identify variable names, these characters must be entered twice as regular text in a command line. For example the following command c:\dir >> filelist.txt is interpreted at procedure runtime as c:\dir > filelist.txt.
- **Types of Variable Values Possible** - The following are the types of variable values typically obtained by using the **getVariable()** parameter.
 - **Registry Value** and **64-Bit Registry Value** - See **64-Bit Commands** (page 103) - Data from the specified registry value on the managed machine. The last single backslash in a string is used to delimit the registry key from the registry value. To include backslashes as part of the value string, specify double slashes for each slash character. For example, the string HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey\Value\Name is interpreted as the key HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey with a value of Value\Name.
 - **File Content** - Data from a specified file on the managed machine. See **64-Bit Commands** (page 103).
 - **Constant Value** - Specified constant as typed in the procedure editor.
 - **Agent Install Directory Path** - Directory in which the agent is installed on the managed machine.
 - **Agent Install Drive** - Drive in which the agent is installed on the managed machine, such as c:\.
 - **Agent Working Directory Path** - Working directory on the managed machine as specified using Agent > Working Directory (page 64).

Warning: Do not delete files and folders in the working directory. The agent uses the data stored in the working directory to perform various tasks.

- **User Temporary Directory Path** - The temporary directory for the user currently logged on the managed machine. This path is the expansion of the %TEMP% environment variable for the

currently logged on user. If no user is logged on, it is the default Windows temporary directory.

- **Machine.Group ID** - Machine ID of the agent executing the procedure.
- **File Version Number** - The software version number of the specified file on the managed machine. For example, an `exe` or `dll` file often contain the version number of their release.
- **File Size** - Size in bytes of the specified file on the managed machine.
- **File Last Modified Date** - The last modified date and time in universal time, coordinated (UTC) of the specified file on the managed machine in the format of `yyyy/mm/dd hh:mm:ss`.
- **Automatic SQL View Data Variables** - SQL view parameters are available as automatically declared procedure variables. Automatic variables enable you to skip using the `GetVariable` command before making use of the variable in a step. Use the format `#SqlViewName.ColumnName#` in a procedure to return the value of a `dbo.SqlView.Column` for the agent running the agent procedure. See [System > Database Views](#) (page 419) for a list of the SQL views and columns that are available.

Note: SQL View Data - This older method of returning a database view value is only necessary if you are trying to return a value from a *different machine than the machine running the agent procedure*.

Use the `GetVariable` command with the `SQL View Data` option to create a new procedure variable and set it to the value of a `dbo.SqlView.Column` value. Use the format `SqlViewName/ColumnName/mach.groupID` or `SqlViewName/ColumnName`. If the optional machine ID is omitted, then the value for the agent executing the procedure is retrieved. If `ColumnName` contains a space, surround it with square brackets. Example: `vSystemInfo/[Product Name]`. See [System > Database Views](#) (page 419) for a list of the SQL views and columns that are available.

- **Automatic Administrator Variables** - Three administrator variables are declared automatically. These automatic administrator variables allow agent procedures to access values not present from an SQL view.
 - ✓ `#adminDefaults.adminEmail#` - Email address of the VSA user who scheduled the agent procedure.
 - ✓ `#adminDefaults.adminName#` - Name of the VSA user who scheduled the agent procedure.
 - ✓ `#scriptIdTab.scriptName#` - Name of the agent procedure.
- **WMI Property** - A WMI namespace, class, and property. The format of the specified WMI property is `NameSpace:Class.Property`. For example, `root\cimv2:Win32_OperatingSystem.FreePhysicalMemory`. Specify an instance using the following syntax: `NameSpace:Class[N].Property` where `[N]` is the instance number. For example, `root\cimv2:Win32_OnboardDevice[3].Description`. The first instance may be specified with or without specifying the `[1]` instance number.
- **Expression Value** - Specify an expression that consists of procedure variables and six mathematical operators `+`, `-`, `*`, `/`, `(`, and `)` that are evaluated and assigned to a new procedure variable. For example, `((#variable1# + #variable2#) + 17.4) / (#variable3# * 4)`. The procedure variables must contain numeric values.
- **Prompt when procedure is scheduled** - Displays a message prompt to enter a value when an agent procedure is run. The value is stored in the variable name you specify. Specify the prompt text and variable name. For example, each time this procedure is run, a VSA user could enter a different machine directory.
- **Alert Variables** - An agent procedure can be assigned to run when an alert is triggered. In most cases the alert passes predefined variables to the agent procedure. These alert variables are documented by alert topic. See [Alerts - New Agent Installed](#) (page 266) for an example.

- **Windows Environment Variables** - You can reference Windows environmental variables within the `executeFile()`, `Execute File in Path` and `executeShellCommand()` only. Enclose the whole command in quotes, because the environmental variable may contain spaces which might affect execution. For other agent procedure commands, use `getVariable()` to get the registry key containing the environmental variables, located under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment`.

Variable Manager

Use the **Variable Manager** to define variables that can be used repeatedly in different agent procedures. You can maintain multiple values for each managed variable, with each value applied to one or more group IDs. Managed variables cannot be re-assigned new values within a procedure. Within a procedure, reference a managed variable by bracketing the variable name with the `<` and `>` character. Example: `<VariableName>`. See **Using Variables** (page 104).


Using managed variables, managed machines can run agent procedures that access *locally available resources* based on the group ID or subgroup ID.

Note: Using `System > Naming Policy` (page 358), this benefit can be applied automatically by IP address even to a highly mobile workforce that travels routinely between different enterprise locations.

Select Variable

Select a variable name from the drop-down list or select `<New Variable>` to create a new variable. Variable *names* are **case sensitive** and cannot include the following characters: `, % ' " / \ : * ? < > |` and the space character.

Rename/Create Variable

Enter a new name for the new variable you are creating or for an existing variable you are renaming. Select the delete icon  to delete the entire variable from all groups.

Public

Selecting the **Public** radio button allows the variable to be used by all users. However, only master role users can create and edit shared variables.

Private

Selecting the **Private** radio button allows the variable to be used only by the user who created it.

Apply

Enter the initial value for a variable. Then select one or more **Group IDs** and click **Apply**. Empty values are not allowed.

Remove

Select one or more group IDs, then click **Delete** to remove the value for this variable from the group IDs it is assigned to.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Group ID

Displays all group IDs the logged in user is authorized to administer.

Value

Lists the value of the variable applied to the group ID.

Manage Files Stored on Server

Agent Procedures > Manage Procedures > Schedule / Create > Manage Files

Use the **Manage Files Stored on Server** popup window to upload a file and store it on the Kaseya Server. You can also list, display and delete files already stored on the Kaseya Server. Agent procedures can distribute these files to managed machines using the **writeFile()** or **writeFileInDirectoryPath()** commands.


Note: This store of files is not machine-specific. **getFile()** (page 116) uploads and stores machine-specific files on the server.

To upload a file:

- Click **Private files** or **Shared files** to select the folder used to store uploaded files. Files stored in the **Private files** folder are not visible to other users.
- Click **Browse...** to locate files to upload. Then click **Upload** to upload the file to the Kaseya Server.

Note: You can modify the maximum file size allowed for uploads.

To delete a file stored on the Kaseya Server:

- Click **Private files** or **Shared files** to select the folder used to store uploaded files.
- Click the delete icon  next to a file name to remove the file from the Kaseya Server.

Note: An alternate method of uploading files is to copy them directly to the managed files directory on the IIS server. This directory is normally located in the `C:\Kaseya\WebPages\ManagedFiles` directory. In that directory are several sub-directories. Put private files into the directory named for that user. Put shared files into the `VSASharedFiles` directory. Any files located in this directory will automatically update what is available in the **Manage Files Stored on Server** user interface at the next user logon.

Folder Rights

Private Folders

Objects you create—such as reports, procedures, or monitor sets—are initially saved in a folder with your user name underneath a **Private** cabinet. This means only you, the creator of the objects in that folder, can view those objects, edit them, run them, delete them or rename them.

To share a private object with others you first have to drag and drop it into a folder underneath the **Shared** cabinet.

Note: A master role user can check the **Show shared and private folder contents from all users** checkbox in **System > Preferences** (page 353) to see all shared and private folders. For Private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

Shared Folders

The following **Share Folder** guidelines apply to folders underneath a **Shared** cabinet:

- All child folders inherit rights from their parent folder unless the child's folders are explicitly set.
- If you have rights to delete a folder, deleting that folder deletes all objects and subfolders as well, regardless of share rights assigned to those subfolders.

Note: Scopes have nothing to do with the visibility of folders and objects in a folder tree. Scopes limit what your folder objects can work with. For example, you can be shared folders containing reports, procedures or monitor sets but you will only be able to use these objects on machine groups within your scope.

- To set share rights to a folder, select the folder, then click the **Share Folder** button to display the **Share Folder** dialog.
 - You can share specific rights to a folder with any individual user or user role you have visibility of. You have visibility of:
 - ✓ Any user roles you are a member of, whether you are currently using that user role or not.
 - ✓ Any individual users that are members of your current scope.
 - Adding a user or user role to the **Shared Pane** allows that user to run any object in that folder. No additional rights have to be assigned to the user or user role to run the object.
 - Checking any *additional rights*—such as **Edit**, **Create**, **Delete**, **Rename**, or **Share**—when you add the user or user role provides that user or user role with those additional rights. You have to remove the user or user role and re-add them to make changes to their additional rights.
 - **Share** means the user or user role can assign share rights for a selected folder using the same **Share Folder** dialog box you used to assign them share rights.

Distribution

Agent Procedures > Manage Procedures > Distribution

The **Distribution** page spreads network traffic and server loading by executing agent procedures evenly throughout the day or a specific block of time in a day. Applies to agent procedures currently scheduled to run on a **recurring basis** only.

Note: Recurring procedures listed here include function-specific procedures *that are not visible as agent procedures in the Schedule / Create (page 80) folder tree*, such as procedures created using a **Patch Management wizard**.

Procedures can cause excessive network loading by pushing large files between the Kaseya Server and agent. Performing these operations with hundreds of agents simultaneously may cause unacceptable network loading levels.

Procedure Histograms

The system plots a histogram for each procedure currently scheduled to run on a recurring basis. Setting the histogram period to match the recurring interval of the procedure counts how many machines execute the procedure in a specific time interval. Peaks in the histogram visually highlight areas where a lot of machines are trying to execute the procedure at the same time. *Click a peak to display a popup window listing all machine IDs contributing to that peak load.* Use the controls, described below, to reschedule the procedure such that the network loading is spread evenly over time. **Only machine IDs currently matching the Machine ID / Group ID filter are counted in the histogram.**

Reschedule selected procedure evenly through the histogram period

Pick this radio control to reschedule selected procedures running on all machines IDs currently matching the **Machine ID / Group ID filter** (page 23). Procedure execution start times are staggered evenly across the entire histogram period.

Agent Procedures

Reschedule selected procedure evenly between <start time> and <end time>

Pick this radio control to reschedule selected procedures running on all machine IDs currently matching the Machine ID / Group ID filter. Procedure execution start times are staggered evenly, beginning with the start time and ending with the end time.

Run recurring every <N> <periods>

This task is always performed as a recurring task. Enter the number of times to run this task each time period.

Skip if Machine Offline

Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Distribute

Click the **Distribute** button to schedule selected procedures, using the schedule parameters you've defined.

Note: The procedure recurring interval is replaced with the histogram period.

Select Histogram Period

Selects the schedule time period to display histograms.

Histogram Plots

Each recurring procedure displays a histogram of all the machine IDs that are scheduled to run that procedure within the selected histogram period. Only machine IDs currently matching the Machine ID / Group ID filter are counted in the histogram.

Above the histogram is a:

- **Procedure name** - name of the procedure. Check the box next to the procedure name to select this procedure for distribution.
- **Peak** - the greatest number of machines executing the procedure at the same time.
- **Total** - total number of machines executing the procedure.

Agent Procedure Status





Agent Procedures > Manage Procedures > Agent Procedure Status





- Similar information is displayed in the Pending Procedures tab of the [Live Connect](#) (page 344) and [Machine Summary](#) (page 131) pages.

The **Agent Procedure Status** page displays the status of agent procedures for a selected machine ID. The list of machine IDs you can select is based on the **Machine ID / Group ID filter** (page 23). Users can, at a glance, find out what time a agent procedure was executed and whether it was successfully executed. See Agent Procedures > **Schedule / Create** (page 80) for more information about agent procedures.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes

-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Procedure Name

The name of the agent procedure.

Time

The date and time the agent procedure was last executed.

Status

Displays the results of the executed agent procedure. Overdue date/time stamps display as **red text with yellow highlight**. Recurring agent procedures display as **red text**.

Admin

Displays the VSA user who scheduled the agent procedure.

Pending Approvals

Agent Procedures > Manage Procedures > Pending Approvals

- This page only displays for **master role users** (page 564).

The **Pending Approvals** page approves *signed* agent procedures, enabling them to be run using the **Schedule / Create** (page 80) page, or selected and run elsewhere throughout the VSA.

Signed Agent Procedures

A **signed** agent procedure helps detect unauthorized changes to an agent procedure. *Unsigned* agent procedures cannot be run anywhere in the VSA.

- An agent procedure is digitally *signed* when it is saved by *any user* using the agent procedure editor.
- *Signed* agent procedures created by **standard users** (page 361) require **approval** using the **Pending Approvals** page.
- Only *users* who are using a *role* that provides access rights to the **Pending Approvals** page can manually *approve* pending, signed agent procedures.
- Agent procedures imported by standard users are *signed* but not yet *approved*.

Automatically Signed and Approved Agent Procedures

Agent procedures are automatically signed and approved when they are:

- Created by master role users.
- Imported by master role users.
- In the database when the VSA is upgraded to 7.0.

Actions

- **Approve Procedure** - Approves selected *signed* agent procedures.
- **Refresh** - Refreshes the page.

Table Columns

- **Script Name** - The name of the agent procedure.
- **Modified By** - The user who last edited the agent procedure.
- **Date Modified** - The date/time the agent procedure was last modified.
- **Location** - The location of the agent procedure in the agent procedure folder tree.

Patch Deploy

Agent Procedures > Installer Wizards > Patch Deploy

The **Patch Deploy** wizard is a tool that creates an agent procedure to distribute and apply Microsoft patches. The wizard walks you through a step by step process resulting in an agent procedure you can schedule, to deploy a patch to any managed machine.

Microsoft releases many hot fixes as patches for very specific issues that are not included in the Microsoft Update Catalog or in the Office Detection Tool, the two patch data sources the **Patch Management** module uses to manage patch updates. **Patch Deploy** enables customers to create a patch installation procedure for these hot fixes, via this wizard, that can be used to schedule the installation on any desired machine.

See Methods of Updating Patches, Configuring Patch Management, Patch Processing, Superseded Patches, Update Classification and Patch Failure for a general description of patch management.

Step 1: Enter 6-digit knowledge base article number.

Microsoft publishes a vast assortment of information about its operating system in the **Microsoft Knowledge Base**. Each article in the Knowledge Base is identified with a 6-digit Q number (e.g. Q324096.) All Microsoft patches have an associated knowledge base article number.

Note: Entering the article number is optional. Leave it blank if you do not know it.

Step 2: Select the operating system type.

Sometimes patches are specific to a certain operating system. If the patch you are trying to deploy applies to a specific OS only, then select the appropriate operating system from the drop-down control. When the wizard creates the patch deploy procedure, it restricts execution of the procedure to only those machines with the selected OS. This prevents inadvertent application of operating system patches to the wrong OS.

Step 3: Download the patch.

This step is just a reminder to fetch the patch from Microsoft. Typically there is a link to the patch on the knowledge base article describing the patch.

Step 4: How do you want to deploy the patch?

The Patch Deploy wizard asks you in step 4 if you want to **Send the patch from the KServer to the remote machine and execute it locally** or **Execute the patch from a file share on the same LAN as the remote machine**. Pushing the patch down to each machine from the VSA may be bandwidth intensive. If you are patching multiple machines on a LAN no internet bandwidth is used to push out the patch. Each machine on the LAN can execute the patch file directly from a common file share.

Step 5: Select the patch file or Specify the UNC path to the patch stored on the same LAN as the remote machine.

If **Send the patch from the KServer to the remote machine and execute it locally** was selected, then the patch must be on the VSA server. Select the file from the drop-down list.

Note: If the patch file does not appear in the list then it is not on the Kaseya Server. Click the [Back](#) button and upload the file to the Kaseya Server by clicking the first [here](#) link.

If **Execute the patch from a file share on the same LAN as the remote machine** was selected, then the patch must be on the remote file share prior to running the patch deploy procedure. The specified path to the file must be in **UNC format** such as `\\computername\dir\`.

Note: If the file is not already on the remote file share, you can put it there via FTP. Click the [Back](#) button and then the second [here](#) link takes you to FTP.

Step 6: Specify the command line parameters needed to execute this patch silently.

To deploy a patch silently you need to add the appropriate command line switches used when executing the patch. Each knowledge base article lists the parameters for **silent install** (page 562). Typical switch settings are `/q /m /z`.

Note: Command line parameters are optional. Leave it blank if you do not know it.

Step 7: Name the procedure.

Enter a name for the new agent procedure you can run to deploy the patch.

Step 8: Reboot the machine after applying the patch.

Check this box to automatically reboot the managed machine after applying the patch. The default setting is to *not* reboot.

Click the Create button.

A new agent procedure is created. Use Agent Procedure > [Schedule / Create](#) (page 80) to display the new agent procedure in the folder tree, under your private folder user name. You can run this new agent procedure to deploy the patch to any managed machine.

Application Deploy

Agent Procedures > Installer Wizards > Application Deploy

The **Application Deploy** page is a wizard tool that creates an agent procedure to distribute vendor installation packages, typically `setup.exe`. The wizard walks you through a step by step process resulting in an agent procedure you can schedule, to deploy an application to any managed machine.

Deploying Software Vendor's Install Packages

Most vendors provide either a single file when downloaded from the web or set of files when distributed on a CD. Executing the installer file, typically named `setup.exe` or `abc.msi`, installs the vendor's application on any operating system.

The **Application Deploy** wizard takes you through an interview process to determine the type of installer and automatically generates a procedure to deploy install vendor packages.

The VSA provides a small utility to automatically identify all supported installer types. Download and run `kInstId.exe` to automatically identify the installer type.

Note: See [Creating Silent Installs](#) (page 115) to ensure vendor installation packages don't pause for user input during installation.

Step 1: How do you want to deploy the application?

The wizard generated procedure tells the managed machine where to get the application installation file to execute. The **Application Deploy** wizard asks you in step 1 if you want to **Send the installer from the VSA server to the remote machine and execute it locally** or **Execute the installer from a file share on the same LAN as the remote machine**.

Pushing the application installation file to each machine from the VSA may be bandwidth intensive. If you are installing to multiple machines on a LAN no internet bandwidth is used to push out the application installation file. Each machine on the LAN can execute the application installation file directly from a common file share.

Step 2: Select the application install file or Specify the UNC path to the installer stored on the same LAN as the remote machine.

If **Send the installer from the VSA server to the remote machine and execute it locally** was selected, then the installer file must be on the VSA server. Select the file from the drop-down list.

Note: If the installer file does not appear in the list then it is not on the VSA server. Click the [here](#) link to upload the file to the server.

If **Execute the installer from a file share on the same LAN as the remote machine** was selected, then the installer file must be on the remote file share prior to running the application deploy procedure. The specified path to the file must be in **UNC format** such as `\\computername\dir\`. When specifying a UNC path to a share accessed by an agent machine—for example `\\machinename\share`—ensure the share's permissions allow read/write access using the credential specified for that agent machine in Agent > **Set Credential** (page 68).

Note: If the file is not already on the remote file share, you can put it there via FTP. Click the [here](#) link to start FTP.

Step 3: What kind of installer is this?

The wizard need to know what kind of installer was used by your software vendor to create the install package. The VSA provides a small utility to automatically identify all supported installer types. Download and run `kInstId.exe` to automatically identify the installer type. Supported installer types are:

- Windows Installer (MSI files)
- Wise Installer
- Installshield - Package For The Web
- Installshield - Multiple Files
- Other

Step 4: Name the agent procedure.

Enter a name for the new agent procedure you can run to install the application.

Step 5: Reboot the machine after installing the application.

Check this box to automatically reboot the managed machine after running the install. The default setting is to *not* reboot.

Click the Create button.

A new agent procedure is created. Use Agent Procedure > **Schedule / Create** (page 80) to display the new agent procedure in the folder tree, under your private folder user name. You can run this new agent procedure to install the application to any managed machine.

Creating Silent Installs

Most vendors provide either a single file, when downloaded from the web, or set of files, when distributed on a CD. Executing the installer file, typically named `setup.exe`, installs the vendor's application on any operating system. Vendors typically use one of three applications to create install packages: **InstallShield**, **Windows Installer**, or **Wise Installer**. Each of these applications provides a method for creating **silent installs** (page 562). When automating the installation of vendor install packages, you'll want to ensure the installation package does not pause for user input during installation.

Silent Installs with InstallShield

InstallShield has a record mode that captures answers to all dialog boxes in the installation procedure. InstallShield requires the recorded response `iis` file to be on the managed machine during the installation. To deploy, the agent procedure must use the `writeFile()` command to send both the `setup.exe` and `record.iis` files from VSA server to the managed machine and then use `executeFile()` (page 93) to run `setup.exe` with the options `/s /f"<path>\record.iis"`. Refer to your InstallShield help guide for more information regarding the silent installation capability with a recorded response file.

Create a custom install package by following these steps:

1. Verify the install package was made with InstallShield.
 - a. Launch the install package.
 - b. Confirm **InstallShield Wizard** displays at the end of the window title bar.
2. Launch the install package in record mode from a command prompt.
 - a. **If the install package is a single file** - Run `setup.exe /a /r /f1c:\temp\record.iss`. `Setup.exe` is the name of the install package. `c:\temp\record.iss` is the full path filename to save the recorded output.
 - b. **If the Install package is a set of files** - Run `setup.exe /r /f1c:\temp\record.iss`. `Setup.exe` is the name of the install package. `c:\temp\record.iss` is the full path filename to save the recorded output.
3. Deploy the install package with the recorded dialog box responses. Use the `writeFile()` agent procedure command to copy both the vendor's install package and `record.iss` file to each managed machine or to a file server accessible by each managed machine.
4. Execute the install package with silent mode command line parameters using the `executeFile()` procedure command.
 - a. **If the install package is a single file** - Run `setup.exe /s /a /s /f1c:\temp\record.iss`. `Setup.exe` is the name of the install package. `c:\temp\record.iss` is the full path filename location of the recorded settings.
 - b. **If the Install package is a set of files** - Run `setup.exe /s /f1c:\temp\record.iss`. `Setup.exe` is the name of the install package. `c:\temp\record.iss` is the full path filename location of the recorded settings.

Silent Installs with Windows Installer

Windows Installer does not have a record mode. As such it can only silently install the **Typical** install configuration. To silently install a Windows Installer package write a procedure to perform the following:

1. Use the `writeFile()` agent procedure command to copy the vendor's install package to each managed machine or to a file server accessible by each managed machine.
2. Run the install package with the `/q` parameter using the `executeFile()` agent procedure command.

Silent Installs with Wise Installer

Wise Installer does not have a record mode. As such it can only silently install the **Typical** install configuration. To silently install a Wise Installer package write a procedure to perform the following:

1. Use the [writeFile\(\)](#) agent procedure command to copy the vendor's install package to each managed machine or to a file server accessible by each managed machine.
2. Run the install package with the `/s` parameter using the [executeFile\(\)](#) agent procedure command.

Packager

Agent Procedures > Custom Installer > Packager

The **Packager** is a wizard tool used to create a package when a pre-defined install solution cannot be used. **Packager** evaluates the state of a source machine before and after an installation and/or resource change. The **Packager** compiles the differences into a single executable file—the **package**—that can be distributed via agent procedures to any managed machine. Distribute a package any way you choose. You can email it, or store it on a server where a [custom procedure](#) (*page 80*) can perform a silent installation on any managed machine.

Step 1: Download the Packager application to the machine you plan to build your install package on.

For best results, we recommend you create a package on a representative machine; that is, a machine that closely resembles the managed machines on which the package will be deployed.

Each Package is OS dependent. To deploy to multiple operating systems, you need to build a package for each OS. During installation, **Packager** checks the target machine's operating system and does not continue if the package is being deployed on an OS different than the source OS.

Step 2: Execute Packager .exe and follow the on-screen instructions to create a distribution package.

The following tasks are performed:

1. **Packager** takes a snapshot of the source system.
2. Install any application and/or resource on the source system.
3. Execute **Packager** again. **Packager** records the changes in the source system and creates a package.

Packager picks up everything you do to a machine between the time you take the first snapshot and create the package. Be careful what additional tasks you perform on the source machine as any system changes will be rolled into the package. Close all applications before running **Packager**. This prevents open applications from modifying the system during package creation.

Step 3: Distribute the package via a procedure.


Use Agent Procedure > [Schedule / Create](#) (*page 80*) to create an agent procedure that downloads the package to managed machines and runs it. Packages can only be executed on machines with agents installed. If the package fails to install, **Packager** has complete rollback capability. The rollback executable and associated restore files are located in the agent directory on the target machine in the directory `C:\Program Files\Kaseya\KPackage`.

Get File

Agent Procedures > File Transfer > Get File

The **Get File** page accesses files previously uploaded from a managed machine. Files can be uploaded to a machine-specific directory on the Kaseya Server using the [getFile\(\)](#) or [getFileInDirectoryPath\(\)](#) commands. Clicking the machine ID displays *all* uploaded files for that machine ID. Click the link underneath a file to display the file or run it.

Note: The files stored on the Kaseya Server using the `getFile()` command are machine-specific. Use [Manage Files Stored on Server](#) (page 108) to access files stored on the Kaseya Server that are not machine-specific.

- Each file is displayed as a link. Click any filename to access that file.
- Remove files by clicking the delete icon  next to the file.

Example 1: Checking Large Number of Managed Machines Simultaneously

Get File is designed to support automated checks on a large number of managed machines simultaneously.

Note: If all you want to do is get a file from a managed machine as a one-time event then [Remote Control > FTP](#) (page 336) is the simplest way.

Use **Get File** in conjunction with an agent procedure to perform some automated task on a set of managed machines. For example, if you have a utility that reads out some information unique to your client computers you can write a procedure to do the following:

1. Send the utility to the managed machine using either the `writeFile()` procedure command or the [Distribute File](#) page.
2. Execute the utility using either the `executeShellCommand()` or `executeFile()` agent procedure command and pipe the output to a text file, such as `results.txt`.
3. Upload the file to the Kaseya Server using the `getFile()` command.

Example 2: Comparing Versions of a File

As an option in the `getFile()` agent procedure command, existing copies of uploaded files can be renamed with a `.bak` extension prior to the next upload of the file. This allows you to examine both the latest version of the file and the previous version. For example, use the [IF-ELSE-STEP](#) agent procedure editor to create a simple `getFile()` agent procedure.

The first time the `getFile()` agent procedure command executes on a managed machine the agent sends `c:\temp\info.txt` to the Kaseya Server and the Kaseya Server stores it as `news\info.txt`. The second time `getFile()` agent procedure executes, the Kaseya Server renames the original copy of `news\info.txt` to `news\info.txt.bak` then uploads a fresh copy and saves it as `news\info.txt`.

Also as an option, an email alert can be sent when a change in the uploaded file has been detected, compared to the last time the same file was uploaded. The `getFile()` command must have either the [Overwrite existing file and send alert if file changed](#) setting or the [Save existing version, get file, and send alert if file changed](#) setting selected.

Example 3: Get File Changes Alerts

To perform continuous health checks on managed machines, run the agent procedure on a recurring schedule and activate a [Get File Changes](#) alert using [Monitor > Alerts - Get Files](#) (page 255). The VSA instantly notifies you of any changes to the results.

Troubleshooting Patch Installation Failures

When patch scan processing reports patch installations have failed, a `KBxxxxxx.log` (if available) and the `WindowsUpdate.log` are uploaded to the Kaseya Server. Additionally, for those patches that required an "Internet based install", a `ptchdlin.xml` file will be uploaded to the Kaseya Server. These files can be reviewed using [Agent Procedures > getFile\(\)](#) (page 116) for a specific machine and can help you troubleshoot patch installation failures. [Info Center > Reporting > Reports > Logs > Agent Procedure Log](#) contains entries indicating these log files have been uploaded to the Kaseya Server for each machine.

Distribute File

Agent Procedures > File Transfer > Distribute File

The **Distribute File** function sends files stored on your VSA server to managed machines. It is ideal for mass distribution of configuration files, such as virus foot prints, or maintaining the latest version of executables on all machines. The VSA checks the integrity of the file every **full check-in** (page 552). If the file is ever deleted, corrupted, or an updated version is available on the VSA, the VSA sends down a new copy prior to any procedure execution. Use it in conjunction with recurring procedures to run batch commands on managed machines.

Note: The procedure command `writeFile()` performs the same action as **Distribute File**. Each time a procedure executes the `writeFile()` command, the agent checks to see if the file is already there or not. If not, the file is written. `writeFile()` is better than **Distribute File** for sending executable files you plan to run on managed machines using agent procedures.

Select server file

Select a file to distribute to managed machines. These are the same set of files managed by clicking the **Manage Files...** link on this page.

Note: The only files listed are your own private managed files or shared managed files. If another user chooses to distribute a private file you can not see it.

Specify full path and filename to store file on remote machine

Enter the path and filename to store this file on selected machine IDs.

Manage Files...

Click the **Manage Files** (page 108)... link to display the **Manage Files Stored on Server** popup window. Use this window to add, update, or remove files stored on the Kaseya Server. This same window displays when you click the **Managed Files** button using **Schedule / Create** (page 80). Private files are listed with (Priv) in front of the filename.

Distribute

Click the **Distribute** button to start distribution management of the file selected in **Select server file** and write it to the location specified in **Specify full path and filename to store file on remote machine**. This effects all checked machine IDs.

Clear

Click the **Clear** button to remove the distribution of the file selected in **Select server file** from all checked machine IDs.

Warning: **Clear** and **Clear All** do *not* delete the file from either managed machines or the Kaseya Server. These functions simply stop the integrity check and update process from occurring at each full check-in.

Clear All









Clear All removes all file distributions from all checked managed machines.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended



Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Server File

The name of the file being distributed.

Agent File Location

The target directory on the managed machine. To the left of each target file location for a specific machine ID are two icons. Click  to cancel that file distribution for that machine ID. Click  to edit the destination path and filename for that machine ID.

Application Logging

Agent Procedures > Administration > Application Logging

The **Application Logging** page displays a log of **Agent Procedures** module activity by:

- **Event ID**
- **Event Name**
- **Message**
- **Admin**
- **Event Date**

This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 17, <http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#6875.htm>).

Chapter 5

Audit

In This Chapter

Audit Overview	122
View Assets	123
Manage Credentials	126
Credentials Log	127
Run Audit.....	128
Audit Summary	129
Configure Column Sets	131
Machine Summary.....	131
System Info.....	134
Installed Applications.....	136
Add/Remove.....	137
Software Licenses	137
Documents	138

Audit Overview

Audit

Agents (page 547) can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the Kaseya Server so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per day is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machines's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > **Reporti** (page 142)ng > Reports are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two **alert** (page 248) types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes**. Collected audit information includes:

- All hardware, including CPUs, RAM, PCI cards, and disk drives.
- All installed software, including licenses, version numbers, full path, and description.
- System Information from DMI and SMBIOS including PC make, model, serial number, mother board type, and over **40** other pieces of information describing the PC and its configuration.
- OS info with version number and service pack build.
- Current network settings including local IP address, gateway IP address, DNS, WINS, DHCP, and MAC address.

Functions	Description
View Assets (page 123)	Provides a consolidated view of all "assets" managed by the VSA.
Manage Credentials (page 126)	Specifies credentials by organization and machine group.
Credentials Log (page 127)	Provides an audit log of the VSA users who create, modify and delete credentials.
Run Audit (page 128)	Schedules latest, system, and baseline audits of machine IDs.
Audit Summary (page 129)	Displays data returned by audits of machines
Configure Column Sets (page 131)	Configures columns sets for the Audit Summary page.
Machine Summary (page 131)	Displays detailed information about a single managed machine.
System Information (page 134)	Shows DMI / SMBIOS data collected.
Installed Applications (page 136)	Shows a list of executable (.exe) files on selected managed machines.
Add/Remove (page 137)	Shows the Add or Remove Programs list from a managed machine.

Software Licenses (page 137)	Shows a list of vendor license codes found on selected managed machines.
Documents (page 138)	Stores files associated with a machine ID.

View Assets

Audit > Asset > View Assets

The Audit > [View Assets](#) page is populated by **Discovery** scans of networks and domains. The [View Assets](#) page provides a consolidated view of all "assets" managed by the VSA. Types of assets include:

- **Agent managed machines and mobile devices** - Computers and mobile devices that have an agent installed on them are always considered managed assets and display on this page for as long as the agent is installed on them.
- **Devices promoted to an asset** - When an agent cannot be installed on a discovered device, the device can still be "promoted" to a managed asset and display on this page. For example, a router or printer may still require monitoring, even if an agent cannot be installed on the machine. There are many different types of non-agent device types that can be managed by the VSA: routers, switchers, printers, firewalls, etc. The [Make Asset](#) button on the Discovery > Discovered Devices - Grid View page enables you to "promote" a device to an asset. When you do the device begins displaying on this page. You can "demote" a asset using the [Demote Asset to Device](#) on this page. When you do, the asset is removed from this page.

All managed assets are assigned a machine group and organization. [Scoping rules](#)

(<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4578.htm>) and [view filtering](#)

(<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#214.htm>) features within the VSA depend on this assignment.

- Multiple credentials can be defined for each asset. For agent assets, one of the credentials can be designated an agent credential and optionally used by **Policy Management** as an agent credential.
- **Service Desk** tickets can be optionally associated with assets listed on this page.

Actions

- **View** - Displays a popup window of information collected about a selected device. Different views, based on the type of probe used to collect the information, can be selected using the [Probe Type](#) drop-down list:
 - **NMAP Probe** - The standard method of discovering a device on a network, using the **Discovery** module.
 - **Machine Audit** - The audit performed on a machine installed with an agent.
 - **vPro** - The inventory of hardware attributes returned by a [vPro audit](#) (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#11552.htm>).
 - **Merge View** - Merges all methods of data collection into one consolidated view. The default view.
- **Demote Asset to Device** - Removes a selected device as an managed asset. Computers and mobile devices that have agents installed on them cannot be demoted.
- **Change Group** - Changes the organization and machine group assigned to an asset.
- **Refresh** - Refreshes the page.

Table Columns

- **Asset Name** - The name of the asset. Typically this is the device name combined with VSA machine group and organization assigned to the asset.

Audit

- **Device Type** - The type of device: computers, mobile devices, routers, switchers, printers, firewalls, etc
- **Computer Agent** - If checked, the asset is a computer and has an agent installed on it.
- **Mobile Agent** - If checked, the asset is a mobile device and has an agent installed on it.
- **Probes** - Click this link to display the list of methods used to probe this computer or device.
- **Monitoring** - If checked, this asset is monitored.
- **Patching** - If checked, this asset is managed by Patch Management.
- **Auditing** - If checked, this asset is audited on a recurring basis.
- **Backing Up** - If checked, this asset is being backed up.
- **Security** - If checked, this asset has antivirus protection.
- **Ticket Count** - Displays the number of open tickets for this asset.
- **Alarm Count** - Displays the number of alarms generated by this asset.
- **Domain / Workgroup** - The domain or workgroup this asset is member of, if any.
- **SNMP Active** - If checked, this asset is SNMP-enabled.
- **vPro Active** - If checked, this asset is vPro-enabled
- **Network** - Click this link to display the list of networks this asset is a member of.
- **Device Name** - The network name of a computer or device. If no network name is available, the IP address of the device displays.

Credentials tab

This tab specifies **credentials** (page 553) by individual asset. These can be referenced by a VSA user when accessing a machine or device. Optionally include a note with each credential. The **Quick View** (page 16) popup window includes a **View Credentials** option. **Quick View** access to the credentials displayed can be limited by role and by scope. Use the **Manage Credentials** (page 126) page to specify credentials by organization and machine group.

Agent Credentials

If the asset is an agent machine, a credential can be optionally used as the **source credential for an agent credential in a Policy Management policy** (<http://help.kaseya.com/webhelp/EN/KPM/7000000/index.asp#8158.htm>). If multiple credentials are defined for a machine, then the most local level defined has precedence: by individual machine, by machine group, or by organization. At any one level, only one managed credential can be designated the source credential for an agent credential.

Actions

- **New / Edit** - Specifies a credential.
 - **Description** - A one line description for the credential.
 - **Username** - The username.
 - **Password** - The password.
 - **Domain** - The domain of the credential, if one exists.
 - **Set as agent credential** - Only one credential for this asset can be designated the source credential for an agent credential.
 - ✓ **Create account** - Check to create a new user account on the managed machine.
 - ✓ **as Administrator** - Check to create the new user account with administrator privileges.
 - ✓ **Local user account** - Select this option to use a credential that logs into this machine locally, without reference to a domain.
 - ✓ **Use machine's current domain** - Create a credential using the domain name this machine is a member of, as determined by the **latest audit** (page 551).

- ✓ **Specified domain** - Use the domain specified above.
- **Notes** - Optionally include a note with the credential. Use the edit toolbar to add images and special formatting to the text. *Images must be uploaded rather than copied and pasted in.*



- ✓ - Hyperlink selected text. You may need to reset links copied and pasted from another source.
- ✓ - Insert a table.
- ✓ - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
- ✓ - Indent text.
- ✓ - Outdent text.
- ✓ - Remove formatting.
- ✓ - Insert a symbol.
- ✓ - Insert an emoticon.
- ✓ - Preview the display of text and images.
- ✓ - Upload a file or image.
- ✓ - Set selected text to subscript.
- ✓ - Set selected text to superscript.
- ✓ - Toggle full screen mode for editing and viewing.
- **View** - Displays the properties of a selected credential.
- **Delete** - Deletes a select credential.

Table Columns

- **Type** - The type of credential.
 - - This is an agent credential.
 - (blank) - This is *not* an agent credential.
- **Name** - The VSA name of this credential.
- **Username** - The username of the credential.
- **Domain** - The domain of the credential, if one is required.
- **Agent Credential** - If checked, this is the agent credential.
- **Create Account** - Created the account if it does not already exist.
- **as Administrator** - Created the account is an administrator-level account.

vPro tab

Audit > View Assets > vPro tab

The Audit > View Assets > **vPro** tab displays hardware information about vPro-enabled machines discovered by enabling a vPro scan using the Edit Network dialog, then running **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#11552.htm>). This information is only available if a machine's vPro credential is specified by the **LAN Watch**.

Types of hardware information returned by the vPro machine include:

- Agent check-in status, if the vPro machine has an agent installed
- Computer Information
- Motherboard Asset Information
- BIOS Information
- Processor Information
- RAM Information

- Hard Drive Information

Note: The **vPro** module provides **vPro management features**

(<http://help.kaseya.com/webhelp/EN/vpro/7000000/index.asp#home.htm>).

Intel vPro Rebate: Kaseya is participating in a vPro rebate program offered by Intel. If you have installed vPro enabled machines and perform a LAN Watch—and the vPro machine qualifies for the rebate—you can quickly generate the information you need by clicking the **Generate Intel® vPro™ rebate file** button. This generates a .CVS file containing the information you need document your rebate claim with Intel. An **Intel® vPro™ Technology Activation Rebate Rules** link is also provided.

Manage Credentials

Audit > Asset > Manage Credentials

The **Manage Credentials** page specifies **credentials** (page 553) by organization and machine group. These can be referenced by a VSA user when accessing a machine or device. Optionally include a note with each credential.

Credentials in Quick View




The **Quick View** (page 16) popup window includes a **View Credentials** option. **Quick View** access to the credentials displayed can be limited by role and by scope. Use the **View Assets** (page 123) page to specify credentials by individual machine or device.

Agent Credentials

If the asset is an agent machine, a credential can be optionally used as the **source credential for an agent credential in a Policy Management policy** (<http://help.kaseya.com/webhelp/EN/KPM/7000000/index.asp#8158.htm>). If multiple credentials are defined for a machine, then the most local level defined has precedence: by individual machine, by machine group, or by organization. At any one level, only one managed credential can be designated the source credential for an agent credential. A managed credential is created when a user runs the **Systems Management Configuration Setup Wizard** (<http://help.kaseya.com/webhelp/EN/KDPM/7000000/index.asp#10070.htm>) for an organization.

Middle Panel Columns

Rows are sorted by organization, then machine group, then machine ID.

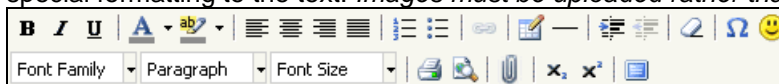
- **(Level)** - Identifies the row as an organization , a machine group  or a machine ID .
- **Name** - The name of the organization, machine group or machine ID.
- **Credentials** - Displays a key if at least one credential is specified for that row.

Right Panel Actions

Select an organization or machine group before performing these actions.

- **New / Edit** - Specifies a credential.
 - **Description** - A one line description for the credential.
 - **Username** - The username.
 - **Password** - The password.
 - **Domain** - The domain of the credential, if one exists.
 - **Set as agent credential** - Only one credential for this organization or machine group can be designated the source credential for an agent credential.
 - ✓ **Create account** - Check to create a new user account on the managed machine.

- ✓ **as Administrator** - Check to create the new user account with administrator privileges.
 - ✓ **Local user account** - Select this option to use a credential that logs into this machine locally, without reference to a domain.
 - ✓ **Use machine's current domain** - Create a credential using the domain name this machine is a member of, as determined by the **latest audit** (page 551).
 - ✓ **Specified domain** - Use the domain specified above.
- **Notes** - Optionally include a note with the credential. Use the edit toolbar to add images and special formatting to the text. *Images must be uploaded rather than copied and pasted in.*



- ✓ - Hyperlink selected text. You may need to reset links copied and pasted from another source.
 - ✓ - Insert a table.
 - ✓ - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
 - ✓ - Indent text.
 - ✓ - Outdent text.
 - ✓ - Remove formatting.
 - ✓ - Insert a symbol.
 - ✓ - Insert an emoticon.
 - ✓ - Preview the display of text and images.
 - ✓ - Upload a file or image.
 - ✓ - Set selected text to subscript.
 - ✓ - Set selected text to superscript.
 - ✓ - Toggle full screen mode for editing and viewing.
- **Delete** - Deletes a select credential.

Table Columns

- **Username** - Username of the credential.
- **Password** - Password of the credential.
- **Domain** - Domain of the credential, if applicable.
- **Inherited From** - The level the credential is inherited from. Credentials can be inherited from a higher level organization or machine group.
- **Agent** - If checked, this is the agent credential.
- **Description** - The VSA name for the credential.
- **Notes** - Notes about the credential.

Credentials Log

Audit > Asset > Credential Logs

The **Credential Logs** page provides an audit log of the VSA users who create, modify and delete credentials on the **View Assets** (page 123) and **Manage Credentials** (page 126) pages.

- **Event ID**
- **Event Name**
- **Message**
- **Admin**
- **Event Date**

Run Audit

Audit > Collect Data > Run Audit

The **Run Audit** page performs audits of the hardware and software configuration of managed machines.

Audits

Agents (page 547) can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the Kaseya Server so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per day is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machine's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > **Reporting** (page 142) > Reports are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two **alert** (page 248) types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes**.

Actions









- **Schedule Audit** - Click **Schedule Audit** or **Reschedule Audit** to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:
 - **Baseline Audit, Latest Audit or System Information** - Type of audit.
 - **Schedule will be based on the timezone of the agent (rather than server)** - If checked, time settings set in the Scheduler dialog reference the local time on the agent machine to determine when to run this task. If blank, time settings reference server time, based on the server time option selected in System > Preferences. Defaults from the System > Default Settings page.
 - **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
 - **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
 - **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
 - **Exclude the following time range - Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.
- **Reschedule Audit** - Populates the scheduler with the values of a pending schedule so you can make adjustments.
- **Run Audit Now** - Schedules an audit to run immediately.
- **Cancel Audit** - Cancels a scheduled audit.

Remind me when accounts need audit scheduled

If checked, displays a pop up warning message if audits have not been scheduled for one or more machine IDs. The warning displays each time you select **Run Audit**. Applies to each VSA user individually.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Machine.Group ID

The top line shows the machine ID. The bottom line displays the last time a System Info audit was performed. Overdue date/time stamps display as **red text with yellow highlight**. Pending and completed date/time stamps display as black text.

System Information / Latest Audit / Baseline Audit

Each column displays the last time that type of audit was performed. Overdue date/time stamps display as **red text with yellow highlight**. Pending and completed date/time stamps display as black text.

Next Audit

Displays the time of the next scheduled Latest Audit. Overdue date/time stamps display as **red text with yellow highlight**. Pending and completed date/time stamps display as black text.

Recurring Interval

Displays the recurring interval for latest audits.

Audit Summary

Audit > View Group Data > Audit Summary

The Audit > **Audit Summary** page provides a view of the data returned by audits of machines using the **Run Audit** (page 128) page. The columns of audit data shown on this page are individually selectable and filterable. User-defined sets of columns can also be selected. Columns sets are defined using the **Configure Column Sets** (page 131) page. Additional data not shown in the **Audit Summary** page is provided using the **Machine Summary** (page 131) page. This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 17).

Columns of audit data, in the default order they display in this page, include:

- **Machine ID** - The name identifying the machine within the VSA. Typically based on the computer name.
- **Current User** - Logon name of the machine user currently logged into the machine (if any).

Audit

- **Last Reboot Time** - Time of the last known reboot of the machine.
- **Last Checkin Time** - Most recent time when a machine checked into the Kaseya Server.
- **Group ID** - The group ID portion of the machine ID.
- **First Checkin Time** - Time when a machine first checked into the Kaseya Server.
- **Time Zone** - The time zone used by the machine.
- **Computer Name** - The name assigned the machine by users of the machine.
- **Domain/Workgroup** - The workgroup or domain the computer belongs to.
- **DNS Computer Name** - The fully qualified DNS computer name identifying the machine on the network. The DNS computer name typically comprises the computer name plus the domain name. For example: `jsmithxp.acme.com`. Displays only the computer name if the machine is a member of a workgroup.
- **Operating System** - Operation system type the machine is running.
- **OS Version** - Operation system version string.
- **CPU Type** - Processor make and model.
- **CPU Speed** - Clock speed of the processor.
- **CPU Count** - The number of CPUs.
- **RAM (MB)** - Megabytes of RAM on the machine.
- **Agent Version** - Version number of the Kaseya agent loaded on the machine.
- **Last Logged In User** - Logon name of the last person to log into the machine.
- **Primary/Secondary KServer** - IP address / name the machine uses to communicate with the Kaseya Server.
- **Quick Checkin Period - Quick check in** (*page 552*) time setting in seconds.
- **Contact Name** - Machine user name entered in **Edit Profile** (*page 65*).
- **Contact Email** - Email address entered in Edit Profile.
- **Contact Phone** - Phone number entered in Edit Profile.
- **Manufacturer** - System manufacturer.
- **Product Name** - System product name.
- **System Version** - Product version number.
- **System Serial Number** - System serial number.
- **Chassis Serial Number** - Serial number on the enclosure.
- **Chassis Asset Tag** - Asset tag number on the enclosure.
- **External Bus Speed** - Motherboard bus speed.
- **Max Memory Size** - Max memory size the motherboard can hold.
- **Max Memory Slots** - Total number of memory module slots available.
- **Chassis Manufacturer** - Manufacturer of the enclosure.
- **Chassis Type** - Enclosure type.
- **Chassis Version** - Enclosure version number.
- **Motherboard Manufacturer** - Motherboard manufacturer.
- **Motherboard Product** - Motherboard product ID.
- **Motherboard Version** - Motherboard version number.
- **Motherboard Serial Num** - Motherboard serial number.
- **Processor Family** - Processor type installed.
- **Processor Manufacturer** - Processor manufacturer.
- **Processor Version** - Processor version ID.
- **CPU Max Speed** - Max processor speed supported.
- **CPU Current Speed** - Speed processor is currently running at.
- **IPv4 Address** - IP address assigned to the machine, in version 4 format.
- **IPv6 Address** - IP address assigned to the machine, in version 6 format.

- **Subnet Mask** - Networking subnet assigned to the machine.
- **Default Gateway** - Default gateway assigned to the machine.
- **Connection Gateway** - IP address seen by the Kaseya Server when this machine checks in. If the machine is behind a DHCP server, this is the public IP address of the subnet.
- **Country** - The country associated with the Connection Gateway.
- **MAC Address** - MAC address of the LAN card used to communicate with the Kaseya Server.
- **DNS Server** - IP address of the DNS server assigned to the machine.
- **DHCP Server** - The IP address of the DHCP server used by this machine.
- **Primary/Secondary WINS** - WINS settings.
- **Free Space** - The free data storage space in gigabytes.
- **Used Space** - The used data storage space in gigabytes.
- **Total Size** - The total data storage space in gigabytes.
- **Number of Drives** - The number of drives on the machine.
- **Portal Access Logon** - Logon name given to a machine user for logging into the Kaseya Server.
- **Portal Access Remote Control** - Enabled if this machine user can log in and get remote control access *to their own machine from another machine*. Disabled if access is denied.
- **Portal Access Ticketing** - Enabled if this machine user can log in and enter trouble tickets. Disabled if access is denied.
- **Portal Access Chat** - Enabled if this machine user can *initiate* chat sessions with a VSA user. Disabled if access is denied.

Configure Column Sets



[Audit](#) > [View Group Data](#) > [Configure Column Sets](#)

The [Configure Columns Sets](#) page defines columns sets that can be used to select a set of columns in the [Audit](#) > [Audit Summary](#) (*page 129*) table.

Actions

- **New** - Create a new column set.
- **Edit** - Edit a selected column set.
- **Delete** - Delete a selected column set.

Select a Column Set

Select an existing column set in the middle panel of this page. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

Machine Summary

[Audit](#) > [View Individual Data](#) > [Machine Summary](#)

- Similar information is provided using [Info Center](#) > [Reporting](#) > [Machine Summary](#) (*page 180*).

Machine Summary

The [Machine Summary](#) page allows users to perform tasks and functions solely for one managed machine. A series of tabbed property sheets provided access to various categories of information about the managed machine.

Audit

Actions



You may wish to edit both custom field values and the data collected for a machine during a system audit. Edits to system audit data will be overwritten by subsequent system audits, unless you remove these system audit fields from automatic collection. Edited system audit fields and custom fields can both be selected using the Agent > **Agent Status** (page 28) page, the **Filter Aggregate Table** (page 27) page and the **Aggregate Table** (page 179) report. You can also automate changes to the values of data items by running the **updateSystemInfo()** (page 102) command in an agent procedure.

- **Edit Machine Data** - Edits the data collected for a machine by a system audit. You can also edit the values for custom fields.
- **Edit Automatic Collection** - Uncheck items to prevent data from being overwritten by subsequent system audits. Used in conjunction the **Edit Machine Data** dialog.
- **Bulk Edit Custom** - Changes the values of custom fields for multiple machines.
 1. Select multiple machine rows.
 2. Click the **Bulk Edit Custom** button.
 3. Select a custom field from the **Custom field to modify** drop-down list.
 4. Choose a replacement value by:
 - ✓ Selecting an existing replacement value from the drop-down list, or...
 - ✓ Entering the replacement value manually.

You can maintain an unlimited number of custom fields of information about managed machines. Custom fields can be maintained on both the **Summary** tab and the Hardware > **Summary** tab of this page. Custom fields can also be maintained on the Audit > **System Information** (page 134) page. Custom fields are supported in views, procedures, and reports. Custom reports do not support more than 40 custom fields.

- **New Custom Field** - Creates a new custom field.
- **Rename Custom Field** - Renames a custom field.
- **Delete Custom Field** - Deletes a custom field.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

Summary

- **Collections** - Displays the **collections** (page 552) a machine is a member of. Defined using the **Only show selected machine IDs** option in **View Definitions** (page 24).
- **Name/OS Information** - Displays the name, operating system and OS version.
- **System Information** - Displays the manufacturer of system, the product name, version and serial number.
- **Network Information** - Displays network configuration settings.
- **CPU/RAM Information** - Displays CPU and RAM specifications.
- **Custom Fields** - Displays custom fields and values assigned by the user to this machine.

Software

- **System Information** - Lists system hardware attributes and related information.
- **Software Licenses** - Lists all software licenses found for a selected machine ID. Duplicate license keys found on more than one machine **display in red text**. Clicking the number link next to the title of a duplicate license lists the machine IDs using the duplicate license.
- **Installed Applications** - Lists all the applications installed on the managed machine.
- **Add/Remove** - Displays programs listed in Add/Remove window of Windows machines.

- **Startup Apps** - Displays programs that start automatically when a user logs on.
- **Security Products** - Identifies the install status of antivirus products registered with a Windows machine's *Windows Security Center*. Windows 7 and later later calls the *Windows Security Center* the *Action Center*.

Hardware

- **Summary**
 - **System Information** - Lists system hardware attributes and related information.
 - **Network Information** - Displays network configuration settings.
 - **Chassis** - The chassis manufacturer, type, version, serial number and asset tag.
 - **Motherboard** - The motherboard manufacturer, product, version, serial number and external bus speed.
 - **CPU/RAM Information** - Displays CPU and RAM specifications.
 - **Custom Fields** - Displays custom fields and values assigned by the user to this machine.
- **Printers** - Lists the printers and ports a machine can direct print jobs to.
- **PCI & Disk Hardware** - Displays type, vendor, and product names.
- **Disk Volumes** - Displays disk volume information.
- **Disk Partitions** - Displays the partitions on each disk volume.
- **Disk Shares** - Displays shared folders.

Agent

- **Settings** - Displays information about the agent on the managed machine:
 - **Agent version**
 - **Current User**
 - **Last check-in**
 - **Last reboot**
 - **First time check-in**
 - **Patch Policy Membership** - Defined using Patch Management > Membership: Patch Policy
 - **View Definition Collections** - Defined using the **Only show selected machine IDs** option in **View Definitions** (page 24).
 - **Working Directory** - Can also be defined using Agent > **Working Directory** (page 64).
 - **Check-In Control** - Can also be defined using Agent > **Check-In Control** (page 61).
 - **Edit Profile** - Can also be defined using Agent > **Edit Profile** (page 65).
 - **Agent Logs and Profiles** - Can also be defined using Agent > **Log History** (page 32).
- **Logs** - Displays the logs available for a machine: Alarm Log, Monitor Action Log, Agent Log, Configuration Changes, Network Statistics, Event Log, Agent Procedure Log, Remote Control Log, Log Monitoring.
 - **Pending Procedures** - Displays pending procedures for a machine and the procedure history for that machine. Includes the execution date/time, status and user who scheduled the procedure.

Alerts

- Defines alerts for a machine: **Agent Status** (page 250), **Application Status** (page 253), **Get File Changes** (page 255), **Hardware Changes** (page 258), **Low Disk Space** (page 260), LAN Watch, **Agent Procedure Failure** (page 262), **Protection Violations** (page 264), **Patch Alert** (page 268), **Backup Alert** (page 271).

Patch Status

Audit

- Displays **Missing** and **Pending** Microsoft patches and schedules missing patches. If a machine belongs to a **patch policy** (page 559), missing patches may be further identified as **Denied** (**Pending Approval**). The user can manually override the denied patch policy by scheduling the patch.
 - Click the **Schedule** button to schedule a selected missing patch.
 - Click the **Cancel** button to cancel a selected pending patch.
 - Click the **Show History** link to display the history of patches installed on the managed machine.

Remote Control

- Displays the status of remote control sessions for the managed machine: Remote Control, FTP, and Chat. The VSA user can set the remote control package to use during a remote control session.

Documents

- Lists documents uploaded to the Kaseya Server for a managed machine. You can upload additional documents. Provides the same functionality as Audit > **Documents** (page 138).

Users

- **Accounts** - Lists all user accounts for the managed machine.
- **Groups** - Lists all user groups for the managed machine.
- **Members** - Identifies the users belonging to each user group for the managed machine.

System Info

Audit > View Individual Data > System Information

- Similar information is provided using Info Center > Reporting > Reports > **Inventory** (page 180).

The **System Info** page displays all DMI / SMBIOS data collected by the system info **audit** (page 551) for a selected machine ID.

Actions



You may wish to edit both custom field values and the data collected for a machine during a system audit. Edits to system audit data will be overwritten by subsequent system audits, unless you remove these system audit fields from automatic collection. Edited system audit fields and custom fields can both be selected using the Agent > **Agent Status** (page 28) page, the **Filter Aggregate Table** (page 27) page and the **Aggregate Table** (page 179) report. You can also automate changes to the values of data items by running the **updateSystemInfo()** (page 102) command in an agent procedure.

- **Edit Machine Data** - Edits the data collected for a machine by a system audit. You can also edit the values for custom fields.
- **Edit Automatic Collection** - Uncheck items to prevent data from being overwritten by subsequent system audits. Used in conjunction the **Edit Machine Data** dialog.
- **Bulk Edit Custom** - Changes the values of custom fields for multiple machines.
 1. Select multiple machine rows.
 2. Click the **Bulk Edit Custom** button.
 3. Select a custom field from the **Custom field to modify** drop-down list.
 4. Choose a replacement value by:
 - ✓ Selecting an existing replacement value from the drop-down list, or...
 - ✓ Entering the replacement value manually.

You can maintain an unlimited number of custom fields of information about managed machines. Custom fields can also be maintained on the Audit > **Machine Summary** (page 131) page. Custom fields are supported in views, procedures, and reports. Custom reports do not support more than 40 custom fields.

- **New Custom Field** - Creates a new custom field.
- **Rename Custom Field** - Renames a custom field.
- **Delete Custom Field** - Deletes a custom field.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

Displayed Data

- System Information
 - **Manufacturer** - system manufacturer
 - **Product Name** - system product name
 - **System Version** - system version number
 - **System Serial Number** - system serial number
- Network Information
 - **IPv4 Address** - IP version 4 address assigned to the machine.
 - **IPv6 Address** - IP version 6 address assigned to the machine.
 - **Subnet Mask** - Networking subnet assigned to the machine.
 - **Default Gateway** - Default gateway assigned to the machine.
 - **Connection Gateway** - IP address seen by the Kaseya Server when this machine checks in. If the machine is behind a DHCP server, this is the public IP address of the subnet.
 - **Country** - The country associated with the Connection Gateway.
 - **MAC Address** - MAC address of the LAN card used to communicate with the Kaseya Server.
 - **DHCP Server** - The IP address of the DHCP server used by this machine.
 - **DNS Server 1, 2** - IP address of the DNS servers assigned to the machine.
- Chassis
 - **Chassis Manufacturer** - manufacturer of the enclosure
 - **Chassis Type** - enclosure type
 - **Chassis Version** - enclosure version number
 - **Max Memory Slots** - total number of memory module slots available
 - **Chassis Serial Number** - serial number on the enclosure
 - **Chassis Asset Tag** - asset tag number on the enclosure
- Motherboard
 - **Motherboard Manufacturer** - motherboard manufacturer
 - **Motherboard Product** - motherboard product ID
 - **Motherboard Version** - motherboard version number
 - **Motherboard Serial Num** - motherboard serial number
 - **External Bus Speed** - motherboard bus speed
- CPU/RAM Information
 - **Processor Manufacturer** - processor manufacturer
 - **Processor Family** - processor type installed

Audit

- **Processor Version** - processor version ID
- **CPU Max Speed** - max processor speed supported
- **CPU Current Speed** - speed processor is currently running at
- **CPU** - Processor make and model.
- **Quantity** - The number of CPUs.
- **Speed** - Clock speed of the processor.
- **RAM** - MBytes of RAM on the machine.
- **Max Memory Size** - maximum memory size the motherboard can hold
- **Max Memory Slots** - Total number of memory module slots available.
- **Custom Fields** - Displays custom fields and their values.
- **On Board Devices** - Lists motherboard based devices (like video or ethernet).
- **Port Connectors** - Lists all the connections available on the chassis.
- **Memory Devices** - Lists memory modules installed on the motherboard.
- **System Slots** - Displays the status of each available card slot.



Installed Applications

Audit > View Individual Data > Installed Applications

- Similar information is provided using [Info Center > Reporting > Reports > Software](#) - [Software Applications Installed \(page 205\)](#).

The Installed Applications page lists all applications found during the [latest audit \(page 551\)](#) for a selected machine ID. The list of machine IDs you can select depends on the [machine ID / group ID filter \(page 23\)](#) and the [scope \(page 369\)](#) you are using. This table supports [selectable columns, column sorting, column filtering and flexible columns widths \(page 17\)](#).

Select a Machine



Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Application** - The filename of the application.
- **Description** - A brief description of the application as reported in the Properties dialog box of the executable file.
- **Version** - The version number of the application.
- **Manufacturer** - The manufacturer of the application.
- **Product Name** - The product name of the application.
- **Directory Path** - The absolute directory path where the application file is located.
- **File Size** - The size, in kilobytes, of the application file.
- **Last Modified** - The modification date of the application file.

Note: You can filter the display of machine IDs on any agent page using the [Contains/Missing application and Version string is > < = N options in View Definitions \(page 24\)](#).

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of

each page of data using the *sort order of the selected column on that page*.



Add/Remove

Audit > View Individual Data > Add/Remove

- Similar information is provided using **Info Center > Reporting > Reports > Software**.
- Alerts can be defined using **Monitor > Alerts > Application Changes** (page 253).

The **Add/Remove** page displays the programs listed in the **Add or Remove Programs** window of the managed machine. Information shown on this page is collected when a **Latest Audit** (page 128) is performed. Click a machine ID to display data for that selected machine. The list of machine IDs you can select depends on the **machine ID / group ID filter** (page 23) and the **scope** (page 369) you are using.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Application Name** - The name of the application.
- **Uninstall String** - The uninstall string in the registry used to uninstall this application.

Software Licenses

Audit > View Individual Data > Software Licenses

- Similar information is provided using **Info Center > Reporting > Reports > Software**.



The **Software Licenses** page displays all software licenses found for a selected machine ID. The list of machine IDs displayed depends on the **Machine ID / Group ID filter** (page 23) and machine groups the user is authorized to see using **System > User Security > Scopes** (page 369).

Information shown on this page is collected when a **Latest Audit** (page 128) is performed. Each vendor stores an application's license key differently so all application software licenses may not be collected.

Duplicate License Keys

Duplicate license keys found on more than one machine **display in red text**. Clicking the number link next to the title of a duplicate license lists the machine IDs using the duplicate license.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Publisher** - The software publisher of the application (e.g. Microsoft).
- **Title** - The name of the application.
- **Product Key** - The product key used to activate the application during installation.
- **License** - The license code associated with the application.
- **Version** - The version of the application.
- **Date** - The version release date.

Documents

Audit > View Individual Data > Documents

- This function can also be accessed using the Documents tab of the Live Connect (page 344) > Agent Data page and the Documents tab of the Machine Summary (page 131) page.

The **Documents** page stores files associated with a machine ID. For example, you can upload scanned copies of purchase receipts, contract information, and configuration notes specific to a machine ID. Uploaded documents are stored in the User Profiles directory of the Kaseya Server. For example:
C:\Kaseya\UserProfiles\368905064566500\Docs.

Note: Documents are not included in the backup of the Kaseya Server database using System > Configure (page 377). A separate backup of Kaseya Server files and directories should be performed as well.

Note: See Administrator Notes (page 12) for a fast way of logging plain text notes for multiple machines without having to upload documents.

To Store a Document


1. Click a machine.group ID link. The list of machine IDs you can select depends on the **machine ID / group ID filter** (page 23) and the **scope** (page 369) you are using. Documents previously stored on the Kaseya Server for this machine ID display or else No files found displays.
2. Click **Browse** to locate a file on your local computer or LAN.
3. Click **Upload** to upload the file to the Kaseya Server.

The added **Filename** displays, along with its file **Size** and the date/time of the **Last Upload**.


New Folder

Optionally click the **New Folder** icon and link to create a new folder to store documents in for the selected managed machine.

Edit

You can click a **Filename** link or edit icon  to display a file or run the file, depending on the application the filename extension is associated with on your local machine.

Delete

Click the delete icon  to delete a stored document or folder from the Kaseya Server.

Chapter 6

Info Center

In This Chapter

Inbox	140
Schedule	141
Reports	142
Report Sets	148
Report Templates	150
Report Parts	166
Name Value Parts	167
Cover Page, Header, Footer	175
Defaults	176
Legacy Report Definitions	176
Management Dashboard	209
View Dashboard	210
Layout Dashboard	211

Inbox

Info Center > Desktop > Inbox

The **Inbox** displays all inbound messages sent to you by other VSA users or by system events. System events include:

- **Reporting** - The **Reports**, **Report Sets** and **Schedule** pages can all generate an inbox message when a report is generated, if a user is specified as a message recipient.
- **Service Desk** - **Service Desk** procedures can specify the sending of a message to one or more users. **Service Desk** generated messages are formatted using Service Desk > Message Templates.

Note: Inbox messages are not archived.

Actions

- **New** - Creates a message to other VSA users.
- **Forward** - Forwards a selected message to other VSA users.
- **Reply** - Replies to a selected message from another VSA user.
- **Delete** - Deletes selected messages.
- **Read** - Sets selected messages to read.
- **Unread** - Sets selected messages to unread.
- **Refresh** - Refreshes the page.

Editing

For **New**, **Forward** and **Reply**:

- Click the **To** **Cc** icons to select one or more VSA users to send a message to. You can filter the list of users to select from.
- Use the following toolbar buttons to add special formatting to the text:






- - Hyperlink selected text. You may need to reset links copied and pasted from another source.
- - Insert a table.
- - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
- - Indent text.
- - Outdent text.
- - Remove formatting.
- - Insert a symbol.
- - Insert an emoticon.
- - Preview the display of text and images.
- - Upload a file or image.
- - Set selected text to subscript.
- - Set selected text to superscript.
- - Toggle full screen mode for editing and viewing.

Schedule

Info Center > Reporting > Schedule

The **Schedule** reports page includes all reports and reports sets *published using the same scope you are currently using*. If your Info Center > **Inbox** (page 140) messages and emails have been deleted, you can always locate a published report you are **authorized to view** (page 148).









Click the  icon next to the name of the report  or report set  to display a **Selected Item History** dialog that contains the publishing history for that report. Click the publishing date of the report you want to see, then click the hyperlink of that report at the bottom of the dialog. Use this same dialog to **Approving / Rejecting Reports** (page 147) a report.

Actions

- **Run Now** - Runs a previously scheduled report or report set immediately. This allows a report that has timed out, generated an error, or was unapproved to be re-run immediately without having to reselect all the schedule options over again.
- **Recipients** - Displays the **Distribution** tab of the **Reschedule Selected Item** (page 145) dialog. Use this tab to change the recipients for a selected report you are rescheduling. *These options are the same as when you originally schedule a report.*
- **History** - Displays a **Selected Item History** dialog, providing a history of all published instances of the report or report set you have received. Click the publishing date of the report or report set you want to see, then click the hyperlink of a report at the bottom of the dialog. Use this same dialog to **Approving / Rejecting Reports** (page 147) a report.
- **Scheduling**
 - **New** - Schedules any report you are authorized to publish.
 - **Edit** - Displays the **Schedule** tab of the **Reschedule Selected Item** (page 145) dialog. Use this tab to reschedule the publishing of a selected report or report set. *These options are the same as when you originally schedule a report.*
 - **Delete** - Permanently deletes a selected published report or report set. This only deletes the record of the report in **Schedule** for your VSA logon. It does *not* delete the report for any other user.
- **Refresh** - Refreshes the page.

Table Columns

This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 17).

- **(Status)**
 -  Pending
 -  Completed and Approval Required - Click the  icon to view the completed report, then approve or reject it. See **Approving / Rejecting Reports** (page 147).
 -  Completed and Rejected - Click the  icon to view the completed and rejected report. You can subsequently approve it.
 -  Completed and Distributed - Click the  icon next to the name of the report to display a **Selected Item History** dialog that contains the publishing history for that report. Click the publishing date of the report you want to see, then click the hyperlink of that report at the bottom of the dialog.
 -  Error - The report failed to publish.
- **Name** - The name of the report.
- **Owner** - The creator of the report.
- **Recurrence** - Click the recurrence—Once, Daily, Weekly, Monthly—to update the schedule.
- **Recipients** - Click the number of recipients to update the list of recipients in the **Reschedule Select Item** (page 145) dialog.

- **Recipient List** - A list of recipients.
- **Last Ran** - The last time this report was published.
- **Next Run** - The next time this report is scheduled to be published.
- **Organization, Machine Group, Machine, View** - The types of **Data Filters** (page 145) used to limit the data included in a report. Use a view to select more than one organization, machine group or machine. All machine groups in all organizations you are authorized by your scope to view are selected by default.
- **Type** - Report or Reportset
- **Status** - The status of the report in text.
- **Location** - The folder the scheduled report is located in, in the middle pane.
- **Date Created** - The date the report was scheduled.
- **Scope** - Visibility of rows in the schedule table is limited by the scope you are using. Your scope must match the scope that was current when the owner scheduled the report. This ensures that only users authorized to view the same data shown in the report can reschedule and modify recipients of the report. Email recipients can always access the completed report in email, even if they are not members of the same scope.

Reports

Info Center > Reporting > Reports

Virtual System Administrator™ provides comprehensive reporting for all applications. **Reports** (page 142) can be customized, using report parameters, and filtered by organization, machine group, machine ID or view definition. You can output reports to PDF, HTML, or Excel document and brand reports with your own logo, cover page, header and footer. Reports can be scheduled to run automatically and on a recurring basis. They can be private or shared, distributed to the **Inbox** (page 140) of VSA users or to email recipients. An optional "requires approval" step is provided, just prior to distribution. Reports can also be bundled into **Report Sets** (page 148), enabling you to schedule a standard batch of reports. Your own **Schedule** (page 141) reports list shows you every report you have access to, so you can always locate any pending report you've created and scheduled or any report you've received.

See the following topics for an overview of working with reports.

- **Report Definitions** (page 143)
- **Report Folder Trees** (page 144)
- **Publishing a Report Immediately** (page 145)
- **Data Filters** (page 145)
- **Scheduling / Rescheduling a Report** (page 145)
- **Managing Scheduled Items** (page 146)
- **Approving / Rejecting Reports** (page 147)
- **Report and Report Set User Security** (page 148)
- **Legacy Report Definitions** (page 176)

Terms and Concepts

- **Published Reports** - Published reports contain the layout and data for a certain date, time, scope and other criteria and are distributed to a selected set of recipients. To see new data in the same report, the report must be republished and redistributed.
- **Report Definitions** - A report is published from a report definition. Report definitions contain all the *default* settings that determine the content, layout and file format of the published report. You can override these defaults when you publish the report.

- **Report Templates** - A report definition is created by copying settings from a report template. Report templates define all the *default* settings for a report definition. There are two types of report templates:
 - **Custom** - Customizable report templates.
 - **Legacy - Fixed layout report templates provided in earlier releases** (page 176).
- **Report Categories** - Report templates are organized by report template categories.

Report Definitions

A report is published from a report definition. Report definitions contain all the *default* settings that determine the content, layout and file format of the published report. You can override these defaults when you run (publish) or schedule the report.

Report definition settings are copied from a report template when the report definition is created. Changing a report definition does not change the report template it was copied from. Changes made to a report template do not affect report definitions already copied from that template.

To create a *custom report definition* based on a *report template*:

1. Click **Info Center > Reporting > Reports > New**.
2. Select the custom **Report** option.
3. Select a **category**, then a **template**, then click **Create**.

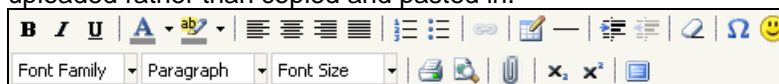
Note: A custom report template must be published (page 150) for you to see it within a **Reports** (page 142) category.

4. Specify options for report definitions using header options and three tabs:
 - **(Header Options)** - Specify the name and report title. You can also **require approval for the report** (page 147).
 - **Layout** - See **Report Templates** (page 150) for a description of these options.









Note: When a legacy report definition (page 176) is added or edited, a **Parameters** tab displays instead of the **Layout** tab.

- **General** - Sets the type of report output—PDF, HTML or EXCEL—paper size and orientation. Also sets the message used to notify users when the report is run. Tokens can be included in report email messages, in both the subject line and the body of the message.
 - ✓ **<gr>** - machine group
 - ✓ **<id>** - machine id
 - ✓ **<rt>** - report name
 - ✓ **<embed>** - In the message body only, you can embed an HTML report at the specified location.

Use the edit toolbar to add images and special formatting to the text. Images must be uploaded rather than copied and pasted in.




- ✓ - Hyperlink selected text. You may need to reset links copied and pasted from another source.
- ✓ - Insert a table.
- ✓ - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
- ✓ - Indent text.
- ✓ - Outdent text.

- ✓  - Remove formatting.
 - ✓  - Insert a symbol.
 - ✓  - Insert an emoticon.
 - ✓  - Preview the display of text and images.
 - ✓  - Upload a file or image.
 - ✓  - Set selected text to subscript.
 - ✓  - Set selected text to superscript.
 - ✓  - Toggle full screen mode for editing and viewing.
- **Cover Page, Header, Footer** - Selects the **cover page, header and footer** (page 174) of the report.

Report Folder Trees

Report definitions are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:



Always Available

- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.



When a Cabinet is Selected

- **Collapse All** - Collapses all branches of the folder tree.
- **Expand All** - Expands all branches of the folder tree.

When a Folder is Selected

- **Folder Properties** - Displays in the right hand pane. Displays the owner and effective **rights** (page 108) of the folder.
- **New**
 - **Folder** - Creates a new folder underneath the selected cabinet or folder.
 - **Report** - Creates a new **custom report definition** (page 143)  in the selected folder of the folder tree.
 - **Legacy Report** - Creates a new **legacy report definition** (page 176)  in the selected folder of the folder tree.
- **Delete** - Deletes a selected folder.
- **Rename** - Renames a selected folder.
- **Share** - Applies to **Shared** cabinet folders only. Shares a folder with user roles and individual users. See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 108) topic.

When a Report Definition is Selected

- **New**
 - **Report** - Creates a new **custom report definition** (page 143)  in the selected folder of the folder tree.
 - **Legacy Report** - Creates a new **legacy report definition** (page 176)  in the selected folder of the folder tree.
- **Edit** - Edits the selected report definition.
- **Copy** - Copies the selected report definition.
- **Make Template** - Applies to custom **report definitions** (page 143) only. Saves a report definition to a selected **Report Templates** (page 150) folder. For example, users may create useful enhancements to

their own report definitions. These in turn might be worth converting into report templates that other users can base their own report definitions on.

- **Delete** - Deletes the selected report definition.
- **Run Now - Publishes a report immediately** (page 145) based on the selected report definition.
- **Schedule - Schedules publishing of a report** (page 145) based on a selected report definition.

Note: This **Schedule** button may be hidden for a standard user. This button is enabled using the **System > System Preferences > Enable Scheduling node on the User Roles - Access Rights tab** (page 366).

Publishing a Report Immediately

Select a report in one of the **report folder trees** (page 144), then click **Run Now** to display the **Data Filters** (page 145) dialog. **Run Now** reports are *not* added to the scheduled list of published reports and are displayed only to the current user.

Data Filters

Data Filters limit the data included in a report. They are shown each time the **Run Now** button is clicked and as a tab when the **Schedule** button is clicked.

- **Organization, Machine Group, Machine ID and Select View**
 - Optionally filter the selection of data included in the report by organization, machine group, machine ID or view.
 - If no view is selected, then all machine groups in all organizations you are authorized by your scope to view are selected by default.
 - **Run Now** data filtering defaults from the machine ID / group ID filter.
 - For some reports a department filter and service desk filter is available.
- **Language** - You can select the language the report is presented in. The language option does not display if language packs are not installed. See **System > Preferences** (page 353).
- **Date Filter** - For *custom* report definitions only, the following **Date Filter** options display only if—for at least one part in the configuration of the report definition—**Inherit from Report** and a *date/time column* were selected for date filtering.
 - **Predefined Ranges** - **This Week**, **Last Week**, **This Month**, **Last Month**, **This Quarter**, **Last Quarter**.
 - **Last N Days** - Enter the value of N in the **Number of Days** field.
 - **Fixed Range** - Enter a **Start DateTime** and **End DateTime**.

Scheduling / Rescheduling a Report

Select a report definition in one of the **report folder trees** (page 144), then click **Schedule** to display a dialog with four tabs. Use the dialog to schedule publication of the report in the future, once or on a recurring basis. *These settings apply only to this specific scheduling of the report. The report definition remains unchanged.* Clicking the **Submit** button publishes the report using the settings currently selected on all four tabs.

A similar **Reschedule Selected Item** dialog displays when you **Reschedule** a previously scheduled report.

- **Schedule** - Schedule the report to run once or periodically. Each type of recurrence—Once, Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence.
- **Filters** - See **Data Filters** (page 145)
- **Distribution** - Select recipients of the report.

- In the upper **Distribution** pane, by default the person running or scheduling the report is selected as an Info Center > **Inbox** (page 140) message recipient.
- You can drag and drop additional users from the lower pane into the upper **Distribution** pane. **Staff** (page 375) members must have an email address to display in lower pane.
- The users you see listed are limited to the same scope you are using as you schedule/reschedule the report.
- Any user in the upper **Distribution** pane can also be sent the same report as an email recipient.
- You can add email addresses to the **Additional Email** edit box *for users outside the same scope you are using*. Enter the email addresses manually, separated by semicolons.
- **General** - Sets the type of report output—PDF, HTML or EXCEL—paper size and orientation. Also sets the message used to notify users when the report is run. Tokens can be included in report email messages, in both the subject line and the body of the message.
 - <gr> - machine group
 - <id> - machine id
 - <rt> - report name
 - <embed> - In the message body only, you can embed an HTML report at the specified location.

Use the edit toolbar to add images and special formatting to the text. Images must be uploaded rather than copied and pasted in.



- - Hyperlink selected text. You may need to reset links copied and pasted from another source.
- - Insert a table.
- - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
- - Indent text.
- - Outdent text.
- - Remove formatting.
- - Insert a symbol.
- - Insert an emoticon.
- - Preview the display of text and images.
- - Upload a file or image.
- - Set selected text to subscript.
- - Set selected text to superscript.
- - Toggle full screen mode for editing and viewing.

Managing Scheduled Reports

Once a selected report definition is *scheduled* for publication the following actions button and table columns display in the right hand pane.









Actions

- **Run Now** - Runs a previously *scheduled* report immediately. This allows a report that has timed out, generated an error, or was unapproved to be re-run immediately without having to reselect all the schedule options over again.
- **Reschedule** - Displays the **Schedule** tab of the **Reschedule Selected Item** (page 145) dialog. Use this tab to reschedule the publishing of a selected report. *These options are the same as when you originally schedule a report.*

- **Recipients** - Displays the **Distribution** tab of the **Reschedule Selected Item** (page 145) dialog. Use this tab to change the recipients for a selected report you are rescheduling. *These options are the same as when you originally schedule a report.*
- **Delete Schedule** - Permanently deletes a selected published report. This only deletes the record of the report in **Schedule** (page 141) for your VSA logon. It does *not* delete the report for any other user.
- **History** - Displays a **Selected Item History** dialog, providing a history of all published instances of the report you have received. Click the publishing date of the report you want to see, then click the hyperlink of that report at the bottom of the dialog.
- **Refresh** - Refreshes the page.

Table Columns





This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 17).

- **(Status)**
 -  Pending
 -  Completed and Approval Required - Click the  icon to view the completed report, then approve or reject it. See **Approving / Rejecting Reports** (page 147).
 -  Completed and Rejected - Click the  icon to view the completed and rejected report. You can subsequently approve it.
 -  Completed and Distributed - Click the  icon next to the name of the report to display a **Selected Item History** dialog that contains the publishing history for that report. Click the publishing date of the report you want to see, then click the hyperlink of that report at the bottom of the dialog.
 -  Error - The report failed to publish.
- **Name** - The name of the report.
- **Owner** - The creator of the report.
- **Recurrence** - Click the recurrence—Once, Daily, Weekly, Monthly—to update the schedule.
- **Recipients** - Click the number of recipients to update the list of recipients in the **Reschedule Select Item** (page 145) dialog.
- **Recipient List** - A list of recipients.
- **Last Ran** - The last time this report was published.
- **Next Run** - The next time this report is scheduled to be published.
- **Organization, Machine Group, Machine, View** - The types of **Data Filters** (page 145) used to limit the data included in a report. Use a view to select more than one organization, machine group or machine. All machine groups in all organizations you are authorized by your scope to view are selected by default.
- **Type** - Report or Reportset
- **Status** - The status of the report in text.
- **Location** - The folder the scheduled report is located in, in the middle pane.
- **Date Created** - The date the report was scheduled.
- **Scope** - Visibility of rows in the schedule table is limited by the scope you are using. Your scope must match the scope that was current when the owner scheduled the report. This ensures that only users authorized to view the same data shown in the report can reschedule and modify recipients of the report. Email recipients can always access the completed report in email, even if they are not members of the same scope.

Approving / Rejecting Reports

Published reports can be configured to require approval before being distributed to recipients. Any user with share access and using the same scope as the one used to create the report can approve or reject the published report.

1. Check the **Needs Approval Before Distribution** checkbox in the header of a report definition.

2. Schedule the report definition to create a published report.
3. Wait for the report to display the **Completed and Approval Required**  status icon.
4. Click the  status icon to display the **Scheduled Item History** dialog.
5. Click either the **Approve** or **Reject** button.
 - Approved reports are distributed to their recipients.
 - Rejected reports display a **Completed and Rejected**  status icon. Optionally click the  status icon to display the rejected report. You can subsequently approve it.

Report and Report Set User Security

Master Users

Master users have access to any report/report set definition, provided the **Show shared and private folder contents from all users** checkbox is checked in System > **Preferences** (page 353). The rest of this topic refers to access rights for *non-master* users.

Access to Scheduling Reports and Report Sets

Other VSA users can publish or reschedule a report/report set definition created by its owner if:

- The folder containing the report/report set definition has been shared with them.
- The currently selected scope of the VSA user *matches the scope used by the owner to create the report/report set definition*.

If both conditions are true, the scheduled report/report set displays on these pages:

- **Schedule** (page 141) - Displays *all* scheduled reports and report sets you are authorized to view.
- **Reports** (page 146) - Displays all scheduled reports for the selected report definition you are authorized to view.
- **Report Sets** (page 149) - Displays all scheduled report sets for the selected report set definition you are authorized to view.

Inbox Recipients

Only VSA users matching the scope used by the owner to create the report/report set definition can be designated **Inbox** recipients of a report/report set.

Email Recipients

Even if the scope of recipient does not match the scope of the owner when the report/report set was created, recipients can view reports and report sets sent to them as email recipients. The published reports/report sets are opened as email attachments.

Setting the Report Header Logo

By default, VSA report headers display the image specified by the System > Site Customization > **Site Header** (page 394). Changing the value in the System > Configure > **Change Reporting Config...** (page 382) > **Logo** field overrides this default, changing the URL *for report headers only*. Changing the URL in the Change Reporting Config... > **Logo** field does not affect the display of the **Site Header** image.

Report Sets

[Info Center](#) > [Reporting](#) > [Report Sets](#)

A **report set** is a *collection* of **report definitions** (page 143). You can schedule a *report set definition* just like you would an individual *report definition*. This saves you the trouble of scheduling individual report definitions one at a time.

See the following topics for an overview of working with report sets.

- [Report Set Definitions](#) (page 149)
- [Report Set Folder Trees](#) (page 149)

Scheduling and managing scheduled *report sets* are the same as scheduling and managing scheduled *reports*. See:

- [Scheduling / Rescheduling a Report](#) (page 145)
- [Data Filters](#) (page 145)
- [Managing Scheduled Reports](#) (page 146)
- [Approving / Rejecting Reports](#) (page 147)
- [Report and Report Set User Security](#) (page 148)

Report Set Definitions

A **report set** is a *collection* of **report definitions** (page 143). You can schedule a *report set definition* just like you would an individual *report definition*. This saves you the trouble of scheduling individual report definitions one at a time.

Creating a New Report Set Definition

Click the **New Report Set** button to create a new report set definition. The **New Report Set** dialog displays the following tabs.

General

- **General** - Enter the report set name and description.
- **Message** - Enter the default subject line and message used to notify users when the report set is distributed.

Reports

- Check the report definitions you want to include in the report set definition.

Editing an Existing Report Set Definition

1. Click an existing report set definitions in the **report set folder trees** (page 149) in the middle pane.
2. Click the **Edit Report Set** button to edit the report set definition. The **Edit Report Set** dialog displays the same options as the **New Report Set** dialog described above.


Viewing Report Set Definition Properties

1. Click an existing report set definitions in the **report set folder trees** (page 149) in the middle pane.
2. You can view the configuration of the report set definition in the right hand pane:
 - The **Assigned Reports** section of the **Schedule** tab displays the report definitions included in the report set. You can **Assign** or **Remove** report definitions using this section.
 - The **General** tab displays the default subject line and message used to notify users when the report set is distributed.

Report Set Folder Trees

Report set definitions are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:


Always Available

- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

When a Cabinet is Selected

- **Collapse All** - Collapses all branches of the folder tree.
- **Expand All** - Expands all branches of the folder tree.

When a Folder is Selected

- **Folder Properties** - Displays in the right hand pane. Displays the owner and effective **rights** (page 108) of the folder.
- **New**
 - **Folder** - Creates a new folder underneath the selected cabinet or folder.
 - **Report Set** - Creates a new **report set definition** (page 149)  in the selected folder of the folder tree.
- **Delete** - Deletes a selected folder.
- **Rename** - Renames a selected folder.
- **Share** - Applies to **Shared** cabinet folders only. Shares a folder with user roles and individual users. See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 108) topic.

When a Report Set Definition is Selected

- **New Report Set** - Opens the report set editor to create a new report set definition in the selected folder of the folder tree.
- **Edit** - Edits the selected report set definition.
- **Delete** - Deletes the selected report set definition.
- **Schedule** - Schedules publishing of the selected report set definition.

Note: This **Schedule** button may be hidden for a standard user. This button is enabled using the **System > System Preferences > Enable Scheduling** node on the **User Roles - Access Rights** tab (page 366).

Report Templates

Info Center > Configure & Design > Report Templates

The **Report Templates** page defines *customizable* report templates. For detailed information see:

- **Folder Tree** (page 152)
- **Add / Edit Report Template** (page 153)
- **Bar Chart** (page 158)
- **Pie Chart** (page 161)
- **Table** (page 155)
- **Name Value Part** (page 163)

Terms and Concepts

- **Report Definitions** - *Report definitions* contain all the settings that determine the content, layout and file format of a report. A report is published from a **report definition** (page 143).
- **Report Templates** - A report definition is created by copying settings from a *report template*. Report templates define all the *default* settings for the content, layout and file format of a report definition. There are two types of report templates:
 - **Custom** - Customizable report templates.
 - **Legacy** - **Fixed layout report templates provided in earlier releases** (page 176).

- **Data Sets** - Customizable report templates are constructed from *data sets*. A data set is a collection of data, in table format, queried from the Kaseya Server SQL server database. Predefined data sets are listed on the **Report Parts** (page 166) page, organized by VSA module folder. For example, in the Agent module folder, the following data sets are provided:

- Agent Configuration
- Agent Portal Access
- Agent Protection Settings
- Agent Status

- **Data Columns** - Each dataset is a collection of one or more *data columns*. For example, the Agent Status data set lists the following data columns.

- agentGuid
- Computer Name
- Current User
- Group Name
- Last Logged On User
- Machine ID
- Online
- Operating System
- OS Information
- Reverse Group Name
- Show Tooltip
- Timezone Offset
- Tooltip Notes
- Transition Time

- **Report Parts** - The content and layout of a report template or report definition is constructed out of *report parts*. When constructing a *report part*, you select the columns of data in a data set you want to display in the report template or report definition. *Each part can only select columns of data from a single data set*. Each report part also determines the display of data in a particular format. There are four types of *report part formats*:

- **Tables** - Displays one or more columns of data in table format returned by a selected data set.
- **Bar Charts** - Displays a bar chart, based on two columns of data returned by a selected data set.
- **Pie Charts** - Displays a pie chart, based on two columns of data returned by a selected data set.
- **Name Value Parts** - Displays a single value with a user-defined label, based on a *custom* data set. For example: Open Tickets: 247.

Report Part Options - Each report part can be configured using the following options:

- **Aggregate Options** - Aggregate options return a single *numeric* value calculated from multiple cells in a selected column. For example, the aggregate option COUNT returns the number of non-null values in a selected column. Except for COUNT or COUNT_BIG, aggregate functions ignore null values.
- **Order by** - Data can be displayed in a preferred order, using combinations of selected columns, aggregate options, and ascending/descending sort orders.
- **Group by** - Returned rows of data can be organized into subheadings and subgroups by selecting "group by" columns. Multiple levels of "group by" columns are supported. *Applies to table parts only*.
- **Filtering** - The data displayed can be limited by specialized data filters. These include:
 - ✓ A specified number of rows or percentage of rows of data.
 - ✓ Comparing selected columns with specified values.
- **Custom Fields** - Custom agent fields—created using the Audit > **Machine Summary** (page 131) or **System Information** (page 134) pages—are supported in views, procedures, legacy reports and in

selected Audit category **reports parts** (page 166). Custom reports do not support more than 40 custom fields.

- **Coverpage, Header, Footer** - This **page** (page 175) defines presentation elements that are independent of the data displayed in the report. You can use these elements to "brand" your reports by creating a unique look and feel. Assign different combinations of coverpages, headers and footers to multiple custom report templates and custom report definitions.
- **Published / Unpublished** - A published report template can be used to create report definitions. Unpublished report templates are hidden from the list of templates available to create report definitions.
- **Make Template** - A **Make Template** button in **Reports** saves a report definition to a selected **Report Templates** folder. For example, users may create useful enhancements to their own report definitions. These in turn might be worth converting into report templates that other users can use to create report definitions.
- **Reusing Parts** - Any time after a part is configured within a template you can optionally save a part to the **Report Parts** (page 166) page This makes it a "standard" part that can be reused in templates and report definitions. You can also copy a part directly from an existing template into another template, without saving it as a "standard" part.
- **Import / Export** - Both report templates and report parts can be imported and exported using System > **Import Center** (page 388).

Folder Tree

Info Center > Configure & Design > Report Templates

Report templates are organized into a single folder tree in the middle pane underneath a **Template** cabinet. Use the following options to manage report templates in this folder tree.

Note: The categories you see when creating a new report definition (page 143) are based on the top-level folders in the **Report Templates** (page 150) folder tree. By default a top-level folder is created for each installed module.

When the Templates Cabinet is Selected

- **Collapse All** - Collapses all branches of the folder tree.
- **Expand All** - Expands all branches of the folder tree.

When a Folder is Selected

A folder for each installed module has been created for you. You can use these or create your own.

- **Add Folder** - Adds a report template folder with a specified name.
- **Add** - Adds a report template in the selected folder.
- **Share** - Shares a folder with user roles and individual users. See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 108) topic.

When a Template is Selected

- **Add** - Adds (page 153) a new report template in the selected folder.
- **Edit** - Edits (page 153) a selected report template.

Note: System report templates  cannot be edited or deleted but can be copied.

- **Delete** - Deletes a selected report template.
- **Rename** - Renames a selected report template.

- **Publish / Unpublish** - Toggles between these two states. Clicking **Publish** enables a report template to be used to create a **report definition** (page 143). Clicking **Unpublish** prevents a report template from being used to create a report definition.
- **Copy** - Creates a copy of an existing report template.
- **Preview** - Generates a report for the current user only, based on a selected report template.

Add / Edit Report Template

Info Center > Configure & Design > Report Templates > Add Report Template / Edit

Report Design Description

- **Name** - The name of the report template.
- **Template Title** - The title displayed.

Note: See **Report Definitions** (page 143) for a description of options on the **General** tab and **Cover Page, Header** and **Footer** tab.

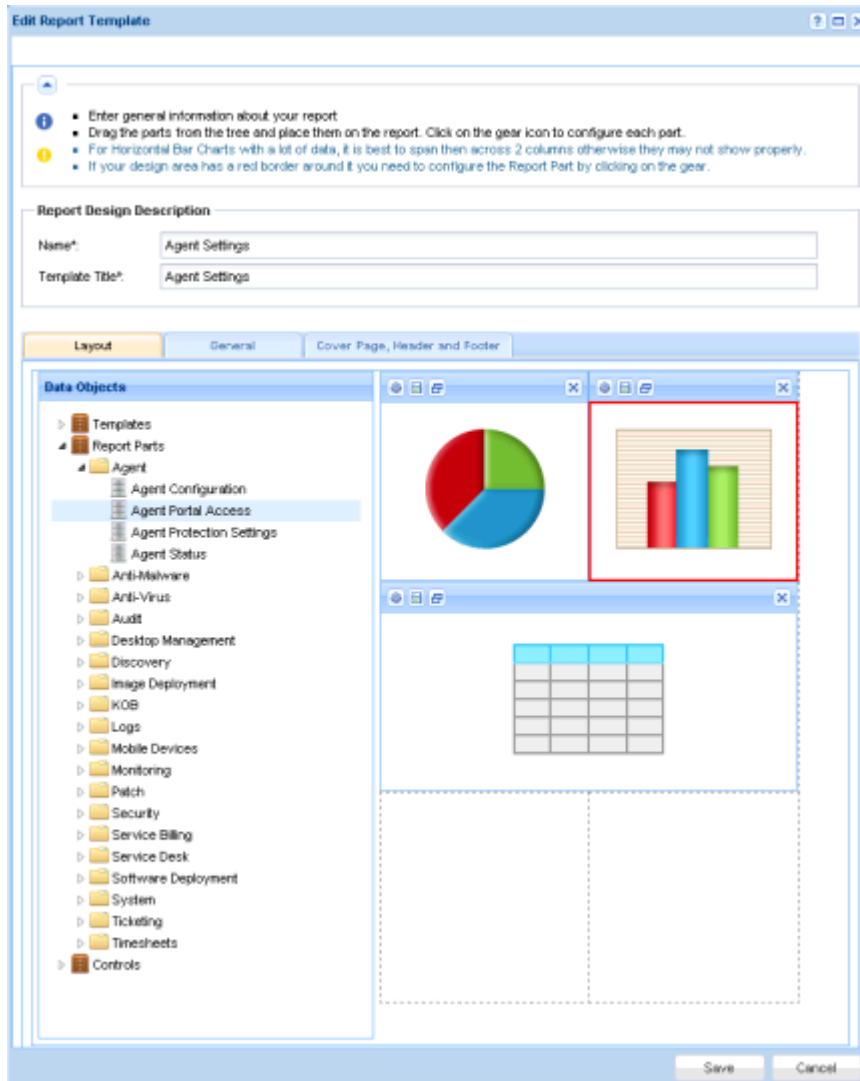
Layouts tab

In the left hand pane, the **Layouts** tab displays a folder tree of data sets. A two-column table displays in the right hand pane. You can drag-and-drop data sets from the folder tree into any of the cells of the two-column table. *A data set can only occupy one or both cells of a single row.* A report part displays data returned by a data set in a specific format. There are four types of report part formats:

- **Tables** - Displays one or more columns of data in table format returned by a selected data set.
- **Bar Charts** - Displays a bar chart, based on two columns of data returned by a selected data set.
- **Pie Charts** - Displays a pie chart, based on two columns of data returned by a selected data set.
- **Name Value Parts** - Displays a single value with a user-defined label, based on a *custom* data set.

Info Center

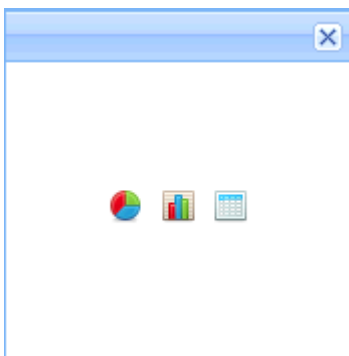
A folder tree of existing templates also displays in the left hand pane. You can drag and drop a part from an existing template into the right hand pane, then modify this new copy of the part for your new template. The source template remains unchanged.




Adding a Report Part to a Layout



1. Drag-and-drop a data set from the folder tree in the left hand pane into one of the cells in the right hand pane.

2. Select the report part format. You can not switch formats after you make this selection. You can delete the report part, re-add it, then select a different format.



3. Click the gear icon  or double-click the cell to configure the report part. The report template cannot be saved until a report part has been configured at least once. Unconfigured report parts display a red box around their cells.



4. Configuring a report part depends on the type of report part selected. See:
 - [Table](#) (page 155)
 - [Bar Chart](#) (page 158)
 - [Pie Chart](#) (page 161)
 - [Name Value Part](#) (page 163)
5. Use the Resize  icon to expand a report part into two cells on a single row or collapse it back to a single cell. *Expanding a report part into multiple rows is not supported.*
6. Any time after a part is configured within a template you can optionally save a part to the [Report Parts](#) (page 166) page by clicking the save icon . This makes it a "standard" part that can be used in templates and report definitions.

Table

Info Center > Configure & Design > Report Templates > Add Report Template / Edit > Gear Icon

A [Table](#) is configured using a three step wizard:

- Step 1 - Select Columns
- Step 2 - Ordering and Grouping
- Step 3 - Filtering

Step 1 - Select Columns

Format

- **Dataset Name** - The name of the data set associated with this table.
- **Title** - Enter a title for the report part.
- **Title Alignment** - Left, Right, Center
- **Show Title** - If checked, the title displays on the published report with this report part. If blank, the title is hidden.
- **Page Break** - If enabled, forces a page break next to this report part. Options include No Page Break, Before, After, Before and After. A break in either cell, before or after, has precedence over no break in the other cell. An After page break is ignored if a table runs beyond the length of the page in the other cell.
- **Text Size** - Extra Small, Small, Normal, Large.

Columns / Column Selections

Drag-and-drop columns from the **Columns** list to the **Column Selections** list.

- **Delete Row** - Removes a selected column from the list.
- **Column** - A column selected for inclusion in the published report.
- **Alias** - Displays as the heading for a selected column, in place of the column name.
- **Aggregate** - Aggregate options return a single *numeric* value calculated from multiple cells in a selected column. For example, the aggregate option **COUNT** returns the number of non-null values in a selected column. Except for **COUNT** or **COUNT_BIG**, aggregate functions ignore null values.
 - **AVG** - Returns the average of the values in a group. Null values are ignored.
 - **COUNT / COUNT_BIG** - Returns the number of items in a group. **COUNT** works like the **COUNT_BIG** function. The only difference between the two functions is their return values. **COUNT** always returns an *int* data type value. **COUNT_BIG** always returns a *bigint* data type value.
 - **MAX** - Returns the maximum value in a group.
 - **MIN** - Returns the minimum value in a group.
 - **STDEV** - Returns the statistical standard deviation of all values in a group.
 - **STDEVP** - Returns the statistical standard deviation for the population for all values in a group.
 - **SUM** - Returns the sum of all the values in a group. **SUM** can be used with numeric columns only. Null values are ignored.
 - **VAR** - Returns the statistical variance of all values in a group.
 - **VARP** - Returns the statistical variance for the population for all values in a group.
- **Weight** - Determines the percentage width of each column by assigning a numerical value. For example, if four rows are sequentially weighted with the values 4, 3,2,1, then,
 - The first row, with a weight of 4, is 40% of the sum of all weight values, 10.
 - The second row, with a weight of 3, is 30% of the sum of all weight values, 10.
 - The third row, with a weight of 2, is 20% of the sum of all weight values, 10.
 - The fourth row, with a weight of 1, is 10% of the sum of all weight values, 10.

Step 2 - Ordering and Grouping

Order by

Determines the order data is displayed, from first to last. Multiple rows can be configured, with a higher row having precedence over a lower row. A selected order by column does not have to be displayed in the report.

- **Add Row** - Adds an order by row.
- **Delete Row** - Deletes an order by row.
- **Column** - Selects a column used to determine the order data displayed, from first to last.

- **Aggregate** - If an aggregate option is selected, the sort order is applied to the numeric value returned by the aggregate option instead of the selected column. See the description for each aggregation option described above.
- **Sort Order** - *Ascending* or *Descending*. Applies to either the selected column or to the aggregate option, if one is specified.

Group by

Returned rows of data can be organized into subheadings and subgroups by selecting "group by" columns. Multiple levels of "group by" columns are supported. Applies to table parts only.

- **Add Row** - Adds a group by row.
- **Delete Row** - Deletes a group by row.
- **Column** - The column selected to group returned rows of data.

Step 3 - Filters

The data displayed can be limited by specialized data filters.

Note: Additional filtering options display when a report definition or report template is run or scheduled.

Row Filter

- **Limit Type** - The type of row limit specified.
 - **Top N** - Limits data returned to the first N number of rows returned. Example: If the **Limit** is 10, the first 10 rows of 300 rows available are returned. Result: 10 rows are returned.
 - **Top N %** - Limits data returned to the first N % of rows returned. Example: If the **Limit** is 10 the first 10% of 300 available rows are returned. Result: 30 rows are returned.
- **Limit** - The number specified for the **Limit Type** field.
- **Select Distinct** - If checked, duplicate rows are not returned. For all columns displayed in the report, the values in a row must match the values of another row to be considered a duplicate.

Date Filter

Date filters only display if date/time columns are included in the report part.

- **Date Filter Column** - Select a date/time column to filter the data queried by this part of the report.

Note: You must select a date/time column for the other date filter options below to have any effect.

- **Time Range Type** - Select a time period to filter the data queried for this part of the report.
 - **Predefined Ranges** - **This Week**, **Last Week**, **This Month**, **Last Month**, **This Quarter**, **Last Quarter**.
 - **Inherit from Report** - When you schedule or run a report, **Date Filter** options display on the **Filters** tab and determine the time period used to query data for this part of the report.
 - **Last N Days** - Enter the value of N in the **Number of Days** field.
 - **Fixed Range** - Enter a **Start DateTime** and **End DateTime**.
- **Number of Days** - Enter the value of N in this field if **Last N Days** was selected.
- **Start DateTime** - Select a start date and time if **Fixed Range** was selected.
- **End DateTime** - Select the end date and time if **Fixed Range** was selected.

Advanced Filters

Rows can be limited by comparing selected columns with specified values.

- **Add Row** - Adds a comparison row.
- **Delete Row** - Deletes a comparison row.
- **Field** - Selects a column used to compare with a specified value.

- **Operator** - The operator used to compare a selected column with a specified value.
 - **Equal (=)** Enter a comma separated list of values to create an OR statement.
 - **Not Equal (!=)** Enter a comma separated list of values to create an OR statement.
 - **Like** - If a selected column contains this specified value as a substring, then display this row. Enter a comma separated list of values to create an OR statement.
 - **Not Like** - If a selected column does not contain this specified value as a substring, then display this row. Enter a comma separated list of values to create an OR statement.
 - **Greater Than (>)**
 - **Greater Than or Equal (>=)**
 - **Less Than (<)**
 - **Less Than Or Equal (<=)**
 - **Between** - If the selected column is between two *string* values, separated by a comma, display this row. Comparison is from left to right. Examples:
 - ✓ Number field format - 1000,9999
 - ✓ String field format - aaa,zzz
 - ✓ Date field format - 01-01-2014,03-31-2014
 - **Is Empty** - If the selected column does not have characters, display this row.
 - **Is Null** - If the selected column is null, display this row.
 - **Not Empty** - If the selected column has characters, display this row.
 - **Not Null** - If a selected column is not null, display this row.
- **Value** - The specified value.

Bar Chart

Info Center > Configure & Design > Report Templates > Add Report Template / Edit > Gear Icon

A **Bar Chart** is configured using a two step wizard:

- Step 1 - Layout
- Step 2 - Filtering

Step 1 - Layout

Title

- **Dataset Name** - The name of the data set associated with this table.
- **Show Title on Report** - If checked, the title displays on the published report with this report part. If blank, the title is hidden.
- **Title** - Enter a title for the report part.
- **Description** - A description of the report part.

Format

- **Bar Chart Type** - The orientation and shape of the bars in the chart.
 - **Vertical Bar**
 - **Vertical Cylinder Bar**
 - **Horizontal Bar**
 - **Horizontal Cylinder Bar**

Note: Horizontal bar charts may require both columns of the report layout to display data correctly.

- **Show Chart in 3D** - If checked, the chart is 3 dimensional. Cylinder bar options must be 3 dimensional.
- **Page Break** - If enabled, forces a page break next to this report part. Options include No Page Break, Before, After, Before and After. A break in either cell, before or after, has precedence over no break in the other cell. An After page break is ignored if a table runs beyond the length of the page in the other cell.
- **Do not show the axis titles** - If checked, axis titles are not displayed.

Data Properties

- **Bar Category** - Any column in the data set that you want to display varying numerical data for. For example, you could display a numerical value for each machine group included in the published report.
- **Bar Value** - Any other column in the data set that can be represented numerically. **A value must either be numeric or evaluate to numeric as the result of an aggregation.** If a *non-numeric* column is selected, you can only use COUNT, or COUNT_BIG as aggregates.
- **Alias** - Displays as the heading for a selected column, in place of the column name.
- **Aggregate** - Aggregate options return a single *numeric* value calculated from multiple cells in a selected column. For example, the aggregate option COUNT returns the number of non-null values in a selected column. Except for COUNT or COUNT_BIG, aggregate functions ignore null values.
 - **AVG** - Returns the average of the values in a group. Null values are ignored.
 - **COUNT / COUNT_BIG** - Returns the number of items in a group. COUNT works like the COUNT_BIG function. The only difference between the two functions is their return values. COUNT always returns an *int* data type value. COUNT_BIG always returns a *bigint* data type value.
 - **MAX** - Returns the maximum value in a group.
 - **MIN** - Returns the minimum value in a group.
 - **STDEV** - Returns the statistical standard deviation of all values in a group.
 - **STDEVP** - Returns the statistical standard deviation for the population for all values in a group.
 - **SUM** - Returns the sum of all the values in a group. SUM can be used with numeric columns only. Null values are ignored.
 - **VAR** - Returns the statistical variance of all values in a group.
 - **VARP** - Returns the statistical variance for the population for all values in a group.

Order by

Determines the order data is displayed, from first to last. Multiple rows can be configured, with a higher row having precedence over a lower row. A selected order by column does not have to be displayed in the report.

- **Add Row** - Adds an order by row.
- **Delete Row** - Deletes an order by row.
- **Column** - Selects a column used to determine the order data displayed, from first to last.
- **Aggregate** - If an aggregate option is selected, the sort order is applied to the numeric value returned by the aggregate option instead of the selected column. See the description for each aggregation option described above.
- **Sort Order** - *Ascending* or *Descending*. Applies to either the selected column or to the aggregate option, if one is specified.

Step 2 - Filters

The data displayed can be limited by specialized data filters.

Note: Additional filtering options display when a report definition or report template is run or scheduled.

Row Filter

- **Limit Type** - The type of row limit specified.
 - **Top N** - Limits data returned to the first N number of rows returned. Example: If the **Limit** is 10, the first 10 rows of 300 rows available are returned. Result: 10 rows are returned.
 - **Top N %** - Limits data returned to the first N % of rows returned. Example: If the **Limit** is 10 the first 10% of 300 available rows are returned. Result: 30 rows are returned.
- **Limit** - The number specified for the **Limit Type** field.
- **Select Distinct** - If checked, duplicate rows are not returned. For all columns displayed in the report, the values in a row must match the values of another row to be considered a duplicate.

Date Filter

Date filters only display if date/time columns are included in the report part.

- **Date Filter Column** - Select a date/time column to filter the data queried by this part of the report.

Note: You must select a date/time column for the other date filter options below to have any effect.

- **Time Range Type** - Select a time period to filter the data queried for this part of the report.
 - **Predefined Ranges** - This Week, Last Week, This Month, Last Month, This Quarter, Last Quarter.
 - **Inherit from Report** - When you schedule or run a report, **Date Filter** options display on the **Filters** tab and determine the time period used to query data for this part of the report.
 - **Last N Days** - Enter the value of N in the **Number of Days** field.
 - **Fixed Range** - Enter a **Start DateTime** and **End DateTime**.
- **Number of Days** - Enter the value of N in this field if **Last N Days** was selected.
- **Start DateTime** - Select a start date and time if **Fixed Range** was selected.
- **End DateTime** - Select the end date and time if **Fixed Range** was selected.

Advanced Filters

Rows can be limited by comparing selected columns with specified values.

- **Add Row** - Adds a comparison row.
- **Delete Row** - Deletes a comparison row.
- **Field** - Selects a column used to compare with a specified value.
- **Operator** - The operator used to compare a selected column with a specified value.
 - **Equal (=)** Enter a comma separated list of values to create an OR statement.
 - **Not Equal (!=)** Enter a comma separated list of values to create an OR statement.
 - **Like** - If a selected column contains this specified value as a substring, then display this row. Enter a comma separated list of values to create an OR statement.
 - **Not Like** - If a selected column does not contain this specified value as a substring, then display this row. Enter a comma separated list of values to create an OR statement.
 - **Greater Than (>)**
 - **Greater Than or Equal (>=)**
 - **Less Than (<)**
 - **Less Than Or Equal (<=)**

- **Between** - If the selected column is between two *string* values, separated by a comma, display this row. Comparison is from left to right. Examples:
 - ✓ Number field format - 1000,9999
 - ✓ String field format - aaa,zzz
 - ✓ Date field format - 01-01-2014,03-31-2014
- **Is Empty** - If the selected column does not have characters, display this row.
- **Is Null** - If the selected column is null, display this row.
- **Not Empty** - If the selected column has characters, display this row.
- **Not Null** - If a selected column is not null, display this row.
- **Value** - The specified value.

Pie Chart

Info Center > Configure & Design > Report Templates > Add Report Template / Edit > Gear Icon

A **Pie Chart** is configured using a two step wizard:

- Step 1 - Layout
- Step 2 - Filtering

Step 1 - Layout

Title

- **Title** - Enter a title for the report part.
- **Show Title on Report** - If checked, the title displays on the published report with this report part. If blank, the title is hidden.

Format

- **Pie Chart Type** - The orientation and shape of the pie chart.
 - **Standard Pie**
 - **Exploded Pie**
- **Show Chart in 3D** - If checked, the chart is 3 dimensional.
- **Page Break** - If enabled, forces a page break next to this report part. Options include No Page Break, Before, After, Before and After. A break in either cell, before or after, has precedence over no break in the other cell. An After page break is ignored if a table runs beyond the length of the page in the other cell.
- **Display Pie Value inside of the Pie Graphic** - If checked, values display inside each wedge of the pie chart. If blank, the values display as callouts around the edge of the pie chart.

Data Properties

- **Category** - Any column in the data set that you want to display varying numerical data for. For example, you could display a numerical value for each machine group included in the published report.
- **Value** - Any other column in the data set that can be represented numerically. **A value must either be numeric or evaluate to numeric as the result of an aggregation.** If a *non-numeric* column is selected, you can only use COUNT, or COUNT_BIG as aggregates.
- **Alias** - Displays as the heading for a selected column, in place of the column name.

- **Aggregate** - Aggregate options return a single *numeric* value calculated from multiple cells in a selected column. For example, the aggregate option **COUNT** returns the number of non-null values in a selected column. Except for **COUNT** or **COUNT_BIG**, aggregate functions ignore null values.
 - **AVG** - Returns the average of the values in a group. Null values are ignored.
 - **COUNT / COUNT_BIG** - Returns the number of items in a group. **COUNT** works like the **COUNT_BIG** function. The only difference between the two functions is their return values. **COUNT** always returns an *int* data type value. **COUNT_BIG** always returns a *bigint* data type value.
 - **MAX** - Returns the maximum value in a group.
 - **MIN** - Returns the minimum value in a group.
 - **STDEV** - Returns the statistical standard deviation of all values in a group.
 - **STDEVP** - Returns the statistical standard deviation for the population for all values in a group.
 - **SUM** - Returns the sum of all the values in a group. **SUM** can be used with numeric columns only. Null values are ignored.
 - **VAR** - Returns the statistical variance of all values in a group.
 - **VARP** - Returns the statistical variance for the population for all values in a group.

Order by

Determines the order data is displayed, from first to last. Multiple rows can be configured, with a higher row having precedence over a lower row. A selected order by column does not have to be displayed in the report.

- **Add Row** - Adds an order by row.
- **Delete Row** - Deletes an order by row.
- **Column** - Selects a column used to determine the order data displayed, from first to last.
- **Aggregate** - If an aggregate option is selected, the sort order is applied to the numeric value returned by the aggregate option instead of the selected column. See the description for each aggregation option described above.
- **Sort Order** - **Ascending** or **Descending**. Applies to either the selected column or to the aggregate option, if one is specified.

Step 2 - Filters

The data displayed can be limited by specialized data filters.

Note: Additional filtering options display when a report definition or report template is run or scheduled.

Row Filter

- **Limit Type** - The type of row limit specified.
 - **Top N** - Limits data returned to the first N number of rows returned. Example: If the **Limit** is 10, the first 10 rows of 300 rows available are returned. Result: 10 rows are returned.
 - **Top N %** - Limits data returned to the first N % of rows returned. Example: If the **Limit** is 10 the first 10% of 300 available rows are returned. Result: 30 rows are returned.
- **Limit** - The number specified for the **Limit Type** field.
- **Select Distinct** - If checked, duplicate rows are not returned. For all columns displayed in the report, the values in a row must match the values of another row to be considered a duplicate.

Date Filter

Date filters only display if date/time columns are included in the report part.

- **Date Filter Column** - Select a date/time column to filter the data queried by this part of the report.

Note: You must select a date/time column for the other date filter options below to have any effect.

- **Time Range Type** - Select a time period to filter the data queried for this part of the report.
 - **Predefined Ranges** - This Week, Last Week, This Month, Last Month, This Quarter, Last Quarter.
 - **Inherit from Report** - When you schedule or run a report, **Date Filter** options display on the **Filters** tab and determine the time period used to query data for this part of the report.
 - **Last N Days** - Enter the value of N in the **Number of Days** field.
 - **Fixed Range** - Enter a **Start DateTime** and **End DateTime**.
- **Number of Days** - Enter the value of N in this field if **Last N Days** was selected.
- **Start DateTime** - Select a start date and time if **Fixed Range** was selected.
- **End DateTime** - Select the end date and time if **Fixed Range** was selected.

Advanced Filters

Rows can be limited by comparing selected columns with specified values.

- **Add Row** - Adds a comparison row.
- **Delete Row** - Deletes a comparison row.
- **Field** - Selects a column used to compare with a specified value.
- **Operator** - The operator used to compare a selected column with a specified value.
 - **Equal (=)** Enter a comma separated list of values to create an OR statement.
 - **Not Equal (!=)** Enter a comma separated list of values to create an OR statement.
 - **Like** - If a selected column contains this specified value as a substring, then display this row. Enter a comma separated list of values to create an OR statement.
 - **Not Like** - If a selected column does not contain this specified value as a substring, then display this row. Enter a comma separated list of values to create an OR statement.
 - **Greater Than (>)**
 - **Greater Than or Equal (>=)**
 - **Less Than (<)**
 - **Less Than Or Equal (<=)**
 - **Between** - If the selected column is between two *string* values, separated by a comma, display this row. Comparison is from left to right. Examples:
 - ✓ Number field format - 1000,9999
 - ✓ String field format - aaa,zzz
 - ✓ Date field format - 01-01-2014,03-31-2014
 - **Is Empty** - If the selected column does not have characters, display this row.
 - **Is Null** - If the selected column is null, display this row.
 - **Not Empty** - If the selected column has characters, display this row.
 - **Not Null** - If a selected column is not null, display this row.
- **Value** - The specified value.

Name Value Part


A **name value part** is a type of data object that can be added to a report template or report definition. A *name value part displays a single value, along with a user-defined label, based on a custom data set.* These custom data sets are defined using the **Name Value Parts** (page 167) page. For example you might want to create a list of single value counts for ticket status.

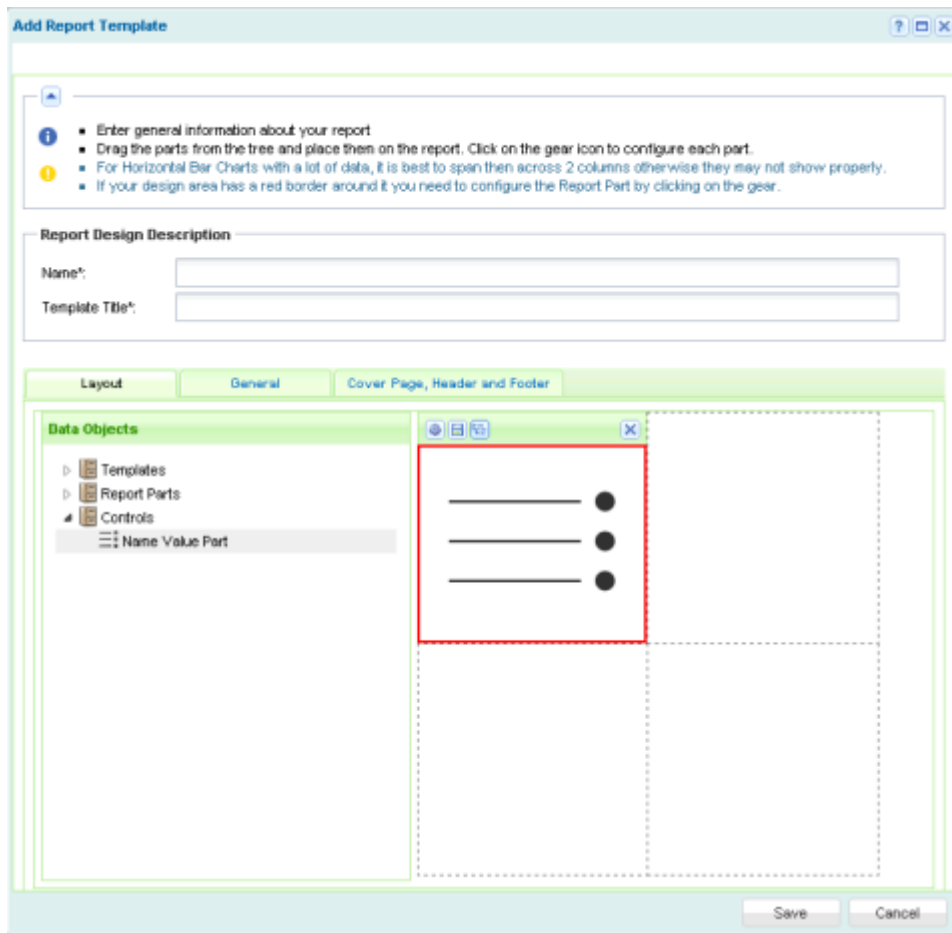
Info Center

Tickets Created Last <N> Days
Total Tickets Past Due
Tickets Closed Last <N> Days
Total Open Tickets

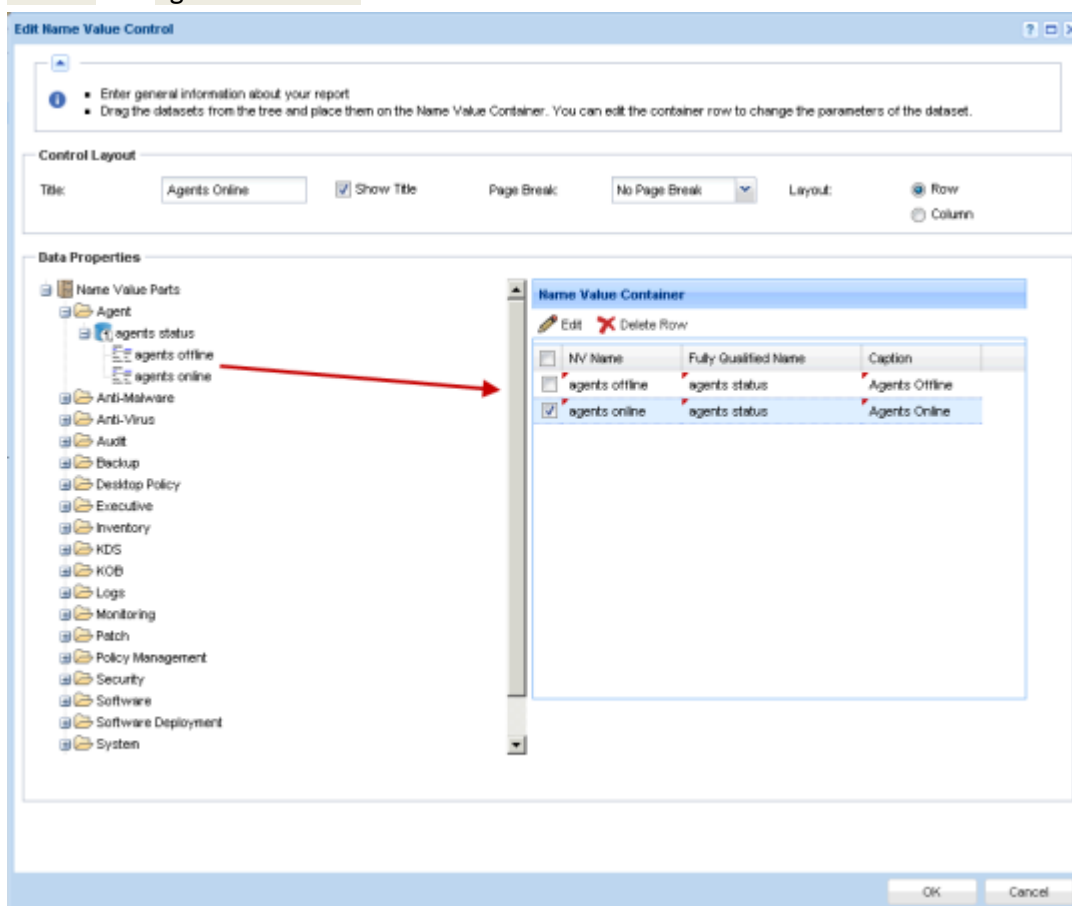
Note: Creating or editing of name value parts is not supported on the Kaseya Cloud platform. All Cloud-based accounts can use pre-defined name value parts via the Control cabinet when creating a report template or a new custom report.

Adding a Name Value Part to a Layout

1. Drag-and-drop a name value part from the folder tree in the left hand pane in to one of the cells in the right hand pane.
2. Click the gear icon  to configure the name value part. The report template cannot be saved until the name value part has been configured at least once. Unconfigured name value parts display a red box around their cells.



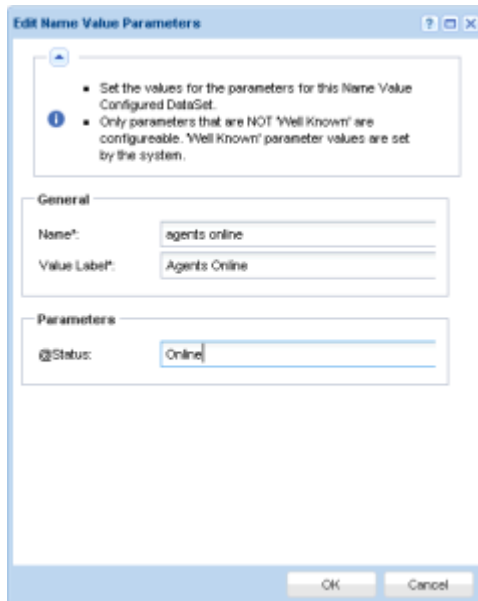
3. Drag-and-drop a name value part from the folder tree in the left hand pane into the **Name Value Container** list in the right hand pane. You can drop multiple instances of the same name value part into the same list. For example a **Name Value Container** list can include two instances: Agents Online and Agents Offline.



You can optionally edit an instance. Let's assume you want to change the Agents Offline instance to Agents All.

4. Select the row of the instance you want to edit in the **Name Value Container** list.
5. Click **Edit**. Any changes you make only applies to this instance in the report template or report definition you are editing.
 - **Name** - The name displayed by this **Name Value Instance** in configuration dialogs.
 - **Name Label** - The label displayed in the report with its corresponding value.
 - **Parameters** - One or more parameters that determine the value returned for this name value part when a report is published. The values a parameter can have are determined by the query or stored procedure specified using the **Name Value Parts** (page 167) page.

Note: Hover the cursor over each parameter's name to see a tooltip description of the acceptable values for that parameter.



Report Parts

Info Center > Configure & Design > Report Parts

The **Report Parts** page lists all pre-defined data sets used in custom reports. This page also enables you to configure report parts outside of a report template or report definition. Report parts defined using this page provide *default "standard" configurations* for report parts added to report templates and report definitions.

Note: See [Report Templates](#) (page 150) for a list of terms and concepts used in this topic.

Custom Fields

Custom agent fields—created using the Audit > [Machine Summary](#) (page 131) or [System Information](#) (page 134) pages—are supported in views, procedures, legacy reports and in selected Audit category reports parts. Custom reports do not support more than 40 custom fields.

Folder Tree

Each module folder in the folder tree lists one or more data sets appropriate to that module. Click any data set in the folder tree to see the columns and column descriptions included in that data set. Clicking an existing report part displays its current configuration in table format in the right hand pane.

When the Cabinet is Selected

- **Collapse All** - Collapses all branches of the folder tree.
- **Expand All** - Expands all branches of the folder tree.

When a Folder is Selected

- No actions are available.

When a Data Set is Selected

- **New** - Creates a report part, based on a selected data set.
 - **Table** - Adds a **Table** (page 155) report part.
 - **Bar Chart** - Adds a **Bar Chart** (page 158) report part.
 - **Pie Chart** - Adds a **Pie Chart** (page 161) report part.

When a Report Part is Selected

- **New** - Creates a report part, based on a selected data set.
 - **Table** - Adds a **Table** (page 155) report part.
 - **Bar Chart** - Adds a **Bar Chart** (page 158) report part.
 - **Pie Chart** - Adds a **Pie Chart** (page 161) report part.
- **Edit** - Edits a selected report part.
- **Delete** - Deletes a selected report part.
- **Rename** - Renames a selected report part.
- **Preview** - Generates a preview of the report part.

Name Value Parts

Info Center > Configure & Design > Name Value Parts

The **Name Value Parts** page creates a custom data set that returns a single value from the SQL database at the time a report is published. The value is displayed with a user-defined, descriptive name on a report. For example, a name value part called **OnlineAgents** could return a single number: a count of all online agents that match the filtering selected for the report. For detailed information see:

- **Folder Tree** (page 168)
- **Add / Edit Data Set** (page 168)
- **Well Known Parameters** (page 170)
- **Report Contexts** (page 173)
- **Name Value Instances** (page 174)

Note: Creating or editing of name value parts is not supported on the Kaseya Cloud platform. All Cloud-based accounts can use pre-defined name value parts via the Control cabinet when creating a report template or a new custom report.

Terms and Concepts

- **Name Value Control** - Name value parts are added to a **Name Value Part** (page 163) cabinet on the **Report Templates** page. Each **Name Value Control** in a report template can display a set of **Name Value Parts** in row or column format. For example, you could create a **Ticket Status** section of the report that shows a series of counts, one for each of the following "names":
 - Tickets Created Last <N> Days
 - Total Tickets Past Due
 - Tickets Closed Last <N> Days
 - Total Open Tickets
- **Parameters** - Each name value part can be passed a number of parameters. Parameters must have default arguments. The argument of a user-defined parameter is entered or confirmed by the user when the report is published.
- **Well Known Parameters** - Certain parameters are already "well known" to the system and do not have to be defined by the user or provided an argument when the report is published. See **Well Known Parameters** (page 170).

- **Name Value Instance** - An instance stores the arguments assigned to user-defined parameters of a custom data set. These name value instances can be added to a name value control, bypassing the need to enter arguments manually each time a report template is created.

Folder Tree

Info Center > Configure & Design > Name Value Parts

Name value parts are organized into a single folder tree in the middle pane underneath a **Name Value Parts** cabinet. Use the following options to manage name value parts in this folder tree.

When the Name Value Parts Cabinet is Selected

- **Collapse All** - Collapses all branches of the folder tree.
- **Expand All** - Expands all branches of the folder tree.

When a Folder is Selected

A folder for each installed module has been created for you. You can use these or create your own.

- **New Data Set - Adds** (page 168) a custom data set in the selected folder.

When a Data Set is Selected

- **Edit Data Set - Edits** (page 168) a selected custom data set.
- **Add Name Value Instance** - Adds a name value instance in the selected folder.
- **Delete** - Deletes a custom data set.

When a Name Value Instance is Selected

- **Edit** - Edits a name value instance.
- **Delete** - Deletes a name value instance.

Add / Edit Data Set

Info Center > Configure & Design > Name Value Parts > New Data Set or Edit Data Set

The **New Data Set** or **Edit Data Set** window specifies the custom data set used to return a single value from a SQL database. The custom data set uses either a SQL select statement or a stored procedure to return data. The value in a selected column, returned by the first row of data, is the value displayed in the report.

Action

- **Create Registration File** - Once you have added or edited a name value part using this dialog:
 1. Click **Create Registration File**. A link to a generated data set XML displays on the subsequent dialog page.
 2. Download the data set XML and place it in the following location:
`\<KServerInstallDirectory>\Xml\Reporting\Custom\DataSetRegistration\1`
 3. Click the System > Server Management > Configure > **Change Reporting Configuration** (page 382) > **Run Registration** button to register the new or modified data part XML with your VSA.

Properties

- **Name** - The name of the custom data set.
- **Description** - A longer description of the custom data set.
- **Category** - The **Name Value Parts** folder, typically corresponding to a module, that a custom data set is located in.

SQL Definition

- **Return Column** - The data column in the SQL select statement that contains the value that will be used in the published report. The value in the first row of data returned is used.
- **Caption** - The caption displayed with the value on the published report.
- **Data Type** - The data type returned. This data type must be compatible with the data type of the data column in the SQL select statement.
 - STRING
 - INT
 - DECIMAL
 - DATE
 - BOOLEAN
- **Context** - Determines the type of filter displayed just before a report is generated. The context should be compatible with the data returned by the SQL definition. For example, if the data returned by the SQL definition supports filtering primarily by agent machines, then the selected context should be `MachineFilter`.
 - `MachineFilter`
 - `ServiceDeskFilter`
 - `AssetsFilter`
 - `DevicesFilter`
 - `MobileDevicesFilter`
 - `TicketingFilter`
- **Text** - A SQL select statement that returns one or more columns of data. Only the first row of data returned by the SQL select statement is used.
- **Stored Procedure** - The name of a stored procedure and any user defined parameters. Only the first row of data returned by the stored procedure is used.

Parameters

User-defined parameters specified by a SQL select statement or stored procedure must be registered here. This enables report templates and name value parts to display these parameters in configuration dialogs.

Actions

- **Add Row** - Adds a parameter row.
- **Delete Row** - Deletes a selected parameter row.

Columns

- **Param Name** - The name of the parameter.
- **Param Value** - The default value for the parameter.
- **Param Type** - The data type of the parameter.
 - STRING
 - INT
 - DECIMAL
 - DATE
 - BOOLEAN
- **Size** - The size of the parameter.
- **Description** - Enter a description of the acceptable values supported by this parameter. When selecting a different value for a parameter, users can reference this description by hovering the cursor over a parameter's name to display its tooltip.

Well Known Parameters

When creating name value parts, you can include **Well Known** parameters in your queries. You insert these in SQL queries using the format `@<wellknownname>`. You must also add them to the parameters table. The following are the well known values you can use:

- `@LogoURL` - The URL to the logo used on the report.
- `@ViewID` - The ID for the view selected when the report was created, or -1.
- `@AdminID` - The ID of the VSA user running the report.
- `@CompanyName` - The organization name set for MyOrg.
- `@EffectiveDate` - The date the report is run, adjusted for time zone.
- `@PartitionID` - The ID of the partition running the report.
- `@ReportDate` - The date the report is run, adjusted for time zone.
- `@ReportTitle` - The title of the report as set when the report was created.
- `@ScopeID` - The ID of the scope the report is run under.
- `@RoleID` - The ID of the role the report is run under.
- `@ReportSessionId` - The ID used for a run of a report. It is used to JOIN to a selected **context** (*page 173*) table. You *must* choose a context from the drop-down when using `@ReportSessionId`.
- `@LangID` - The ID of the language used for the report.
- `@StartDateTime` – A special date parameter, that when used in conjunction with `@EndDateTime` lets you set the date range at report run time.
- `@EndDateTime` - A special date parameter, that when used in conjunction with `@StartDateTime` lets you set the date range at report run time.

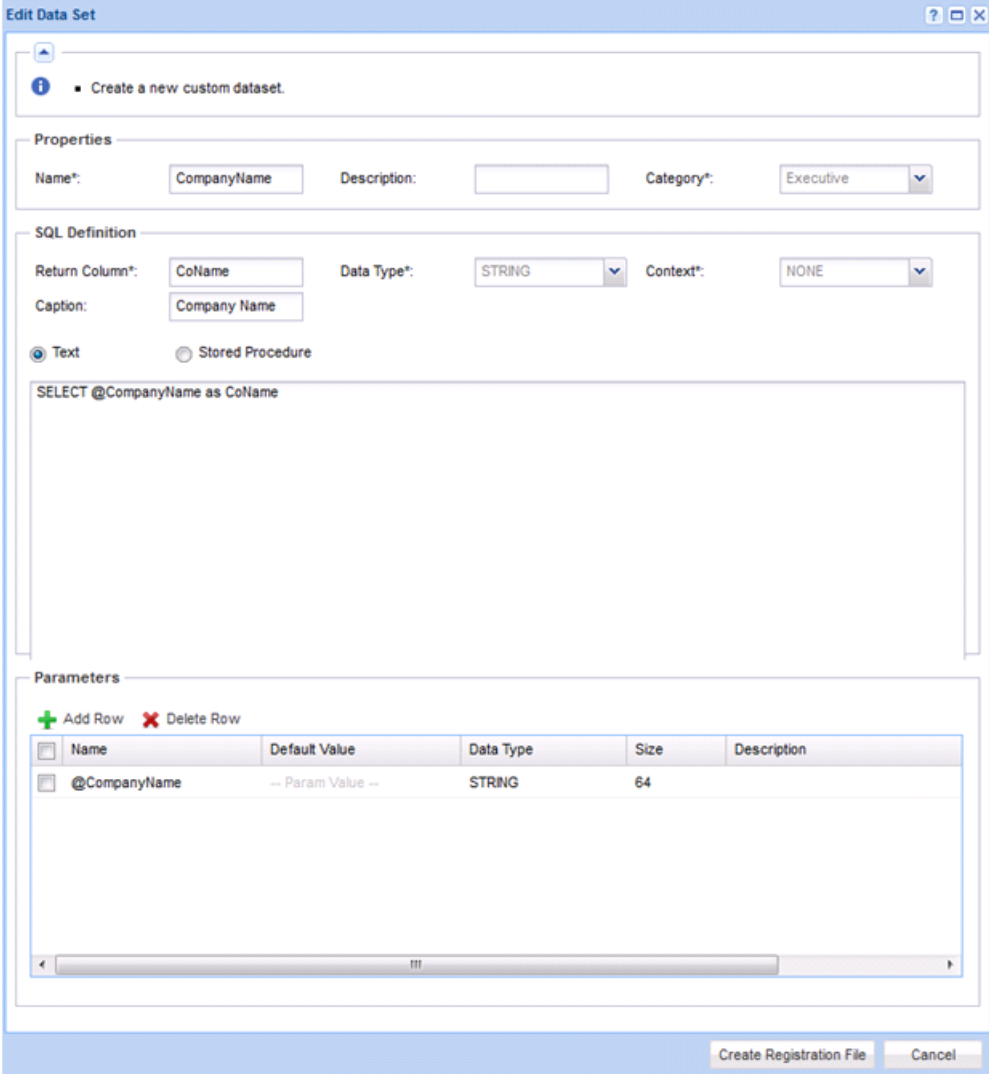
ReportSessionID

If you are using a context, then include a `@ReportSessionId` parameter as the value for one of the parameters.

Examples

Here are some examples of how to make name value parts using well known parameters.

1. This name value part uses @CompanyName to return the company name.



2. This name value part uses @PartitionID to return the machine with the lowest disk space in the partition ID.

The screenshot shows the 'Edit Data Set' dialog box with the following configuration:

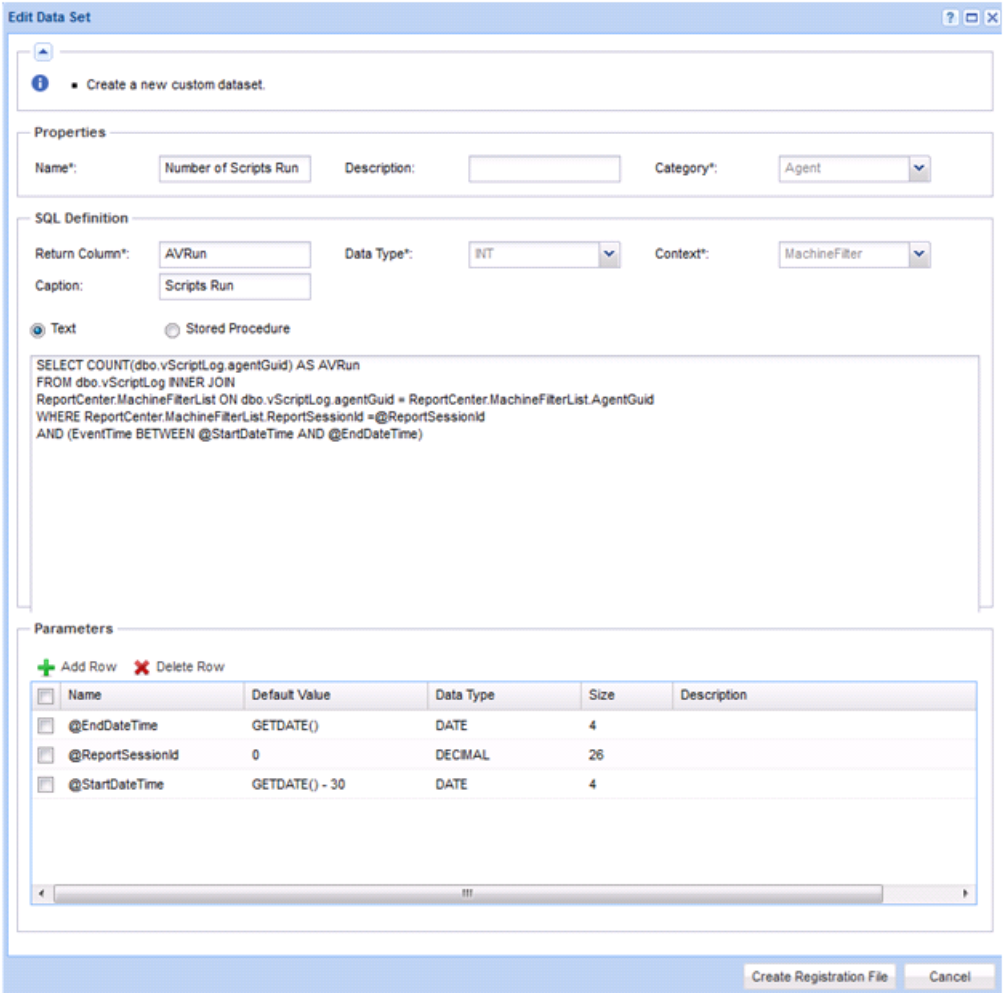
- Properties:** Name: Machine with Lowest [], Description: [], Category*: Audit [v]
- SQL Definition:** Return Column*: machName [], Data Type*: STRING [v], Context*: NONE [v], Caption: Machine with Lowest []
- Text:** Text, Stored Procedure
- SQL Query:**

```
SELECT TOP 1 mnt.machName
FROM dbo.auditRaIDisks ard
JOIN dbo.machNameTab mnt ON mnt.agentGuidStr = ard.agentGuid
WHERE mnt.partitionId = @PartitionID and ard.totalMBytes > 0
ORDER BY ard.freeMBytes
```
- Parameters:** A table with one row: @PartitionID, Default Value: 1, Data Type: DECIMAL, Size: 4.

Name	Default Value	Data Type	Size	Description
@PartitionID	1	DECIMAL	4	

Buttons at the bottom: Create Registration File, Cancel

- 3. This name value part uses the @ReportSessionID parameter to return a count of the number of agent procedures run. The MachineFilter context (page 173) enables you to choose filters when the report is run. The parameters @StartDateTime and @EndDateTime let you pick a date range at run time.



Report Contexts

You can use report contexts to apply filters to your data sets when a report definition is run or when a report part or report template is previewed. Each context provides a different filter. A filter fills a temporary table with a list of items you can JOIN to, which then limits what your query returns. The following table lists available report contexts, the temporary table used by each context, and the column to JOIN on.

Name	TableName	Column
MachineFilter	ReportCenter.MachineFilterList	AgentGuid
ServiceDeskFilter	ReportCenter.IncidentsFilterList	IncidentId
AssetsFilter	ReportCenter.AssetsFilterList	AssetId
DevicesFilter	ReportCenter.DevicesFilterList	DeviceId

Info Center

MobileDevicesFilter	ReportCenter.MobileDevicesFilterList	DeviceId
TicketingFilter	ReportCenter.TicketingFilterList	TicketId

Your query should both JOIN to one of the table columns above and include a WHERE statement using the [Well Known Parameters](#) (page 170) @ReportSessionId parameter. This ensures you get the data for the current run of the report.

Example

The following example uses the MachineFilter context.

```
SELECT COUNT(u.agentGuid) AS agentCount
FROM dbo.users u
INNER JOIN ReportCenter.MachineFilterList mfl ON mfl.AgentGuid = u.agentGuid
WHERE mfl.ReportSessionId = @ReportSessionid AND u.firstCheckin IS NOT NULL
```

Here is how you enter it in the name value part edit dialog.

Edit Data Set

■ Create a new custom dataset.

Properties

Name: Agent Count Description: Category: Agent

SQL Definition

Return Column: agentCount Data Type: INT Context: MachineFilter

Caption: Agent Count

Text Stored Procedure

```
SELECT COUNT(u.agentGuid) AS agentCount
FROM dbo.users u
INNER JOIN ReportCenter.MachineFilterList mfl ON mfl.AgentGuid = u.agentGuid
WHERE mfl.ReportSessionId = @ReportSessionid AND u.firstCheckin IS NOT NULL
```

Parameters

+ Add Row - Delete Row

Name	Default Value	Data Type	Size	Description
@ReportSessionid	0	DECIMAL	26	

Create Registration File Cancel

Name Value Instances

Info Center > Configure & Design > Name Value Parts

A **Name Value Instance** stores the arguments assigned to user-defined [parameters](#) (page 168) of a custom data set. These name value instances can be added to a [Name Value Part](#) (page 163), bypassing the need

to enter arguments manually each time a report template is created.

Fields

- **Name** - The name of the custom data set.
- **Value Label** - The label displayed with the returned value of the custom data set.

Parameters

These are the arguments for each parameter that are stored with an instance of the custom data set.

Cover Page, Header, Footer

[Info Center](#) > [Configure & Design](#) > [Coverpage, Header, Footer](#)

The [Coverpage, Header, Footer](#) page defines presentation elements that are independent of the data displayed in the report. You can use these elements to "brand" your reports by creating a unique look and feel. Assign different combinations of coverpages, headers and footers to multiple custom report templates and custom report definitions.

Tabs

Each type of element is defined using a separate tab.

- [Cover Page](#)
- [Header](#)
- [Footer](#)




Actions

Each element tab displays the same set of buttons.

- **Add / Edit** - Displays the *element designer window*.
- **Delete** - Deletes the element.
- **Default** - Sets this element as the default.
- **Preview** - Generates a preview of the element.

Element Designer Window

Once the element designer window opens, drag and drop any control into any of cells on the right side of the page to add it to the element's page layout. Once added, the grid cell displays the following icons:

-  - Configures the grid element. Added controls must be configured to save the element.
-  - Resizes the grid element.
-  - Deletes the grid element.

Add or change the following in the header of the element designer window.

- **Name** - The name of the element.
- **Description** - The description of the element.
- **Default** - If checked, this element serves as the default when a report template is created.

Cover Page Controls

The following controls are available in the element designer window for [Cover Page](#) elements.

- **Report Logo** - Sets the width, height and alignment of the report logo.

Note: By default, VSA report headers display the image specified by the System > Site Customization > Site Header (page 394). Changing the value in the System > Configure > Change Reporting Config... (page 382) > Logo field overrides this default, changing the URL *for report headers only*. Changing the URL in the Change Reporting Config... > Logo field does not affect the display of the Site Header image.

- **Text Box** - Specifies the text, alignment and format of a text box. Both the **Text Box** and **Text Area** controls support the following embedded tags.
 - <rt> = report name
 - <rd> = report date
 - <org> = organization filter
 - <gr> = machine group filter
 - <id> = machine filter
- **Text Area** - Specifies the text, alignment and format of a text area.
- **Filter Table** - Includes a cover legend describing the filtering applied to the report.
- **Horizontal Line** - Specifies the format and color of a horizontal line separating other rows of the grid.
- **Spacer** - Specifies the size of vertical white space separating other rows on the grid.

Header and Footer Controls

The following controls are available in the element design window for **Header** and **Footer** elements.

- **TextBox** - Specifies the text, alignment and format of a text box.
- **Page #** - Specifies the text, alignment and format of a page number.

Defaults

Info Center > Configure & Design > Defaults

The **Defaults** page sets defaults for report definitions. Defaults include:

- **Default Paper Size**
- **Default Distribution**

Legacy Report Definitions

A report is published from a report definition. Report definitions contain all the *default* settings that determine the content, layout and file format of the published report. You can override these defaults when you run (publish) or schedule the report.

Report definition settings are copied from a report template when the report definition is created. Changing a report definition does not change the report template it was copied from. Changes made to a report template do not affect report definitions already copied from that template.

To create a *legacy report definition* based on a *report template*:

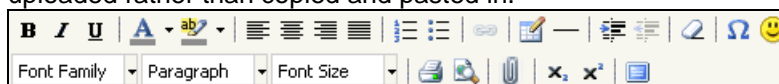
1. Click **Info Center > Reporting > Reports > New**.
2. Select the **Legacy Report** option.
3. Select a **category**, then a **template**, then click **Create**.
4. Specify options for report definitions using header options and three tabs:

- **(Header Options)** - Specify the name and report title. You can also **require approval for the report** (page 147).
- **Parameters** - See the list of predefined *legacy report templates* below for a description of each of these parameters.

Note: When a *custom report definition* (page 143) is added or edited, a **Layout** tab displays instead of the **Parameters** tab.

- **General** - Sets the type of report output—PDF, HTML or EXCEL—paper size and orientation. Also sets the message used to notify users when the report is run. Tokens can be included in report email messages, in both the subject line and the body of the message.
 - ✓ **<gr>** - machine group
 - ✓ **<id>** - machine id
 - ✓ **<rt>** - report name
 - ✓ **<embed>** - In the message body only, you can embed an HTML report at the specified location.

Use the edit toolbar to add images and special formatting to the text. Images must be uploaded rather than copied and pasted in.



- ✓ - Hyperlink selected text. You may need to reset links copied and pasted from another source.
 - ✓ - Insert a table.
 - ✓ - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
 - ✓ - Indent text.
 - ✓ - Outdent text.
 - ✓ - Remove formatting.
 - ✓ - Insert a symbol.
 - ✓ - Insert an emoticon.
 - ✓ - Preview the display of text and images.
 - ✓ - Upload a file or image.
 - ✓ - Set selected text to subscript.
 - ✓ - Set selected text to superscript.
 - ✓ - Toggle full screen mode for editing and viewing.
- **Cover Page, Header, Footer** - Selects the **cover page, header and footer** (page 174) of the report.

You can create legacy report definitions based on the following legacy report templates.

In This Section

Antivirus - Antivirus Installation Statistics.....	179
Anti-Malware - Anti-Malware Installation Statistics	179
Audit - Aggregate Table	179
Audit - Disk Utilization	179
Audit - Inventory	180
Audit - Machine Changes.....	180
Audit - Machine Summary.....	180
Audit - Network Statistics	181
Backup - Backup	182
Desktop Management - Power Savings.....	182
Desktop Management - User State.....	184
Executive - Executive Summary	184

KDS - Domain Activity	189
Data Backup Summary	189
Data Backup Usage Over Time	189
Logs - Admin Notes.....	190
Logs - Agent Log.....	190
Logs - Agent Procedure	190
Logs - Alarm Log.....	191
Logs - Configuration Changes	191
Logs - Event Logs	191
Logs - Event Logs Frequency	192
Logs - Log Monitoring	192
Logs - Network Statistics Log.....	192
Logs - Remote Control.....	193
Mobile Devices - Device Applications	193
Mobile Devices - Device Status	193
Mobile Devices - Device Summary	194
Mobile Devices - Lost Devices	194
Monitoring - Logs	194
Monitoring - Monitor 95th Percentile	195
Monitoring - Monitor Action Log	195
Monitoring - Monitor Alarm Summary	196
Monitoring - Monitor Configuration.....	196
Monitoring - Monitor Log	197
Monitoring - Monitor Set.....	197
Monitoring - Monitor Trending.....	197
Monitoring - Uptime History.....	197
Patch - Patch Management.....	198
Policy Management - Agents Policy Status	199
Policy Management - Policy Info & Association.....	199
Security - Configuration.....	199
Security - Security	199
Security - Historical Threats	200
Security - KES Log.....	200
Service Billing - Past Billed Invoices	200
Service Billing - Sales Order Summary.....	200
Service Billing - Unbilled Revenue by Customer	201
Service Billing - Unbilled Revenue by Item Type	201
Service Billing - Work Order Summary	201
Service Desk - Custom Tickets.....	201
Service Desk - Service Goals	202
Service Desk - Service Hours	203
Service Desk - Service Times	203
Service Desk - Service Volumes.....	203
Service Desk - Tickets	204
Software - Software Applications Changed	204
Software - Software Applications Installed.....	205
Software - Software Licenses	205
Software - Software Licenses Summary.....	205
Software - Software Operating Systems.....	206
Software Deployment - Profile Status by Machine.....	206
Software Deployment - Recent Deployments	206
Software Deployment - Software Installed by Machine	207
Software Deployment - Machine Changes	207
Ticketing - Customizable Ticketing	207
Ticketing - Ticketing	208
Time Tracking - Timesheet Summary.....	209

Time Tracking - Timesheet Entries	209
---	-----

Antivirus - Antivirus Installation Statistics

Info Center > Reporting > Reports > Antivirus

- Displays only if the Antivirus add-on module is installed.

The **Antivirus Installation Statistics** report definition generates reports for the following types of **Antivirus** data maintained by the VSA.

- **Show Summary Table** - Displays the number of machines installed with **Antivirus** per machine group. Installation details include the install date and version installed, per machine in each machine group.
- **Show Installation Month Bar Chart** - Displays a count of the number of machines installed with **Antivirus**, per month.

Anti-Malware - Anti-Malware Installation Statistics

Info Center > Reporting > Reports > Anti-Malware

- Displays only if the AntiMalware add-on module is installed.

The **Anti-Malware Installation Statistics** report definition generates reports for the following types of **AntiMalware** data maintained by the VSA.





- **Show Summary Table** - Displays the number of machines installed with **AntiMalware** per machine group. Installation details include the install date and version installed, per machine in each machine group.
- **Show Installation Month Bar Chart** - Displays a count of the number of machines installed with **AntiMalware**, per month.

Audit - Aggregate Table

Info Center > Reporting > Reports > Audit - Aggregate Table

The **Aggregate Table** report definition generates a tabular report mixing any data collected by the VSA. Each report generates a single table with a row for each machine and a column for each piece of data specified.

Adding and Removing Items

To add items, select items in the left hand list, then click the right arrow  button. To remove items, click items in the right hand list, then click the left arrow  button. To change the order items are listed, click an item in the right hand list, then click the up arrow  or down arrow .

Advanced Filter

Click the **Advanced Filter** (*page 27*) tab to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

Audit - Disk Utilization

Info Center > Reporting > Reports > Audit - Disk Utilization

The **Disk Utilization** report definition generates a graphical report representing the free space, used space and total space on each disk drive.

Three types of reports are available:

- **Show Bar Chart with Percent of Disk Space Used**
- **Show Bar Chart with Disk Space Used, Free Space, and Total Disk Size**

- [Show Table with Disk Space Used, Free Space, and Total Disk Size](#)

Audit - Inventory

[Info Center](#) > [Reporting](#) > [Reports](#) > [Audit - Inventory](#)

- Similar information is provided using [Audit > System Information](#) (page 134).

The **Inventory** report definition generates a report listing all unique items collected during an audit and identifies the machines containing that item.

Filtering

Filter fields restrict the items listed in the inventory report to only those items matching the filter. For example, If you run an Inventory report on the **Motherboard Manufacturer** field and set the filter to ***Intel*** you will only see items manufactured by **Intel**, or **Intel Corp**, or any other variation in the report.

PCI & Disk HW Inventory Reports

The **PCI & Disk HW** option displays additional fields for filtering the data in the report.

- [Hardware Type](#)
- [Description Notes Filter](#)
- [Product Filter](#)
- [Vendor Filter](#)

Audit - Machine Changes

[Info Center](#) > [Reporting](#) > [Reports](#) > [Audit - Machine Changes](#)

- Similar information is provided using [Audit > System Information](#) (page 121), and [Installed Applications](#) (page 136)

The **Machine Changes** report definition generates a differences report between each machine's latest audit and its own baseline *or* compares it to the baseline audit or latest audit from a selected machine. Machine changes examined include CPU, RAM, disk space and applications installed.

Configure your report using the following options:

- **Compare with Machine's own Baseline Audit** - Displays all machine changes found on each machine by comparing the information from the latest audit against the information from the baseline audit.
- **Compare to selected Machine ID** - Displays all machine changes found on each machine by comparing the information from the latest audit against the audit from a *selected machine ID*. Use this function to identify differences in a group of machines when compared against the standard for the group.
- **Use Baseline Audit** - Enabled if **Compare to selected machine ID** is selected. If checked, the selected machine ID's baseline audit is used for comparison instead of the selected machine ID's latest audit.

Audit - Machine Summary

[Info Center](#) > [Reporting](#) > [Reports](#) > [Audit - Machine Summary](#)

- Similar information is provided using [Audit > Machine Summary](#) (page 131) and [Live Connect](#) (page 344).

The **Machine Summary** report definition generates a detailed report for each machine ID matching the **machine ID / group ID filter** (page 556). Use the **Machine Summary** report to generate comprehensive reports for individual machines. Separate "add and remove" selection windows are provided for system data and application data to include in the **Machine Summary** report.





Machine Summary Sections

The **Machine Summary** report can include the following sections:

- **Add/Remove Programs** - Lists programs in the Add/Remove list of a managed machine.

- **Agent Control/Check-In** - Displays information on baseline and latest audits, last check-in times, quick check-in periods, primary and secondary server and port information.
- **Applications** - Lists applications installed on the managed machine. The list of applications can be filtered by clicking the **App Filter** button.
- **Apps Added Since Baseline** - All new applications detected by **Latest Audit** (page 128) that have appeared on the machine since the **Baseline Audit** (page 128) was run.
- **Apps Removed Since Baseline** - All applications that were present when the **Baseline Audit** (page 128) was ran but are missing when **Latest Audit** (page 128) last ran.
- **Computer/Network** - Displays the managed machine Windows network name, operating system, CPU, RAM, IP address, gateway, DNS/DHCP server, and WINS server information.
- **Distribute Files** - List files being distributed to the managed machine by the Kaseya Server.
- **File Access** - Lists protected files.
- **License Codes** - Lists license codes installed on the managed machine.
- **Logical Disk** - Lists the logical volumes on the managed machines, including removable, fixed, and CD-ROM drives.
- **Miscellaneous** - Lists miscellaneous agent settings, such as WinVNC and user logs status.
- **Network Access** - Lists applications that have restricted network access.
- **PCI Devices** - Lists installed PCI devices on the managed machine.
- **Pending Procedures** - Lists scheduled procedures on the managed machine.
- **Physical Disk** - Lists physical disk information for the managed machine, such as hard disks, DVD, and CD-ROM drives.
- **Printers** - Lists the printers found by the audit for this machine.
- **Recurring Procedures** - Lists procedures that are executed on a scheduled basis on the managed machine.
- **System Info** - All items collected by the **System Info** (page 134) function in the **Audit** module. Click the **Sys Info** button to make additional System Information selections.
- **User Profile** - Lists out user contact information associated with this machine ID.

Adding and Removing Items

To add items, select items in the left hand list, then click the right arrow  button. To remove items, click items in the right hand list, then click the left arrow  button. To change the order items are listed, click an item in the right hand list, then click the up arrow  or down arrow .

Advanced Filter

Click the **Advanced Filter** (page 27) tab to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed. This option only displays if you select the **System Info** option above.

Audit - Network Statistics

Info Center > Reporting > Reports > Network Statistics

- Info Center > Reporting > Reports > Logs > Network Statistics Log (page 192) identifies *all* network access activity.
- Related information is provided using System > Statistics (page 389).

The **Network Statistics** report definition generates a report displaying the *top consumers* of TCP/IP-protocol-based network bandwidth on selected machines. Typically this report refers to bandwidth consumption caused by accessing both internal and external *internet* sites, but can include internal LAN traffic that also uses the TCP/IP protocol.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.

- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Report Parameters

- **Applications** - Displays a graph outlining each application and corresponding network bandwidth consumption over the specified period.
- **Machines** - Displays a graph outlining the machines selected in the machine ID / group ID filter and corresponding network bandwidth consumption.
- **Display <N> Consumers of Bandwidth** - The number of top consumers of bandwidth included in the report, either applications or machines.

Note: This report requires the **Audit > Network Access** (page 75) driver be enabled. This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. The driver is *disabled* by default.

Backup - Backup

Info Center > Reporting > Reports > Backup

- Displays only if the **Backup** add-on module is installed.
- Similar information is provided using **Backup > Backup Status**.

The **Backup** report definition generates a report summarizing data retrieved from the backup logs.

Configure the report using the following options:

- **Show backup logs from the last <N> days** - Specify how many days of backup log entries to include in the report.
- **Show backup log summary data** - If checked, includes a summary table totaling types of backup events for the last N number of days for volumes and folders.
- **Show backup log status by machine and event** - List the backup log information collected in the last N days for each machine.
 - **Backup type filter** - **Volume Backups** or **Folder Backups**.
 - **Result filter** - **<All Results>**, **Success**, **Failure**, **Warning**, **Informational**
- **Ignore machines without data** - If checked, only displays machine IDs that have data matching the other filter parameters.

Desktop Management - Power Savings

Info Center > Reporting > Reports > Desktop Management > Power Savings

- Displays only if the **Desktop Policy** add-on module is installed.

The **Power Savings** page generates a report that shows an estimate of how much money can be saved, or has been saved, using a particular power policy. An independent power audit is scheduled as part of the standard audit and collects power settings from all managed machines *including those without the Desktop Policy client installed*.

Comparison Settings

A power audit is performed on a machine whenever a power policy is applied to the machine and is also performed by the **latest audit** (page 551), typically on a daily basis.

- **Compare machine baseline audit information with:**
 - **Compare With** - Select a defined power policy to see how much you can save by switching over to the selected power policy.

- **Include All Machines** - If checked, includes the independent power audit results for all Windows 2003 and Windows XP machines without **Desktop Policy** installed along with the results from machines with **Desktop Policy** installed. Checked by default. Does not include Windows 2000, Vista, or 7 machines.
- **Compare most recent power audit data with:**
 - **Compare With - Baseline Power Policy** - Shows power savings by comparing the baseline power policy to the latest audit for each machine. The baseline power policy represents what was in place before **Desktop Policy** was installed on the machine.
 - **Compare With - Last Deployed Power Policy** - Shows power savings by comparing the last deployed power policy to the latest audit for each machine. This value should be the same as the most recent power audit data, unless some of the users have changed their settings since the last time a power policy was applied.
- **Report Period** - Enter the reporting period for the report: **Year, Month, From Baseline Collection Time**.

Set Report Values

Set the values that the power savings estimate is based on or leave them set to their default values.

- **Average PC Watts** - Enter the number of watts an average PC in the system uses.
- **Average Monitor Watts** - Enter the number of watts an average monitor in the system uses.
- **Cost of kilowatt-hour (kWh)** - Enter the cost per kilowatt-hour (kWh).
- **Currency Symbol** - Enter the currency symbol associated with the cost entered in the **Cost of kilowatt-hour (kWh)** field. This currency symbol displays in the report.

Advanced Settings

Make changes to the following advanced settings or leave them set to their default values:

- **PC Watts When Stand By** - Enter the number of watts an average PC uses while it is in standby mode.
- **Workstation Hours Per Day** - Enter the number of hours per day a workstation is in use.
- **Workstation Days Per Week** - Enter the number of days per week the workstation is in use.
- **% of Machines Powered Down at end of Day** - Enter the number of machines that are physically turned off at the end of the day.
- **Workstation Days Idle Per Year (Holidays, Vacations, etc)** - Enter the number of days per year the average workstation is not in use, in addition to weekends.
- **Select Machine Data Based on:**
 - **Most Savings** - If selected, the calculation uses the single user on a machine that provides the highest estimated power savings, as though no other user ever used that machine. This represents the best possible power savings for that machine.
 - **Average User** - If selected, the calculation uses an average of the estimated power savings of all users on a machine, as though each user was logged on to that machine an equal amount of time. This generates an equal or smaller power savings estimate than the **Most Savings** option.
- **Hard Drive Watts** - Enter the number of watts a hard drive uses.
- **Server Hours Per Day** - Enter the number of hours per day a server is in use.

Note: Any OS that has the word Server in its name is treated as a server for the purposes of this report.

- **Server Days Per Week** - Enter the number of days per week a server is in use.
- **Include Monitors for Servers** - If checked, the calculation assumes each server has a monitor attached and the power settings for the monitors are included.
- **Show Settings per User** - If checked, the report shows the savings for each user on each machine.

Desktop Management - User State

Info Center > Reporting > Reports > Desktop Management > User State

- Displays only if the Desktop Policy add-on module is installed.
- Similar information is provided using Desktop Management > Status.

The **Desktop Policy** page generates reports for the following types of **Desktop Policy** data maintained by the VSA.

Select the subtopics to include in the **Desktop Policy** report:

- **Include User Type** - List all user groups that each user on the machine is a member of.
- **Include Mapped Drives** - List the drive mappings for each user.
- **Include Printers** - List printer mappings for each user.
- **Include Share points** - List all the directory shares for the machine.
- **Include machines with no data** - Show entries in the report for all machines, including those that have not had **Desktop Policy** information collected.

Executive - Executive Summary

Info Center > Reporting > Reports > Executive - Executive Summary

The **Executive Summary** report definition generates a summary report of the status of all selected machines. This includes a **network health score** (*page 186*) representing the overall health of all selected machines as a group.

Configure your report definition using the following parameters:

Time Selection

- **Summarize Data collected in the last N days** - Number of days back from the current date/time to include in the report.

Report Parameters - Report Selection

- **Show Client Information** - Displays the number of machines, both servers and workstations, and the names of the primary points of contact for this group.
 - **Contact Person** - Optionally enter a customer contact name, representing the point of contact inside the organization receiving the IT service.
 - **IT Manager** - Optionally enter an IT manager name, representing the person responsible for delivering IT services to the client organization.
- **Show System Activity** - Specify search criteria for counting the number of times certain log events occurred. Examples include the number of times machines were audited and scanned for missing patches. Click **Change Rows...** to fully customize this section.
- **Show Ticket Status** - Displays a summary of ticket counts over the specified number of days. If **Service Desk** is installed and activated, displays tickets count only for **Service Desk** tickets. Additional ticket counts display for the number of tickets in each Status defined. Uncategorized Tickets displays if one or more tickets are not set to any Status.
- **Show Anti-Virus Statistics** - Displays Anti-Virus protection and threats **statistics** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#7189.htm>).

Note: The **Show Anti-Virus Statistics** section only displays if you have installed the Antivirus add-on module.

- **Show Disk Space Used for** - Displays a graph of the percentage free disk space on all selected machines. Restrict this chart to servers only by selecting **Show servers only**.
- **Show Percent Uptime for** - Displays a graph of the percentage machines are up for on all selected machines. Restrict this chart to servers only by selecting **Show servers only**.

- **Show Network Health Score** - Displays individual component scores and an overall health score for all the selected machines as a group. See **Network Health Score** (page 186) for details. Click **Change Score...** to fully customize this section.
- **Show Operating Systems** - Displays a pie chart showing the break down of operating systems in the selected group.
- **Show Patch Status** - Displays a pie chart summarizing the state of missing patches for all selected machines.
- **Show Security** - Lists statistics for untreated security protection threats.

Note: The **Show Security** section only displays if you have installed the **Endpoint Security add-on** module.

- **Show Alarm Notifications** - Summarizes alerts issued for the specified number of days. This section breaks the alarm count down by category of alarm.
- **Show License Summary** - Summarizes the OS and MS Office licenses found by audit.
- **Show "How to read" notes at end of report** - Displays standard explanatory notes at end of the report. Click **Edit Notes...** to customize these notes.

System Activity

Info Center > Reporting > Reports > Executive Summary > System Activity

The **System Activity** section of the **Executive Summary** (page 184) report gives you a summary view of system activity of selected machines as a group. Each row lists a *count* or *value* of a filtered log item in the *last N number of days*.

- Use the **Status** column in the **Pending Procedures** tab of the **Machine Summary** (page 180) page or **Live Connect** (page 344) to identify search filter phrases to use for a procedure-based row type.

Note: You must enter at least an ***** in the **Search Filter** field to return any results.

- **Log Monitoring** does not display in **Pending Procedures**. Review **Log Monitoring** in **Agent Logs** in the **Machine Summary** page or **Live Connect** to identify search filter phrases to use.
- **Log Monitoring Custom** refers to the *value* or *count* of a numeric log parsing parameter within the *last N number of days*.

Row Type	Search Item	Search Filter Examples	Count
Alarm Log	<All Alarms> or any specific alert/alarm.	* or *text*	Not applicable.
Script Log	Select a system, private or public agent procedure.	*Success THEN* or *Failed ELSE* or *Success ELSE*	Not applicable.
Backup Log	<All Backup Events> or Volume Backups or Folder Backups	*Backup completed successfully*	Not applicable.
Log Monitoring	Select a Log File Parser (page 314).	*device error*	Not applicable.
Log Monitoring Custom	Select a Log File Parser with a numeric parameter.	EventCode or ErrorCode	Average, Count, Min, Max or Total

Network Health Score

Info Center > Reporting > Reports > Executive Summary > Change Score...

The **Network Health Score** section of the **Executive Summary** (page 184) report gives you a summary view of the health and usability of selected machines as a group. The score is broken into **score types**. Each score type is subdivided into one of five possible **percentage buckets**—typically 100%, 75%, 50%, 25% and 0% if none of the first four percentage buckets apply—based on the count for a specified criteria.

Score Type Calculation Example: To keep things simple, an **Executive Summary** report only includes three machines. For a single score type within that report, one machine meets the criteria for the 100% bucket. The other two machines meet the criteria for the 75% bucket. $(100\% + 75\% + 75\%)/3 = 83\%$ health for that score type. You could assign a weight of 2 to double the weight of this score type compared to all the other score types in the report.

Weight Calculation Example: You set one score type to a weight of 2 and seven score types to a weight of 1. The total weight for all 8 score types is 9. The percentage of the score type weighted by 2 is multiplied by 2/9 in the final percentage score calculation. In contrast, the percentages of the other seven score types weighted by 1 are multiplied only by 1/9 in the final percentage score calculation. The final network health score computes the *weighted average* of all score type percentages and normalizes them to provide the final percentage score. 100% represents perfect.

- In most cases, you can customize the counts used to assign percentage scores.
- Set the weight to 0 to *turn off that score type*.
- For the **OS Score** type only, the standard percentage buckets of 100%, 75%, 50%, and 25% are overridden by the values you set. Each bucket is associated with a different type of operating system. What you're deciding is how healthy a machine should be considered, based on its operating system. Older operating systems tend to be assigned lower **OS Score** percentages.
- You cannot modify the **Patch Score** criteria.

Note: Ticketing is ignored when calculating the overall network health score.

Patch Score - This score is calculated using the average number of missing patches on each machine. Each machine is scored based on the number of missing patches as follows:

Fully patched	100%
missing 1-2 patches	75%
missing 3-5 patches	50%
missing > 5 patches	25%
unscanned machines	0%

OS Score - Modern operating systems score higher than older operating systems. The overall OS score is an average of each machine's score calculated as follows:

Win7/Vista/2008	100%
XP/2003	100%
2000	75%
Apple OS	100%
All others	0%

Note: The OS score weighting can be customized. You can individually weight the OS score given to Win7/Vista/2008, 2003, XP and 2000. Enter the % weights (0 to 100) in the four columns normally used for % score. All legacy OSs are given a zero. If you have a large number of legacy OSs deployed, considered turning off the OS score.

Disk Score - Full disk drives can have a severe negative impact on your system. As such disk space

used contributes to the overall system score. Disk score is computed as follows:

0% to 65% full	100%
65% to 75% full	75%
75% to 85% full	50%
85% to 95% full	25%
100% full	0%

Ticket Score - Past due tickets assigned to machines are scored as follows:

0 past due	100%
1 or 2 past due	75%
3 to 5 past due	50%
6 to 10 past due	25%
more than 10 past due	0%

Note: The system does not delete tickets when deleting machine IDs. The ticket summary chart includes tickets matching the machine ID / group ID filter. Because no machine data exists for deleted machine IDs, views are not applied to this table.

Event Log Score - Monitored event log alerts represent potential system problems. The number of event log alerts generated by each machine over the specified period of time is scored as follows:

0 alerts	100%
1 to 4 alerts	75%
5 to 10 alerts	50%
11 to 20 alerts	25%
more than 20 alerts	0%

Backup Score - Counts days since the backup last ran. The older the backup is, the lower the score.

0 to 3 days since last backup ran	100%
4 to 7 days since last backup ran	75%
8 to 14 days since last backup ran	50%
15 to 30 days since last backup ran	25%
more than 30 days since last backup ran	0%

Alarm Score - The fewer alarms generated, the higher the score.

0 to 3 alarms	100%
4 to 9 alarms	75%
10 to 19 alarms	50%
20 or more alarms	25%

Workstation Uptime Score - The greater the percentage of time workstations are up, the higher the score.

90	100%
80	75%
70	50%
60	25%

Server Uptime Score - The greater the percentage of time servers are up, the higher the score.

99	100%
----	------

97	75%
95	50%
90	25%

Security Score - Untreated threats represent potential system problems. The number of untreated threats generated by each machine over the specified period of time is scored as follows:

0 untreated threats	100%
1 to 4 untreated threats	75%
5 to 10 untreated threats	50%
11 to 19 untreated threats	25%
more than 20 untreated threats	0%

Note: The Security Score only displays if you have separately purchased the Endpoint Security add-on module.

Antivirus Score - The Antivirus rating is a composite score weighted as follows for each individual machine:

- **Anti-virus install percentage - 40%** - Is Antivirus installed on the machine?
- **Full scans run during the period - 40%** - Has at least one Antivirus scan run during the period?
- **Active threats - 20%** - Has zero threats been detected during the period?

After each machine Antivirus rating is determined, they are grouped into the following percentage buckets, which can be customized: 100%, 75%, 50%, 25%.

Note: The Antivirus Score only displays if you have separately purchased the Antivirus add-on module.

AntiMalware Score - The **AntiMalware** rating is a composite score weighted as follows for each individual machine:

- **Anti-virus install percentage - 40%** - Is **AntiMalware** installed on the machine?
- **Full scans run during the period - 40%** - Has at least one **AntiMalware** scan run during the period?
- **Active threats - 20%** - Has zero threats been detected during the period?

After each machine **AntiMalware** rating is determined, they are grouped into the following percentage buckets, which can be customized: 100%, 75%, 50%, 25%.

Note: The AntiMalware Score only displays if you have separately purchased the AntiMalware add-on module.

Procedure Score - Procedures provide a recurring beneficial service to a machine. The more often the procedure runs, the better shape that machine is likely to be in. The longer it has been since the procedure ran, the lower the score. The weighted thresholds for the procedure score count the number of days since the procedure last ran on the machines. The default values provide the following score:

1	0 to 3 days since procedure ran	100%
2	4 to 9 days since procedure ran	75%
3	10 to 19 days since procedure ran	50%
4	20 or more days since procedure ran	25%

Note: You must enter at least an * in the Description Filter field to return any results.

KDS - Domain Activity

Info Center > Reporting > Reports > KDS - Domain Activity

- Displays only if the **Discovery** add-on module is installed.

The **Domain Activity** report definition generates a report of domain configuration changes visible to **Discovery**.

Configure your report definition using the following parameters:

Time Selection

Filter by date range.

- **Start DateTime**
- **End DateTime**

Activity

Filter by type of object and type of actions performed on those objects.

- **Objects Types** - Computer, Contact, Container, Domain, Group, Organization Unit, User
- **Action Types** - Created, Updated, Deleted

Data Backup Summary

Info Center > Reporting > Reports > KOB - Data Backup Summary

- Displays only if the **Data Backup** add-on module is installed.

The **Data Backup Summary** report definition generates a summary report of **Data Backup** activities by machine ID.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Parameters

- **Include Machines with No Data** - If checked, includes machines that have no backups.
- **Show Detail** - If checked, displays all backup activities for a machine. If blank, only the last backup activity is displayed.

Data Backup Usage Over Time

Info Center > Reporting > Reports > KOB - Data Backup Usage Over Time

- Displays only if the **Data Backup** add-on module is installed.

The **Data Backup Usage Over Time** report definition generates a report of **Data Backup** usage by time period.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Parameters

- **Include Machines with No Data** - If checked, includes machines that have no backups.
- **Select the Time Period** - Daily, Weekly, Monthly, Quarterly, Yearly.
- **Select the Usage Type** - Show Peak Usage, Show Average Usage.

Logs - Admin Notes

Info Center > Reporting > Reports > Logs - Admin Notes

The **Admin Notes** report definition generates reports of **administrator notes** (page 12).

Configure your report definition using the following parameters:

- **Number of days to query log*** - Number of days back from the current date/time to include in the report.
- **Show entries matching the following description (use * for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Agent Log

Info Center > Reporting > Reports > Logs - Agent Log

- Agent > Agent Logs (page 31) displays log entries by log type and machine ID.

The Agent Log report definition generates a report of agent log entries by machine ID.

Configure your report definition using the following parameters:

- **Number of days to query log*** - Number of days back from the current date/time to include in the report.
- **Show entries matching the following description (use * for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Agent Procedure

Info Center > Reporting > Reports > Logs - Agent Procedure

- Agent > Agent Logs (page 31) displays log entries by log type and machine ID.

The **Agent Procedure** report definition generates a report of all system and user-defined agent procedures run on each machine ID, including the agent procedure's success or failure status and the VSA user that scheduled them.

Configure your report definition using the following parameters:

- **Number of days to query log*** - Number of days back from the current date to include in the report.
- **Agent Procedure Name Filter** - Filter entries by agent procedure name.
- **Administrator Filter (Admin that scheduled the agent procedure)** - Filter by the VSA user who scheduled the agent procedure.
- **Show entries matching the following description (use * for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Alarm Log

Info Center > Reporting > Reports > Logs - Alarm Log

- Agent > Agent Logs (page 31) displays log entries by log type and machine ID.

The **Alarm Log** report definition generates a report of alarm log entries by machine ID.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Parameters

- **Choose an alert type to display** - Filters by **alert types** (page 550).
- **Filter on email address alarm was sent to** - Filters by alert email recipient.
- **Alarm subject line filter** - Filters by alert email subject line.
- **Alarm message body filter** - Filters by alert email body text.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Configuration Changes

Info Center > Reporting > Reports > Logs - Configuration Changes

- Agent > Agent Logs (page 31) displays log entries by log type and machine ID.

The **Configuration Changes** report definition generates a report of VSA setting changes made to each machine ID.

Configure your report definition using the following parameters:

- **Number of days to query log*** - Number of days back from the current date/time to include in the report.
- **Show entries matching the following description (use * for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Event Logs

Info Center > Reporting > Reports > Logs - Event Logs

- Agent > Agent Logs (page 31) displays log entries by log type and machine ID.

The **Event Logs** report definition generates a report of **event log** (page 554) data collected by Windows by machine ID.

Configure your report definition using the following parameters:

- **Display log entries for last N days(s)** - Number of days back from the current date to include in the report.
- **Choose Event Type** - Filter by event log type.
- **Filter by event set** - Filter by a selected event set. Otherwise all events are reported.
- **Event Categories** - Filter by event category.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Event Logs Frequency

[Info Center](#) > [Reporting](#) > [Reports](#) > [Logs - Event Logs Frequency](#)

- [Agent](#) > [Agent Logs](#) (page 31) displays log entries by log type and machine ID.

The [Event Logs Frequency](#) report definition generates a report of the *most frequent event IDs* in [event log](#) (page 554) data collected by Windows, by machine ID.

Configure your report definition using the following parameters:

Time Selection

- [Select the Time Range Type](#) - Filters by a fixed type of date range.
- [Number Of Days](#) - Applies only if [Last N Days](#) is selected time range type.
- [Custom Start DateTime](#) - Applies only if [Fixed Range](#) is select time range type.
- [Custom End DateTime](#) - Applies only if [Fixed Range](#) is select time range type.

Report Parameters

- [Select the <N> most frequent Event IDs for each machine ID](#) - Select the number of most frequent event IDs.
- [Choose Event Type](#) - Filter by event log type.
- [Event Categories](#) - Filter by event category.
- [Ignore machines without data](#) - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Log Monitoring

[Info Center](#) > [Reporting](#) > [Reports](#) > [Logs - Log Monitoring](#)

- [Agent](#) > [Agent Logs](#) (page 31) displays log entries by log type and machine ID.

The [Log Monitoring](#) report definition generates a report of '[Log Monitoring](#) (page 555)' log entries.

Configure your report definition using the following parameters:

Time Selection

- [Select the Time Range Type](#) - Filters by a fixed type of date range.
- [Number Of Days](#) - Applies only if [Last N Days](#) is selected time range type.
- [Custom Start DateTime](#) - Applies only if [Fixed Range](#) is select time range type.
- [Custom End DateTime](#) - Applies only if [Fixed Range](#) is select time range type.

Report Parameters

- [Choose Log File Parser](#) - Filter by log parser definition.
- [Show entries matching the following description](#) - Enter a string to filter entries by their description. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- [Ignore machines without data](#) - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Network Statistics Log

[Info Center](#) > [Reporting](#) > [Reports](#) > [Logs - Network Statistics Log](#)

- [Info Center](#) > [Reporting](#) > [Reports](#) > [Audit](#) > [Network Statistics](#) (page 181) identifies *top consumers* of network bandwidth.
- Related information is provided using [System](#) > [Statistics](#) (page 389).
- [Agent](#) > [Agent Logs](#) (page 31) displays log entries by log type and machine ID.

The [Network Statistics Log](#) report definition generates a report of [network statistics](#) (page 181), by machine ID.

Note: This report requires the Audit > Network Access (page 75) driver be enabled. This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. The driver is disabled by default.

Configure your report definition using the following parameters:

- **Number of days to query log*** - Number of days back from the current date to include in the report.
- **Show applications matching the following description (use * for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

Logs - Remote Control

Info Center > Reporting > Reports > Logs - Remote Control

- Agent > Agent Logs (page 31) displays log entries by log type and machine ID.

The **Remote Control** report definition generates a report of remote control sessions, by machine ID.

Configure your report definition using the following parameters:

- **Number of days to query log*** - Number of days back from the current date/time to include in the report.
- **Show entries matching the following description (use * for wildcards)** - Enter a string to filter entries by their description. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Ignore machines without data** - Check this box to only display machine IDs that have data matching the other filter parameters.

Mobile Devices - Device Applications

Info Center > Reporting > Reports > Mobile Devices - Device Applications

- Displays only if the **Mobile Device Management** add-on module is installed.

The **Device Applications** report definition generates a report listing the application installed on a device.

Filtering and Sorting Parameters

- **Operating System Type** - Android, Apple
- **Manufacturer** - The manufacturers of device hardware.
- **Home carrier** - The main service providers of devices.
- **Current carrier** - The carriers currently being used by devices.
- **Application Name** - The name of applications installed on devices.

Mobile Devices - Device Status

Info Center > Reporting > Reports > Mobile Devices - Device Status

- Displays only if the **Mobile Device Management** add-on module is installed.

The **Device Status** report definition generates a report listing the status of each device.

Filtering and Sorting Parameters

- **Mobile Device Status** - Only the most common commands are listed below.
 - **Invited** - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
 - **Normal** - The app is installed and working normally.

- **Command Pending** - A command is pending for the Kaseya Agent app on the user's device.
- **Operating System Type** - **Android**, **Apple**
- **Track** - **True**, **False**

Mobile Devices - Device Summary

Info Center > Reporting > Reports > Mobile Devices - Device Summary

- Displays only if the **Mobile Device Management** add-on module is installed.

The **Device Summary** report definition generates a summary report of all audit information of selected devices.

Filtering and Sorting Parameters

- **Mobile Device Status** - *Only the most common commands are listed below.*
 - **Invited** - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
 - **Normal** - The app is installed and working normally.
 - **Command Pending** - A command is pending for the Kaseya Agent app on the user's device.
- **Operating System Type** - **Android**, **Apple**
- **Manufacturer** - The manufacturers of device hardware.
- **Home carrier** - The main service providers of devices.

Detail Tables to Display

- **Show Operating System Detail**
- **Show Device Info Detail**
- **Show Platform Detail**
- **Show Home Network Detail**
- **Show Current Network Detail**

Detail Charts to Display

- **Show Mobile Device Status Chart**
- **Show OS Type Chart**
- **Show Manufacturer Chart**
- **Show Home Carrier Chart**
- **Show Current Carrier Chart**

Mobile Devices - Lost Devices

Info Center > Reporting > Reports > Mobile Devices - Lost Devices

- Displays only if the **Mobile Device Management** add-on module is installed.

The **Lost Devices** report definition generates a report of all lost devices.

Time Range

- **From** - Filters the report date range by this start date.
- **To** - Filters the report date range by this end date.

Monitoring - Logs

Info Center > Reporting > Reports > Monitoring - Logs

The **Logs** report definition provides a single point of access for generating any other type of log report. All parameters for all log reports are provided on the Parameters tab. When specifying a log report,

only parameters that support that type of log report apply. Consult the following log topics for the parameter fields that apply.

- [Logs - Agent Log](#) (page 190)
- [Logs - Configuration Changes](#) (page 191)
- [Logs - Network Statistics](#) (page 192)
- [Logs - Event Logs](#) (page 191)
 - Application Event Log
 - Security Event Log
 - System Event Log
 - All Event Logs
- [Logs - Agent Procedure](#) (page 190)
- [Logs - Admin Notes](#) (page 190)
- [Logs - Alarm Log](#) (page 191)
- [Logs - Remote Control](#) (page 193)
- [Logs - KES Log](#) (page 200)

Monitoring - Monitor 95th Percentile

[Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring](#) - [Monitor 95th Percentile](#)

The **Monitor 95th Percentile** report definition specifies two dates and calculates the 95th percentile, meaning 95% of the time the value is below what is calculated in the report. Identifies *typical* bandwidth requirements for a machine or a device, just below infrequent "peak usage" events. The report supports SLA and planning calculations.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Report Parameters

- **Select the monitor set or SNMP set**
- **Percentile** - Set the percentile to use in the report.
- **Select the counters/MIB objects to add to the report** - Select specific counters in the selected monitor set or specific MIB objects within the selected SNMP set to include in the report.

Monitoring - Monitor Action Log

[Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring](#) - [Monitor Action Log](#)

The **Monitor Action Log** report definition generates a report of **alert conditions** (page 551) and the actions taken in response to each alert condition.

A user can assign monitor sets, SNMP sets, alerts, system checks or log monitoring to machine IDs *without checking the Create Alarm checkbox* and a **Monitor Action Log** entry will still be created. These logs enable a VSA user to review *alerts* that have occurred with or without being specifically notified by the creation of an alarm, email or ticket. You can generate a report using [Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring](#) > [Monitor Action Log](#) (page 195).

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Report Parameters

- **Monitor Type** - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- **Message Filter** - Enter a string to filter alarms by their message text. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Sort by Log Event Date Time** - Ascending, Descending

Monitoring - Monitor Alarm Summary

[Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring - Monitor Alarm Summary](#)

- [Review alert conditions without creating alarms using Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring](#) > [Monitor Action Log](#) (page 195).

The **Monitor Alarm Summary** report definition generates a report of created alarms by machine ID. Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Report Parameters

- **Monitor Type** - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- **Alarm Type** - Alarm, Trending
- **Message Filter** - Enter a string to filter alarms by their message text. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Sort by Log Event Date Time** - Ascending, Descending
- **Display Message with Each Alarm** - Include a detailed message generated for each alarm.

Monitoring - Monitor Configuration

[Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring - Monitor Configuration](#)

The **Monitor Configuration** report definition generates a report of the configuration details of each monitor set assigned to a machine ID or SNMP set assigned to a device.

Configure your report definition using the following parameters:

- **List Assigned Set Only** - If checked, only displays for selection monitor sets assigned to machine IDs and SNMP sets assigned to devices.
- **Select Sets to be Displayed** - Select sets in the right hand pane and click the > button to move them to the right hand pane.

Monitoring - Monitor Log

[Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring - Monitor Log](#)

The **Monitor Log** report definition generates a report of monitor log data for monitor sets and SNMP sets, by machine ID, counter and MIB object.

Configure your report definition using the following parameters:

- [Specify the Number of Log Entries for Each Counter and Machine](#)
- [Show Counter Log Data](#)
- [Show Service Log Data](#)
- [Show Process Log Data](#)
- [Show SNMP Log Data](#)

Monitoring - Monitor Set

[Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring - Monitor Set](#)

The **Monitor Set** report definition generates a report of the monitor logs for a single monitor set or SNMP set, by machine ID.

Configure your report definition using the following parameters:

- [Select Monitor Set](#) - Select a single monitor set or SNMP set.
- [Display Last](#) - Number of periods back from the current date/time to include in the report.

Monitoring - Monitor Trending

[Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring - Monitor Trending](#)

The **Monitor Trending** report definition generates a report of the monitor logs for a single monitor set counter or for a single SNMP set MIB object, by machine ID.

Configure your report definition using the following parameters:

- [Select Monitor Set](#) - Select a single monitor set or SNMP set.
- [Select Counter](#) - Select a counter in the selected monitor set or a MIB object in the selected SNMP set.
- [Display Last](#) - Number of periods back from the current date/time to include in the report.

Monitoring - Uptime History

[Info Center](#) > [Reporting](#) > [Reports](#) > [Monitoring - Uptime History](#)

The **Uptime History** report definition generates a graphical report representing:

- When each managed machine was turned on.
- When each managed machine was connected to the network.
- Any abnormal shut downs.

Hovering the mouse over any segment on the chart presents a tool tip that reads out the exact start and end time of that segment.

Configure your report definition using the following parameters:

- [Display N days of Machine Uptime and Online Time](#) - Number of days back from the current date to include in the report.
- [Display all times in the local time zone for each agent](#) - Display events in local machine time.
- [Display all times in the system server time zone](#) - Display events using Kaseya Server time.

Patch - Patch Management

Info Center > Reporting > Reports > Patch Management

- Similar information is provided using Patch Management > Patch Status, Machine History, Machine Update and Patch Update.

The **Patch Managements** report definition generates a report that lists the patch state for all selected machine IDs. Reports can be filtered by patch category or knowledge base article number. Reports can include patches denied by patch policy. Reports include links to KB articles.

Configure your report definition using the following parameters:

Display Options

- **Machine Patch Summary Pie Chart** - Display a pie chart showing the number of machines that are:
 - Fully patched systems
 - Missing 1 or 2 patches
 - Missing 3, 4, or 5 patches
 - Missing more than 5 patches
 - Have never been scanned
- **Machine Patch Summary Table** - Display a machine patch summary table.
- **Missing Patch Occurrence Bar Chart** - Display a bar chart illustrating which patches have the most machines that are missing that patch.
- **Table of Missing Patches** - This is a composite report that shows all patches that are missing from any and all machines in the selected group. This table lists a section for each missing patch showing: patch ID, KB article number, and patch title. If Show (Include machines missing each patch) is selected, then the report lists each machine ID missing the patch.
- **Table of Installed Patches** - This is a composite report that shows all patches that are installed on any and all machines in the selected group. This table is basically the opposite of the **Table of Missing Patches** section. This table lists a section for each installed patch showing: patch ID, knowledge base article number, and patch title. If Show (Include machines missing each patch) is selected, then the report lists each machine ID with the patch installed.
- **Patch Status for each Machine** - For each machine ID a list of both installed and missing patches are shown. Patches are grouped by application. If Show (include titles for each patch) is selected, the titles describing the patches are also displayed.
- **Missing Patches for each machine** - For each machine ID a list only of missing patches are shown. Patches are grouped by application. If Show (include titles for each patch) is selected, titles describing the patches are also displayed.
- **Patches installed in the last <N> days** - For each machine ID, a list of patches are displayed that were installed during the last number of days specified in the text box. If Show (include titles for each patch) is selected, titles describing the patches are also displayed.

Filters

- **KB Article Numbers and/or Security Bulletin Numbers** - Enter a comma delimited list of KB Article numbers and/or Security Bulletin numbers to generate a report that only lists patches for these numbers.
- **Standard Filter** - Select a filter criteria for the patch report.
- **Show patches denied by Patch Approval Policy** – By default, only missing patches that have been approved for installation are included in the report. Check the checkbox to ignore the **Patch Approval Policy** (page 559) and include all patches whether approved or denied.

Policy Management - Agents Policy Status

Info Center > Reporting > Reports > Policy Management - Agent Policy Status

- Displays only if the **Policy Management** add-on module is installed.

The **Agents Policy Status** report definition generates a policy status report. Can be filtered by:

- **Agent's Policy Status**
- **Policy Object Type**
- **Policy Object Status**

Policy Management - Policy Info & Association

Info Center > Reporting > Reports > Policy Management - Policy Info & Association

- Displays only if the **Policy Management** add-on module is installed.

The **Policy Info & Association** report definition generates a report of policies and associations. Can be filtered by:

- **Policy Status**
- **Policy Object Type**

Security - Configuration

Info Center > Reporting > Reports > Security > Configuration

- Displays only if the **Security** add-on module is installed.
- Similar information is provided using **Security > Security Status, View Logs, and View Threats**.

The **Security - Configuration** report definition generates reports for the following types of security data maintained by the VSA.

- Install Time
- Installer
- Version
- License Expiration
- Assigned Profile
- Profile Details
- Alarm Settings

Security - Security

Info Center > Reporting > Reports > Security > Current Threats

- Displays only if the **Security** add-on module is installed.
- Similar information is provided using **Security > Security Status, View Logs, and View Threats**.

The **Security - Current Threats** report definition generates reports for the following types of security data maintained by the VSA.

- Summary
- Threat Category Summary
- Current Threats

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Security - Historical Threats

Info Center > Reporting > Reports > Security > Historical Threats

- Displays only if the [Security](#) add-on module is installed.
- Similar information is provided using [Security > Security Status](#), [View Logs](#), and [View Threats](#).

The [Security - Historical Threats](#) report definition generates reports for the following types of security data maintained by the VSA.

- Summary
- Threat Category Summary
- Current Threats

Time Selection

- [Select the Time Range Type](#) - Filters by a fixed type of date range.
- [Number Of Days](#) - Applies only if [Last N Days](#) is selected time range type.
- [Custom Start DateTime](#) - Applies only if [Fixed Range](#) is select time range type.
- [Custom End DateTime](#) - Applies only if [Fixed Range](#) is select time range type.

Security - KES Log

Info Center > Reporting > Reports > Security - KES Log

- Displays only if the [Security](#) add-on module is installed.
- [Agent > Agent Logs](#) ([page 31](#)) displays log entries by log type and machine ID.

The KES Log report definition generates a report of Endpoint Security log entries by machine ID.

Configure your report definition using the following parameters:

- [Number of days to query log*](#) - Number of days back from the current date/time to include in the report.
- [Show entries matching the following description \(use * for wildcards\)](#) - Enter a string to filter entries by their description. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- [Ignore machines without data](#) - Check this box to only display machine IDs that have data matching the other filter parameters.

Service Billing - Past Billed Invoices

Info Center > Reporting > Reports > Service Billing - Past Billed Invoices

- Displays only if the [Service Billing](#) add-on module is installed.

The [Past Billed Invoices](#) report definition generates a report listing billed invoices.

Time Selection

- [Select the Time Range Type](#) - Filters by a fixed type of date range.
- [Number Of Days](#) - Applies only if [Last N Days](#) is selected time range type.
- [Custom Start DateTime](#) - Applies only if [Fixed Range](#) is select time range type.
- [Custom End DateTime](#) - Applies only if [Fixed Range](#) is select time range type.

Service Billing - Sales Order Summary

Info Center > Reporting > Reports > Service Billing - Sales Order Summary

- Displays only if the [Service Billing](#) add-on module is installed.

The [Sales Order Summary](#) report definition generates a summary report of sales orders.

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Service Billing - Unbilled Revenue by Customer

Info Center > Reporting > Reports > Service Billing - Unbilled Revenue by Customer

- Displays only if the **Service Billing** add-on module is installed.

The **Unbilled Revenue by Customer** report definition generates a detailed or summary report of unbilled revenue, by customer.

Parameters

- **Detailed**
- **Summary**

Service Billing - Unbilled Revenue by Item Type

Info Center > Reporting > Reports > Service Billing - Unbilled Revenue by Item Type

- Displays only if the **Service Billing** add-on module is installed.

The **Unbilled Revenue by Item Type** report definition generates a detailed or summary report of unbilled revenue, by item type.

Parameters

- **Detailed**
- **Summary**

Service Billing - Work Order Summary

Info Center > Reporting > Reports > Service Billing - Work Order Summary

- Displays only if the **Service Billing** add-on module is installed.

The **Work Order Summary** report definition generates a summary report of work orders.

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Service Desk - Custom Tickets

Info Center > Reporting > Reports > Service Desk - Custom Tickets

- Displays only if the **Service Desk** add-on module is installed.

The **Custom Tickets** report definition generates a report displaying **Service Desk** ticket summary information and ticket details.

Configure your report definition using the following parameters.

General

- **Service Desk**

Info Center

- **Notes / Summary / Submitter Filter** - List only tickets or ticket counts containing this string in any note, summary line or submitter information line. Use * for wildcard.
- **Display all Tickets** - If checked, list all tickets individually.
- **Display Notes with each ticket** - If checked, display notes with each ticket.
- **Hide Hidden Notes** - If checked, hide hidden notes.
- **Display Ticket Status Chart for each Admin** - Displays a separate ticket status bar chart for each user plus for unassigned.
- **Display pie chart for each selected Ticket Category Column of Data** - Assignee, Status, Priority, Category, Sub Category.

Time Range

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Display all open tickets plus tickets closed within the last N days** - Applies only if Last N Days is selected time range type.
- **Custom Start DateTime** - Applies only if Fixed Range is select time range type.
- **Custom End DateTime** - Applies only if Fixed Range is select time range type.

Columns

Values for all desk definitions are displayed in the drop-down lists. Select multiple items using Ctrl+Click and Shift+Click, unless otherwise noted.

- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.

Filters

- **Assignee Filter** - Only one item can be selected.
- **Status Filter**
- **Priority Filter**
- **Category Filter**
- **SubCategory Filter** - Only displays subcategories for selected categories in the **Category Filter**.

Service Desk - Service Goals

Info Center > Reporting > Reports > Service Desk - Service Goals

- Displays only if the **Service Desk** add-on module is installed.

The **Service Goals** report definition generates a report displaying summary information and ticket details related to meeting **Service Desk** goals.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if Last N Days is selected time range type.
- **Custom Start DateTime** - Applies only if Fixed Range is select time range type.
- **Custom End DateTime** - Applies only if Fixed Range is select time range type.

Parameters

- **Include Only Tickets with Goals** - If checked, only tickets with goals are displayed.
- **Select Report-By Type** - Service Goals by Ticket, Ticket Number.
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.

Service Desk - Service Hours

Info Center > Reporting > Reports > Service Desk - Service Hours

- Displays only if the **Service Desk** add-on module is installed.

The **Service Hours** report definition generates a report displaying summary information and ticket details related to **Service Desk** hours worked.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Parameters

- **Include Only Tickets with Goals** - If checked, only tickets with goals are displayed.
- **Select Report-By Type** - **Service Hours by Ticket**, **Service Hours by Contributor**, **Service Hours by Organization**.
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.

Service Desk - Service Times

Info Center > Reporting > Reports > Service Desk - Service Times

- Displays only if the **Service Desk** add-on module is installed.

The **Service Times** report definition generates a 12-month report, starting with a specified month and year, showing how many tickets have been created, closed, resolved, past due within fixed time buckets.

Configure your report definition using the following parameters:

Parameters

- **Month** - Select a month.
- **Year** - Select a year.
- **Display Tickets Created** - If checked, display tickets created.
- **Display Tickets Closed** - If checked, display tickets closed.
- **Display Tickets Resolved** - If checked, display tickets resolved.
- **Display Tickets Past Due** - If checked, display tickets past due.
- **Display Ticket Service Time Details Tables** - If checked, display tickets detail tables.

Service Desk - Service Volumes

Info Center > Reporting > Reports > Service Desk - Service Volumes

- Displays only if the **Service Desk** add-on module is installed.

The **Service Volumes** report definition generates a 12-month report, starting with a specified month and year, showing the number of tickets in each month that belong to each possible value in a specified ticket column.

Configure your report definition using the following parameters:

Parameters

- **Group by** - Select the column to group by.

- **Sort Column Direction** - Ascending, Descending.
- **Month** - Select a month.
- **Year** - Select a year.
- **Display Ticket Volumes Chart** - If checked, display a tickets volumes chart.

Service Desk - Tickets

Info Center > Reporting > Reports > Service Desk - Tickets

- Displays only if the **Service Desk** add-on module is installed.

The **Tickets** report definition generates a report displaying **Service Desk** ticket summary information and ticket details.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Display all open tickets plus tickets closed within the last N days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Parameters

- **Notes / Summary / Submitter Filter** - List only tickets or ticket counts containing this string in any note, summary line or submitter information line. Use * for wildcard.
- **Display all Tickets** - If checked, list all tickets individually.
- **Display Notes with each ticket** - If checked, display notes with each ticket.
- **Hide Hidden Notes** - If checked, hide hidden notes.
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.
- **Display Ticket Status Chart for each Admin** - Displays a separate ticket status bar chart for each user plus for unassigned.
- **Display pie chart for each selected Ticket Category Column of Data** - Assignee, Status, Priority, Category, Sub Category.

Column Filters

Values for all desk definitions are displayed in the drop-down lists. Select multiple items using **Ctrl+Click** and **Shift+Click**, unless otherwise noted.

- **Assignee Filter** - Only one item can be selected.
- **Status Filter**
- **Priority Filter**
- **Category Filter**
- **SubCategory Filter** - Only displays subcategories for selected categories in the **Category Filter**.

Software - Software Applications Changed

Info Center > Reporting > Reports > Software - Software Applications Changed

- Similar information is provided using **Audit > Add/Remove** (page 137).

The **Software Applications Changed** report definition generates a report displaying lists of applications added to and removed from machine IDs. Uses data collected from the latest audit.

Note: This report was called the **Software - Add/Removes Programs** report before the Kaseya 2 release.

Configure your report definition using the following parameters:

- **Add/Remove List Item Filter** - Enter a string to filter items by their name. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **List machine IDs that contain each application** - If checked, then the machine ID of each machine add/remove program is listed.

Software - Software Applications Installed

[Info Center](#) > [Reporting](#) > [Reports](#) > [Software - Software Applications Installed](#)

- Similar information is provided using [Audit](#) > [Installed Applications](#) (page 136),

The **Software Applications Installed** report definition generates a report displaying each unique application found on all machines. The total number of unique copies of the application are also listed. Uses data collected from the latest audit.

Configure your report definition using the following parameters:

- **Application Filter** - Filters by application name (theApp.exe).
- **Product Name Filter** - Filters by product name string as provided by the software vendor.
- **Description Filter** - Filters by software description string as provided by the software vendor.
- **Manufacturer Filter** - Filters by software vendor name.
- **Version Filter** - Filters by software version number.
- **Show Unregistered Applications** - If checked, includes programs not in the registry. Registered applications place an App Paths key in the registry identifying the location of their main executable. Sorting on this value is a good way to separate main applications from all the helper and secondary applications.
- **List machine IDs that contain each application** - If checked, then the machine ID of each machine installed with the program is listed.
- **Display Column(s)** - Application, Product, Description, Manufacturer, Version.
- **Sort By** - Application, Product, Description, Manufacturer, Version.

Software - Software Licenses

[Info Center](#) > [Reporting](#) > [Reports](#) > [Software - Software Licenses](#)

- Similar information is provided using [Audit](#) > [Software Licenses](#) (page 137).

The **Software Licenses** report definition generates a report listing the number of software licenses found in a group of machines. This report lists the total number of licenses and the number of unique licenses found across all machines. Uses data collected from the latest audit.

Configure your report definition using the following parameters:

- **Show Publisher matching** - Filters by software vendor name.
- **Show Title matching** - Filters by software title.
- **Do Not List Machine IDs** - Machine IDs are not listed.
- **List Machine IDs** - The machine ID of each machine installed with the application is listed.
- **List Machine IDs by License Code** - License codes and product keys installed on each machine are displayed.

Software - Software Licenses Summary

[Info Center](#) > [Reporting](#) > [Reports](#) > [Software - Software Licenses Summary](#)

- Similar information is provided using [Audit](#) > [Software Licenses](#) (page 137).

The **Software Licenses** report definition generates a table summarizing the licenses on all machines in a group or view. Uses data collected from the latest audit. This report presents four tables of information summarizing the following:

- **Servers** - Lists all server types found and the number of machines running that server OS.
- **Workstations** - Lists all workstation types found and the number of machines running that workstation OS.
- **Microsoft Office Licenses** - Lists the number of machines with each version of Microsoft Office loaded.
- **Other Applications** - Summarizes the number of machines with each application license found that is not contained in the first 3 tables.

Configure your report definition using the following parameters:

- **Show Publisher matching** - Filters by software vendor name.
- **Show Title matching** - Filters by software title.

Software - Software Operating Systems

Info Center > Reporting > Reports > Software - Operating Systems

The **Operating Systems** report definition generates a composite view chart of all operating systems found on all machine IDs.

Note: Each machine reports its operating system type and version with each check-in. Audit does not have to complete to obtain operating system information. Therefore, the number of operating systems reported by this report may be higher than the number of licenses reported for that operating system if all machines have not completed an audit.

Configure your report definition using the following parameters:

- **Show Pie chart**
- **Show Bar chart**
- **Show Table**

Software Deployment - Profile Status by Machine

Info Center > Reporting > Reports > Software Deployment - Profile Status by Machine

- Displays only if the **Software Deployment and Update** add-on module is installed.

The **Profile Status by Machine** report definition generates a report showing the compliance status of machines managed by **Software Deployment and Update**.

- **Display Options** - Detailed or Summary

Software Deployment - Recent Deployments

Info Center > Reporting > Reports > Software Deployment - Recent Deployments

- Displays only if the **Software Deployment and Update** add-on module is installed.

The **Recent Deployments** report definition generates a report listing recent deployments.

Time Range

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if Last N Days is selected time range type.
- **Custom Start DateTime** - Applies only if Fixed Range is select time range type.
- **Custom End DateTime** - Applies only if Fixed Range is select time range type.

Software Deployment - Software Installed by Machine

Info Center > Reporting > Reports > Software Deployment - Software Installed by Machine

- Displays only if the **Software Deployment and Update** add-on module is installed.

The **Software Installed by Machine** report definition generates a report showing the software titles installed on machines managed by **Software Deployment and Update**.

- **Display Options** - Detailed or Summary

Software Deployment - Machine Changes

Info Center > Reporting > Reports > Software Deployment - Machine Changes

- Displays only if the **Software Deployment and Update** add-on module is installed.

The **Machine Changes** report definition generates a report showing the software titles and version changes on machines managed by **Software Deployment and Update**.

Comparison Parameters

- **Compare with Machine's own Baseline Scan** - Displays all machine software changes found on each machine by comparing the information from the latest scan against the information from the baseline scan.
- **Compare to selected Machine ID** - Displays all machine software changes found on each machine by comparing the information from the latest scan against the scan from a *selected machine ID*. Use this function to identify differences in a group of machines when compared against the standard for the group.
- **Use Baseline Scan** - Enabled if **Compare to selected machine ID** is selected. If checked, the selected machine ID's baseline scan is used for comparison instead of the selected machine ID's latest scan.

Display Options

- **Show Updates** - Machines with updated software.
- **Show Adds** - Machines with software added.
- **Show Removes** - Machines with software removed.
- **Show No Changes** - Machines with no software changes.
- **Show Unprofiled** - Machines with no assigned profiles.

Ticketing - Customizable Ticketing

Info Center > Reporting > Reports > Ticketing > Customizable Ticketing

- Similar information is provided using Ticketing > [View Summary \(page 400\)](#).

The **Customizable Ticketing** report definition generates a report listing all **Ticketing** module tickets assigned to selected organizations, machine groups, machines, departments, or staff records.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Display all open tickets plus tickets closed within the last N days** - Applies only if **Last N Days** is selected time range type.
- **Custom Start DateTime** - Applies only if **Fixed Range** is select time range type.
- **Custom End DateTime** - Applies only if **Fixed Range** is select time range type.

Parameters

- **Display Ticket Status Chart for each Admin** - Displays a separate ticket status bar chart for each user plus for unassigned.
- **Display pie chart for each selected Ticket Category** - Assignee, Status, Category, Priority.
- **Display none** - Do not list individual tickets in the report.
- **Display all tickets** - List all tickets individually.
- **Display all tickets with notes** - List all tickets, include both public and hidden notes.
- **Display all tickets but hide hidden notes** - List all tickets, include public notes but hide hidden notes.

Filters

- **Notes/Summary/Submitter Field** - Enter a string to filter tickets by their notes or summary line or submitter fields. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Assignee Filter** - Filter tickets by Assignee.
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.
- **Status** - Filter tickets by Status
- **Category** - Filter tickets by Category.
- **Priority** - Filter tickets by Priority.
- **Resolution** - Filter tickets by Resolution.
- **(Custom Fields)** - Filter tickets by one or more Custom Fields.

Columns

Select the tickets columns included in the report. All columns are included by default.

Ticketing - Ticketing

Info Center > Reporting > Reports > Ticketing > Ticketing

- Similar information is provided using Ticketing > View Summary (page 400).

The **Ticketing** report definition generates a report listing all **Ticketing** module tickets assigned to selected organizations, machine groups, machines, departments, or staff records.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Display all open tickets plus tickets closed within the last N days** - Applies only if Last N Days is selected time range type.
- **Custom Start DateTime** - Applies only if Fixed Range is select time range type.
- **Custom End DateTime** - Applies only if Fixed Range is select time range type.

Parameters

- **Display Ticket Status Chart for each Admin** - Displays a separate ticket status bar chart for each user plus for unassigned.
- **Display pie chart for each selected Ticket Category** - Assignee, Status, Category, Priority.
- **Notes / Summary / Submitter Filter** - List only tickets or ticket counts containing this string in any note, summary line or submitter information line. Use * for wildcard.
- **Display none** - Do not list individual tickets in the report.
- **Display all tickets** - List all tickets individually.
- **Display all tickets with notes** - List all tickets, include both public and hidden notes.
- **Display all tickets but hide hidden notes** - List all tickets, include public notes but hide hidden notes.

- **Notes/Summary/Submitter Field** - Enter a string to filter tickets by their notes or summary line or submitter fields. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- Filter tickets by
 - **Assignee**
 - **Status**
 - **Category**
 - **Priority**
- **Sort Column** - Select the column to sort tickets on.
- **Sort Direction** - Ascending, Descending.

Time Tracking - Timesheet Summary

Info Center > Reporting > Reports > Time Tracking > Timesheet Summary

The **Timesheet Summary** report definition generates a report listing the status of all timesheets for a specified date range.

Configure your report definition using the following parameters.

Time Selection

- **Custom Start DateTime** - The start date.
- **Custom End DateTime** - The end date.

Parameters

- **Choose Group Type** - Grouped by **Period** or by **Status**.
- **Staff List** - The staff to include in the report. The list comprises all staff with timesheets that your scope authorizes you to see.

Note: For each staff record and time period, a timesheet is only created if at least one time entry is added to the timesheet.

Time Tracking - Timesheet Entries

Info Center > Reporting > Reports > Time Tracking > Timesheet Entries

The **Timesheet Entries** report definition generates a report listing all timesheet entries for a specified date range.

Configure your report definition using the following parameters.

Time Selection

- **Custom Start DateTime** - The start date.
- **Custom End DateTime** - The end date.

Parameters

- **Staff List** - The staff to include in the report. The list comprises all staff with timesheets that your scope authorizes you to see.

Management Dashboard

Info Center > Dashboard > Management Dashboard

The **Management Dashboard** page shows the current status of all agent machines a VSA user is authorized to see. The dashboard comprises a set of dashlets, with each dashlet displaying a unique

metric.

- All agent dashlets provide drill down capability to show the list of individual agent machines in that dashlet.
- Dashboards obey scope and **machinelD/groupID** (page 23) filtering.

Dashlets displayed on this page include:

- **Machines Online**
- **Servers Online**
- **Servers Offline**
- **Agents Pending Reboot**
- **Agents Missing Patches with Patch Policy**
- **Agents Out of Compliance** with assigned **Policy Management** policies.
- **Agents with No Policies** assigned by **Policy Management**.
- **Agents Suspended**
- **Machines with Low Disk Space**
- **Agents in Unnamed Group**
- **Agents Missing Patches with No Patch Policy**
- **Top 10 Machines with Low Disk Space**
- **Agent Procedure Pending Approval**
- **Logged on Administrators**

Actions

- Click any dashlet to show a list of individual machines and devices in that dashlet.

View Dashboard

Info Center > Dashboard > View Dashboard

The **View Dashboard** page gives you a quick view of the total system's status, highlighting the machine IDs and tasks you need to work on first. The results displayed by the dashboard depend on the **Machine ID / Group ID filter** (page 556). You can manage **tasks** and send **messages** to other users using the dashboard. Customize the dashboard display using Info Center > **Layout Dashboard** (page 211).

Agent Status

Summarizes the online status of all machine IDs matching the current machine ID / group ID filter. Gives you an at-a-glance count of how many machines are **online**, have **users logged into** them, have been offline for **less than 30 days** and offline for **over 30 days** and the **total number of agents** matching the current machine ID / group ID filter.

Patch Status

Uses a pie chart to highlight machines missing patches and matching the current machine ID / group ID filter. The chart displays with or without applying a patch policy.

- Click the **Use Policy** button to apply the **Patch Policy** (page 559) when generating the pie chart.

Note: The Patch Policy incurs a significant performance penalty. If you have a lot of machine IDs this pie chart takes a long time to generate when using the patch policy.

- Click the **Hide Policy** button to generate the pie chart without the patch policy. This shows all missing patches including those denied by patch policy.

- Clicking on any pie segment opens a sub window listing all machine IDs that make up that pie segment.

Operating Systems

Uses a pie chart to show the mix of operating systems in use, for machines matching the current machine ID / group ID filter. Clicking any pie segment opens a sub window listing all machine IDs that make up that pie segment.

Tickets

Lists recent tickets issued against the machine IDs matching the current machine ID / group ID filter. Applies to [Ticketing](#) module tickets only.

System Status

Identifies the number of current and total VSA users and [Portal Access](#) (page 67) users. Also displays the size of the database, the database size per machine account and the last backup date.

Tasks

Use this section to create, edit, and monitor tasks you or other users need to perform. A pop up window alerts you when new tasks created for you have been added to your task list. Additional pop ups occur when the task becomes past due. You can have the system remind you of a past due task again, by clicking the [Snooze](#) button when the task reminder dialog box displays. You can clear all outstanding task notification messages by clicking the [Clear Snooze](#) button on the System > [Preferences](#) (page 353) page.

Messages

Use this section to send messages to other VSA users. Other VSA users see the messages as popup windows. Messages you have received are listed in the lower part of this pane.

Note: Send messages to machine users using [Remote Control](#) > [Send Message](#) (page 341).

Layout Dashboard

[Info Center](#) > [Dashboard](#) > [Layout](#)

The [Layout Dashboard](#) page displays/hides each section of the [View Dashboard](#) (page 210) page and sets the order they appear, from top to bottom. To display an item, check the box next to the item.

Two items have additional customization control: [Tickets](#), and [Messages](#). Both display time dependent data. To make it easy to quickly distinguish new item from old items, you can specify different highlight colors from data rows depending on how recently the data item was generated.

Recommendation

- Highlight the most recent tickets and messages in red. All tickets and messages created in the last N days are **highlighted in red**.
- Highlight the next most recent tickets and messages in yellow. All tickets and messages that are older than the red highlight date but more recent than the number entered are **highlighted in yellow**.
- Disable highlighting by setting the number of days to zero.

Chapter 7

Monitor

In This Chapter

Monitor Overview.....	214
Monitor Terms and Concepts.....	216
Dashboard List.....	219
Dashboard Settings.....	227
Alarm Summary.....	227
Suspend Alarm.....	229
Live Counter.....	230
Monitor Lists.....	231
Update Lists By Scan.....	232
Monitor Sets.....	234
SNMP Sets.....	241
Alerts.....	248
Event Log Alerts.....	276
SNMP Traps Alert.....	283
Assign Monitoring.....	286
Monitor Log.....	291
System Check.....	293
Assign SNMP.....	297
SNMP Log.....	305
Set SNMP Values.....	306
Set SNMP Type.....	308
Parser Summary.....	309
Log Parser.....	312
Assign Parser Sets.....	317
Viewing Log Monitoring Entries.....	322

Monitor Overview

Monitor

The **Monitoring** module in **Virtual System Administrator™** provides six methods of monitoring machines and log files:

- **Alerts** - Monitors events on *agent* machines.
- **Event Log Alerts** - Monitors events in the event logs of *agent* machines.
- **Monitor Sets** - Monitors the performance state on *agent* machines.
- **SNMP Sets** - Monitors the performance state on *non-agent devices*.
- **System Check** - Monitors events on *non-agent* machines.
- **Log Monitoring** - Monitors events in *log files*.

You can monitor the health in real time of managed machines and SNMP devices and be notified immediately if any problems arise. When programmable alarms are triggered, **Monitor** executes email notifications, procedures and job ticketing, for such problems and state changes as:

- When any critical server or desktop computer goes off-line.
- When a machine user disables remote control.
- When any software application is added or removed.
- When the hardware configuration changes.
- When the computer is running low on disk space.
- When a specific event or any event log entry is generated.
- When any protection policy violation occurs.
- When any agent procedure fails execution.
- When an unapproved application attempts to access the network.
- When an unapproved application attempts to access a protected file.
- When a new device appears on the local area network.
- When an external log records a specific log entry.

In addition to generating alert notifications when **event log entries** are generated, event log entries collected from your managed machines are stored on the VSA. The event log data is always available, even if the managed machine goes offline or suffers a hard failure. Event log data is presented in a familiar and concise form using the Agent > **Agent Logs** (*page 31*) page, as well as Info Center > Reporting > Reports > Logs.

Note: You can download a **Monitoring Configuration**

(http://help.kaseya.com/webhelp/EN/VSA/7000000/EN_monitoringconfiguration70.pdf#zoom=70&navpanes=0) PDF from the first topic of online user assistance.

Note: You can download a **Configuring Log Parsers Step-by-Step**

(http://help.kaseya.com/webhelp/EN/VSA/7000000/EN_logparsers70.pdf#zoom=70&navpanes=0) PDF from the first topic of online user assistance.

Note: **Kaseya Monitor™ Service** (<http://www.kaseya.com/services/it-services.aspx>) extends monitoring past nine-to-five. By out-tasking systems management and monitoring during off-hours, MSPs can offer customers 24/7/365 "Always-On" monitoring.



Note: Any agent used for monitoring must be updated using the Agent > **Update Agent** (*page 72*) page.

Function	Description
Dashboard List (page 219)	Provides multiple monitoring views.
Dashboard Settings (page 227)	Users can customize the Dashboard List page.
Alarm Summary (page 227)	Lists alarms for monitored machines.
Suspend Alarms (page 229)	Suspends alarm notifications for specific machine IDs.
Live Counter (page 230)	Displays live performance counter data for a selected machine ID.
Monitor Lists (page 231)	Configures the monitor list objects for monitoring.
Update Lists By Scan (page 232)	Scans machines for monitor counters and services.
Monitor Sets (page 234)	Configures monitor sets.
SNMP Sets (page 241)	Configures SNMP monitor sets.
Add SNMP Object (page 246)	Manages SNMP MIB objects.
Alerts (page 248)	Configures monitor alerts for machines.
Event Log Alerts (page 276)	Triggers an alert for an event log entry.
SNMP Traps Alert (page 283)	Configures alerts for SNMP Trap event log entries created on selected managed machines.
Assign Monitoring (page 286)	Assigns, removes and manages alarms of monitor sets on machines.
Monitor Log (page 291)	Views monitor log data in chart and table format.
System Check (page 293)	Assigns, removes and manages alarms for system checks on machines.
Assign SNMP (page 297)	Assigns, removes and manages alarms of SNMP monitor sets on devices.
SNMP Log (page 305)	Views SNMP log data in chart and table format.
Set SNMP Values (page 306)	Sets SNMP values on the specified device.
Set SNMP Type (page 308)	Assigns SNMP types to SNMP devices.
Parser Summary (page 309)	Defines alerts for parser sets and copy parser set assignments to multiple machine IDs.
Log Parser (page 312)	Defines log parsers and assigns them to machine IDs.
Assign Parser Sets (page 317)	Creates and assigns parsers sets to machine IDs and creates alerts on parser set assignments.

Monitor Terms and Concepts

The same alert management terms and concepts apply to all methods of monitoring.

Alerts and Alarms

- **Alerts** - An alert is created when the performance of a machine or device matches a pre-defined criteria or "alert condition".
- **Alarms** - *Alarms* are a graphical way of notifying the user that an *alert* has occurred. In many graphical displays throughout the VSA, when an alert exists, the VSA displays by default a red traffic light  icon. If no alert exists, a green traffic light icon  displays. These icons can be customized.
- **Logs** - Two logs distinguish between alerts and alarms.
 - **Alarm Log** - Tracks any *alarm that was created by an alert*.
 - **Monitor Action Log** - Tracks any *alert that was created*, whether or not an alarm or any other type of action was taken in response to the alert.

Actions

Creating an alarm represents only one *type of action* that can be taken when an alert occurs. Two other types of actions are notifications. They include **send an email** or **create a ticket**. A fourth type of action is to **run an agent procedure** to automatically respond to the alert. These four types of actions are called the **ATSE code**. Whether assigned to a machine ID, a group ID, or an SNMP device, the ATSE code indicates which types of actions will be taken for the alert defined.

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure
- E = **Email Recipients**

None of the ATSE actions are required to be set when configuring an alert. Both the alert and the ATSE action, including no action, are reported in the Info Center > Monitor - **Monitor Action Log** (*page 195*) report.

Types of Alerts

Types of alerts include:

- Discovery > **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>)
- Backup > Backup Alerts
- Monitor > **Alerts** (*page 248*) - These are specialized "fixed" alerts that are ready to apply to a machine.
- Monitor > **Assign Monitoring** (*page 286*)
- Monitor > **SNMP Traps Alert** (*page 283*)
- Monitor > **Assign SNMP** (*page 297*)
- Monitor > **System Checks** (*page 293*)
- Monitor > **Parser Summary** (*page 309*)
- Monitor > **Assign Parser Sets** (*page 317*)
- Patch Management > Patch Alerts
- Remote Control > Offsite Alerts
- Security > Apply Alarm Sets

Other add-on modules have alerts not listed here.

Six Methods of Monitoring

Each of the six methods of monitoring in **Virtual System Administrator™** is either *event-based* or *state-based*.

- Event-based
 - **Alerts** - monitors events on *agent* machines
 - **Event Log Alerts** - monitors events in the event logs of *agent-installed* machines
 - **System Check** - monitors events on *non-agent* machines
 - **Log Monitoring** - monitors events in *log files*
- State-based
 - **Monitor Sets** - monitors the performance state on *agent* machines
 - **SNMP Sets** - monitors the performance state on *non-agent devices*

Event-Based Alerts

Alerts (page 248), **System Check** (page 293), Event Log Alerts and **Log Monitoring** (page 312) represent **event-based alert** that occur perhaps once. For example a backup may fail. Even if the backup succeeds later, the failure of the backup is a historical event in the alarm log. If an alarm is created for this type of event, then *the alarm remains "open" in the alarm log even if the alert condition recovers*. Typically you use the **Alarm Summary** (page 227) page to review alarms created by event-based alerts. When the issue is resolved you "close" the alarm.

Event-based alerts are usually easier to configure, since the possibilities are reduced to whether one or more of the events happened or did not happen within a specified time period.

State-Based Alerts

Monitor set (page 234) counters, services, and processes and **SNMP set** (page 241) objects are either currently within their expected state range or outside of it and display as red or green alarm icons *dynamically* in monitoring dashlets. These are known as **state-based alerts**.

- *If an alert condition currently exists, monitor dashlets (page 219) show a red alarm icon.*
- *If an alert condition does not currently exist, monitor dashlets show a green alarm icon.*

If you create an alarm for state-based alerts, they'll create alarm entries in the alarm log just like event-based alarms, which you can then choose to close. But because state-based alerts typically go in and out of an alert condition dynamically, you may want to avoid creating an alarm each time this happens. Instead use the **Network Status** (page 223) dashlet to identify the *current status* of state-based alerts. Once the issue is corrected on the machine or device, the status of the alert automatically returns to a green icon. You don't have to manually "close" the alert in this dashlet.

Note: If you do decide to create traditional alarms for monitor sets and off-line alerts specifically, these two types of alerts can be closed automatically when they recover. See the **Enable auto close of alarms and tickets** checkbox on the **System > Configure** (page 377) page.

Typically state-based alarms require more thought to configure than event-based alarms, because the intent is to measure the level of performance rather than outright failure.

Dashboards and Dashlets

The **Dashboard List** page is the VSA's primary method of visually displaying monitoring data, including alerts and alarms. The **Dashboard List** page maintains configurable monitoring windows called **Dashboard Views**. Each dashboard contains one or more panes of monitoring data called **Dashlets**. Each VSA user can create their own customized dashboards. Types of dashlets include:

- **Alarm List** (page 220)
- **Alarm Network Status** (page 220)
- **Alarm Rotator** (page 222)
- **Alarm Ticker** (page 223)
- **Network Status** (page 223)
- **Group Alarm Status** (page 223)
- **Monitoring Set Status** (page 224)

Monitor

- [Monitor Status](#) (page 226)
- [Machines Online](#) (page 226)
- [Top N - Monitor Alarm Chart](#) (page 226)

Reviewing Alarms

All alert conditions that have the [Create Alarm](#) checkbox checked—both state-based alarms and event-based alarms—are recorded in the [alarm log](#). An alarm listed in the alarm log does not represent the *current status* of a machine or device, rather it is a *record* of an alarm that has occurred *in the past*. An alarm log record remains [Open](#) until you close it.

Created alarms can be, reviewed, [Closed](#) or [Deleted...](#) using:

- Monitor > [Alarm Summary](#) (page 227)
- Monitor > Dashboard List > any [Alarm Summary Window](#) (page 221) within a dashlet
- Agent > Agent Logs > [Alarm Log](#) (page 31)
- [Live Connect](#) (page 344) > Agent Data > Agent Logs > Alarm Log

Created alarms can also be reviewed using:

- Monitor > Dashboard List > [Alarm List](#) (page 220)
- Monitor > Dashboard List > [Alarm Network Status](#) (page 220)
- Monitor > Dashboard List > [Alarm Rotator](#) (page 222)
- Monitor > Dashboard List > [Alarm Ticker](#) (page 223)
- Monitor > Dashboard List > [Group Alarm Status](#) (page 223)
- Monitor > Dashboard List > [Monitor Set Status](#) (page 224)
- Monitor > Dashboard List > [Monitor Status](#) (page 226)
- Monitor > Dashboard List > [Top N - Monitor Alarm Count](#) (page 226)
- Monitor > Dashboard List > [KES Status](#) (page 226)
- Monitor > Dashboard List > [KES Threats](#) (page 226)
- Info Center > Reporting > Reports > Monitoring > Logs > Alarm Log
- Info Center > Reporting > Reports > Monitoring > Monitor Action Log

Reviewing Performance (with or without Creating Alarms)

You can review the *current status* of monitor sets and SNMP set performance results, *with or without creating alarms*, using:

- Monitor > [Live Counter](#) (page 230)
- Monitor > [Monitor Log](#) (page 291)
- Monitor > [SNMP Log](#) (page 305)
- Monitor > Dashboard > [Network Status](#) (page 223)
- Monitor > Dashboard > [Group Alarm Status](#) (page 223)
- Monitor > Dashboard > [Monitoring Set Status](#) (page 224)
- Info Center > [Reporting](#) (page 142) > Reports > Monitoring > Logs

Suspending Alarms

The triggering of alarms can be suspended. The [Suspend Alarms](#) page suppresses [alarms](#) (page 550) for specified time periods, including recurring time periods. This allows upgrade and maintenance activity to take place without generating alarms. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms*.

Group Alarms

Alarms for alerts, event log alerts, system check, and log monitoring are automatically assigned to a [group alarm](#) category. If an alarm is created, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the [Group Alarm Status](#) (page 223) dashlet of the Monitor > [Dashboard List](#) page.

You can create new groups using the [Group Alarm Column Names](#) tab in Monitor > [Monitor Lists](#) (page 231). Group alarm column names are assigned to monitor sets using [Define Monitor Set](#) (page 235).

Dashboard List

[Info Center](#) > [Dashboard](#) > [Dashboard List](#)




[Monitor](#) > [Dashboard](#) > [Dashboard List](#)

- Similar information is provided using [Monitor](#) > [Alarm Summary](#) (page 227) and [Info Center](#) > [Reporting](#) > [Reports](#) > [Monitor Alarm Summary](#) (page 196).


The [Dashboard List](#) page is the VSA's primary method of visually displaying monitoring data, including alerts and alarms. The [Dashboard List](#) page maintains configurable monitoring windows called [Dashboard Views](#). Each dashboard contains one or more panes of monitoring data called [Dashlets](#). Each VSA user can create their own customized dashboards.

Adding Dashboard Views and Dashlets

To add a new dashboard:

1. Click  to create a new [Dashboard View](#). The new dashboard displays in a popup window.
2. Enter a [Title](#) and [Description](#) for your new dashboard.
3. Click the [Add Dashlets](#) tab. A side panel displays a list of dashlets. These choices include:
 - [Alarm List](#) (page 220)
 - [Alarm Network Status](#) (page 220)
 - [Alarm Rotator](#) (page 222)
 - [Alarm Ticker](#) (page 223)
 - [Network Status](#) (page 223)
 - [Group Alarm Status](#) (page 223)
 - [Monitoring Set Status](#) (page 224)
 - [Monitor Status](#) (page 226)
 - [Machines Online](#) (page 226)
 - [Top N - Monitor Alarm Chart](#) (page 226)
 - [KES Status](#) (page 226)
 - [KES Threats](#) (page 226)
4. Check as many checkboxes as you like, then click the [Add](#) button. The side panel closes and the [Dashlets](#) display in the [Dashboard View](#).
5. Move and resize the [Dashlets](#) within the [Dashboard View](#).
6. Click the [Delete](#) tab to delete dashlets already displayed in the [Dashboard View](#).
7. Click  to save the [Dashboard View](#). Click  to save the [Dashboard View](#) using a different title and description.
8. Click [Share](#) to share this [Dashboard View](#) with other users, user roles or to make it public for all users to use and edit.

Configuring Dashlet Options

You can size and position each dashlet within the [Dashboard View](#). You can also access additional configuration options for each dashlet by clicking the configure icon  located in the upper left hand corner of the dashlet. Common configuration options include:


- [Show Title Bar](#) - If checked, displays the dashlet with a title bar.
- [Title](#) - Specifies the title of the dashlet.

Monitor


- **Refresh Rate** - Specifies how often the data in the dashlet is refreshed.
- **Machine** - Filters the dashlet by machine ID. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Machine Group** - Filters the dashlets by group ID. Select <All Groups> to see all groups you are authorized to see.

Note: Dashlets are unaffected by the *main machine ID / machine group filter* (page 556) at the top of the VSA page.

Add Dashboard

Click  to create a new dashboard. The new dashboard displays in a popup window.

Title




Enter a title for your dashboard and click the filter icon  to filter the list of dashboards listed in the paging area. Include an asterisk (*) wildcard with the text you enter to match multiple records. Enter a different title to rename the dashboard.

My Dashboards

If checked, only the dashboards you are the owner of display.

View

Displays the view icons available for each dashboard.

-  - Click to view this dashboard.
-  - Click to configure this dashboard.
-  - Click to delete this dashboard.

Owner

The owner of the dashboard.

Title

The name of the dashboard.

Description

The description of the dashboard.

Load on Startup

If checked, this dashboard displays when the user logs in. Choices apply only to the currently logged in user.

Alarm List

[Dashboard](#) > [Dashboard List](#) > [Alarm List](#)

The **Alarm List** dashlet displays all alarms for all machine IDs matching the dashlet's machine ID/group ID filter. The display lists the most recent alarms first.

Alarm Network Status

[Dashboard](#) > [Dashboard List](#) > [Alarm Network Status](#)

Initially the **Alarm Network Status** dashlet displays each machine group as an icon. You can click any group icon to display the machines within that group. If a machine has even a single Open alarm, then

the icon for that machine displays a red exclamation point. Click any machine icon to display an [Alarm Summary Window](#) (page 221) of Open alarms for that machine.

Alarm Summary Window

[Dashboard](#) > [Dashboard List](#) > [Alarm Network Status](#)

[Dashboard](#) > [Dashboard List](#) > [Group Alarm Status](#)

[Dashboard](#) > [Dashboard List](#) > [Monitor Set Status](#)

The [Alarm Summary](#) window displays a filtered list of alarm log records. The filtering depends on how you accessed the window. An alarm listed in the alarm log does not represent the *current status* of a machine or device, rather it is a *record* of an alarm that has occurred *in the past*. An alarm log record remains Open until you close it.

Note: Within a dashlet, the [Alarm Summary](#) window displays *only* Open alarm log records. If you attempt to filter alarms using the Closed status within a dashlet, the dashlet will reset your selection to Open. Closing an alarm makes it disappear from this dashlet's alarm summary list. You can review both Open and Closed alarms using the [Alarm Summary](#) (page 227) page.

Filtering Alarms

Select or enter values in one or more of the following [Alarm Filter](#) fields. The filtering takes effect as soon as you select or enter a value.

- [Alarm ID](#) - A specific alarm ID.
- [Monitor Type](#) - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- [Alarm State](#) - Open or Closed. You can only select the Open status for an alarm listed in a dashlet [Alarm Summary Window](#).
- [Alarm Type](#) - Alarm or Trending.
- [Alarm Text](#) - Text contained in the alarm. Bracket text with asterisks, for example: `*memory*`
- [Filter Alarm Count](#) - The number of alarms displayed using the current filter criteria.

Closing Alarms

You can close alarm log records in one of two ways:

- Click the [Open](#) link in the [State](#) column of the [Alarm Summary](#) window.

Or:

1. Set the [Alarm State](#) drop-down list to Closed.
2. Select one or more alarms listed in the paging area.
3. Click the [Update](#) button.



Deleting Alarms

1. Select one or more alarms listed in the paging area.
2. Click the [Delete...](#) button.

Adding Notes

1. Enter a note in the [Notes](#) field.
2. Select one or more alarms listed in the paging area.
3. Click the [Update](#) button.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and .


Monitor

buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Select All/Unselect All









Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Alarm ID

Lists a system-generated and unique ID for each alarm. The expand icon  can be clicked to display specific alarm information.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369). Each dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Alarm Date

The date and time the alarm was created.

Type

The type of monitor object: Counter, Process, Service, SNMP, Alert, System Check, Security and Log Monitoring.

Ticket

If a ticket has been generated for an alarm a [Ticket ID](#) link displays. Clicking this link displays the ticket in the Ticketing > [View Ticket](#) (page 403) page. If no ticket has been generated for an alarm a [New Ticket...](#) link displays. Click this link to create a ticket for this alarm.

Name

The name of the monitoring object.

Alarm Rotator

[Dashboard](#) > [Dashboard List](#) > [Alarm Rotator](#)

The [Alarm Rotator](#) dashlet displays current alarms that have occurred within the last 10 minutes. Each alarm displays one at a time, in a rotating fashion, for 10 seconds. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Alarm Ticker

Dashboard > Dashboard List > Alarm Ticker

The **Alarm Ticker** dashlet displays current alarms that have occurred within a specified period. Each alarm displays one at a time, in a "ticker-tape" fashion, for 10 seconds. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Network Status

Dashboard > Dashboard List > Network Status

The **Network Status** dashlet is specific for machines assigned *monitor sets* or devices assigned *SNMP sets*. This dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

The value of this dashlet is that you can see the *current state* of monitor sets on machines or SNMP sets on devices *dynamically*.

Initially the **Network Status** dashlet displays each machine group as an icon. You can click any group icon to display the machines and SNMP devices within that group. If even a single monitor set or SNMP set is in an alarm state, then the icon for that machine or device displays a red exclamation point. Click any machine icon or device icon to display a list of monitor set alarms or SNMP set alarms that are *currently* outside their alarm thresholds. Alarms in this list are automatically removed as soon as the monitor set or SNMP set returns to a "no alarm" state.

Dismissed

You can manually force an alarm to return to a "no alarm" state by clicking the **Dismiss** link for that alarm. The "alarm" state will reappear again if the monitor set or SNMP set crosses its alarm threshold again. The timing of the reappearance depends on the alarm interval criteria defined for that monitor set or SNMP set.

Note: Dismissing an alarm *state* should not be confused with the **Open** or **Closed** status of an alarm *record* entered in the alarm log, which is displayed, for example, using the **Alarm Summary Window** (page 221). Alarm log entries can remain **Open** indefinitely, long after the alarm state has returned to "no alarm".

Group Alarm Status


Dashboard > Dashboard List > Group Alarm Status

The **Group Alarm Status** dashlet summarizes the alarm status of all **group alarm** (page 555) categories, for all machine IDs matching the *dashlet's* unique machine ID/group ID filter. Alarms for alerts, event log alerts, system check, and log monitoring are automatically assigned to a **group alarm** category. If an alarm is created, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the **Group Alarm Status** (page 223) dashlet of the Monitor > **Dashboard List** page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > **Monitor Lists** (page 231). Group alarm column names are assigned to monitor sets using **Define Monitor Set** (page 235).

Note: Do not confuse *group alarm categories* with *machine group IDs*.

- Click the **machine group ID** link to display the group alarm status of all machine IDs and SNMP device IDs included in that machine group ID.
- Click the **Machine ID/SNMP Device ID** link to display a **Monitor Set Status** (page 224) window for the machine ID and any SNMP devices linked to it.

Monitor

- Click any red icon  in the table to display the **Alarm Summary Window** (page 221) for that combination of *group alarm category and machine group ID* or *group alarm category and machine ID*.
- Click **Filter...** to filter a dashlet by group alarm category or by machine group ID. Click **Reset** to return a filtered dashlet back to its default. You can also re-order the display of group alarm categories.

Monitoring Set Status

Dashboard > Dashboard List > Monitoring Set Status

- You can also display a **Monitoring Set Status** dashlet using a **Group Alarm Status** dashlet, by clicking a **machine group ID** link, then a **machine ID** link.

The **Monitoring Set Status** dashlet displays all alarms assigned to a machine ID, whether created by **monitor set** (page 558), **alert** (page 549), **system check** (page 564), **SNMP set** (page 241), or **Log Monitoring** (page 555). Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Display only alarmed monitor objects




If checked, only alarmed monitor objects are displayed in the list.

Display only alarmed machines

If checked, only alarmed machines are displayed in the list.








First Row of Information

The first row of information displays:

- The **check-in status** (on page 552) icon - Click to display the **Live Connect** (page 344) window. Alt-click to display the **Machine Summary** (page 131) page.
- The machine status icon  - Click to display the **Machine Status** (page 225) popup window. This window enables you to set up a permanent display of charts or tables of monitor set objects for a specific machine ID. Applies to monitor set objects only—not alerts, system-checks or SNMP sets.
- The expand icon  - Click to display all alarms assigned to a machine ID.
- The collapse icon  - Click to display only the header description of each alarm assigned to a machine ID.
- The **machine ID.group ID** (page 556).

Monitor Sets



If a monitoring set is assigned to a machine ID, the following displays below the name of the monitor set:

- The triggered alarm  or no-alarm  status of the monitoring set.
- The expand icon  - Click to display collection and threshold information.
- The **Quick Status** link or the quick chart icon  - Click to display a **Quick Status Monitor** popup window. This feature enables you to select *any* monitor set counter, service or process from *any* machine ID and add it to the same single display window. Using **Quick Status**, you can quickly compare the performance of the same counter, service or process on different machines, or display selected counters, services and processes from different monitor sets all within a single view. SNMP sets provide a similar **Quick Status** view for selected SNMP objects. *Any Quick Status view you create exists only for the current session.* Use the **Machine Status** (page 225) icon  to permanently save chart display selections.
- The monitoring log icon  - Click to display the **monitoring log** (page 291) for this single alarm counter in a popup window.
- The live monitoring log icon  - Click to display current, ongoing counter log information in a popup window.

- The monitor set object name.
- For triggered alarms, the [Alarm](#) hyperlink displays. Click to display the [Alarm Summary Window](#) (page 221). The [Alarm Summary Window](#) is restricted to just Open alarms for the selected monitor set object and machine ID.



Alerts

If an alert is assigned to a machine ID, the following displays with each alert:

- The triggered alarm  or no-alarm  status of the alert.
- The alert type.
- For triggered alarms, the [Alarm](#) hyperlink displays. Click to display the [Alarm Summary Window](#) (page 221). The [Alarm Summary Window](#) is restricted to just Open alerts for the selected machine ID.






System Checks

If a system check is assigned to a machine ID, the following displays with each system check:

- The triggered alarm  or no-alarm  status of the system check.
- The system check type.
- For triggered alarms, the [Alarm](#) hyperlink displays. Click to display the [Alarm Summary Window](#) (page 221). The [Alarm Summary Window](#) is restricted to just Open system checks for the selected machine ID.

SNMP Devices

If a SNMP set is assigned to a SNMP device, the following displays with each SNMP set object:

- The device status icon  - Click to set up a permanent display of charts or tables of monitor set objects for a specific SNMP device. Displays the [Device Status](#) (page 226) popup window.
- The IP address of the SNMP device.
- The name of the SNMP device.
- The name of the SNMP set assigned to the SNMP device. The following displays with each SNMP set:
 - The triggered  or no-alarm  status of the SNMP set.
 - The expand icon  - Click to display collection and threshold information.
 - The monitoring log icon  - Click to display the [SNMP log](#) (page 305) for this single alarm counter in a popup window.
 - The SNMP set object name.
 - For triggered alarms, the [Alarm](#) hyperlink displays. Click to display the [Alarm Summary Window](#) (page 221). The [Alarm Summary Window](#) is restricted to just Open alarms for the selected SNMP set object and SNMP device.

Machine Status

Dashboard > Dashboard List > Monitor Set Status > Machine Status icon 

The [Machine Status](#) popup window selects and displays charts or tables for [monitor set](#) (page 558) objects. The setup is specific for each machine ID and can be saved permanently. Applies to monitor set objects only. Monitor sets must be assigned to a machine ID before using this window.

- Click the [Setup...](#) button to select monitoring objects to display and to set the chart or table format.
- Click the [Save Position](#) button to save the selection and format of monitoring objects on the [Monitor Set Status](#) popup window.

Device Status

Dashboard > Dashboard List > Monitor Set Status > Machine Status icon 

The **Device Status** popup window selects and displays charts or tables for **SNMP devices** (page 562). The setup is specific for each SNMP device and can be saved permanently.

- Click the **Setup...** button to select monitoring objects to display and to set the chart or table format.
- Click the **Save Position** button to save the selection and format of monitoring objects on the **Monitor Set Status** popup window.

Monitor Status

Dashboard > Dashboard List > Monitor Status

The **Monitor Status** dashlet displays a bar chart showing the number of alarms created for the selected time interval. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. This dashlet can be customized using Monitor > **Dashboard Settings** (page 227).

Machines Online

Dashboard > Dashboard List > Machines Online

The **Machines Online** chart shows the percentage of servers and workstations online. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. This dashlet can be customized using Monitor > **Dashboard Settings** (page 227).

Top N - Monitor Alarm Chart

Dashboard > Dashboard List > Top N - Monitor Alarm Chart

The **Top N - Monitor Alarm Chart** dashlet displays a bar chart showing which machines have the *most* alarms for the selected time interval. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. The chart shows up to 10 machines. This dashlet can be customized using Monitor > **Dashboard Settings** (page 227).

KES Status

Dashboard > Dashboard List > KES Status

The **KES Status** dashlet displays different views of the security status of machine IDs using Endpoint Security protection. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. The three views of security status are:

- **Machine Configuration**
- **Scan Details**
- **Profile Chart**

Note: This dashlet does not display unless the Endpoint Security add-on module is installed for the VSA.

KES Threats

Dashboard > Dashboard List > KES Threats

The **KES Threats** dashlet displays different views of the security threats reported for machine IDs using Endpoint Security protection. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. The three views of security threats are:

- **Most Recent**
- **Most Common**

- [Profile Chart](#)

Note: This dashlet does not display unless the Endpoint Security add-on module is installed for the VSA.

Dashboard Settings

[Info Center](#) > [Dashboard](#) > [Settings](#)

[Monitor](#) > [Dashboard](#) > [Dashboard Settings](#)

The [Settings](#) page enables you to customize controls for dashlets.

- [Turn notification sounds on or off for all popup monitoring windows](#) - Applies only to the [Monitor Set Status](#) (page 224) dashlet.
- The [Chart Total Monitor Alarms](#) and [Chart Top N Monitor Alarms](#) title and background colors are customizable. Each chart parameter is customizable, this includes the chart time interval and the number of machines referenced by the [Chart Top N Monitor Alarms](#).
- The [Customize machines online chart zone](#) specifies two percentages to create three zones of machines online:
 - The percentage of machines online, below which represents an alert condition.
 - The additional percentage of machines online, below which represents a warning condition.
- [Show refresh time](#)
- [Custom Dashboard Skin](#) - Select the border and titlebar style you want dashlets to display.

Alarm Summary

[Monitor](#) > [Status](#) > [Alarm Summary](#)

- Similar information is provided using [Monitor](#) > [Dashboard Lists](#) (page 219) and [Info Center](#) > [Reporting](#) > [Reports](#) > [Monitor](#).

The [Alarm Summary](#) page displays [alarms](#) (page 550) for all machine IDs that match the current [machine ID / group ID filter](#) (page 23). You can include additional filtering for listed alarms using fields in the [Alarm Filters](#) panel. You can also close alarms or re-open them and add notes to alarms.

Filtering Alarms

Select or enter values in one or more of the following [Alarm Filter](#) fields. The filtering takes effect as soon as you select or enter a value.

- [Alarm ID](#) - A specific alarm ID.
- [Monitor Type](#) - Counter, Process, Service, SNMP, Alert, System Check, Security or Log Monitoring.
- [Alarm State](#) - Open or Closed. You can only select the Open status for an alarm listed in a dashlet [Alarm Summary Window](#).
- [Alarm Type](#) - Alarm or Trending.
- [Alarm Text](#) - Text contained in the alarm. Bracket text with asterisks, for example: `*memory*`
- [Filter Alarm Count](#) - The number of alarms displayed using the current filter criteria.

Closing Alarms

You can close alarm log records in one of two ways:

- Click the [Open](#) link in the [State](#) column of the [Alarm Summary](#) window.

Or:

1. Set the [Alarm State](#) drop-down list to [Closed](#).

Monitor

2. Select one or more alarms listed in the paging area.
3. Click the [Update](#) button.



Deleting Alarms

1. Select one or more alarms listed in the paging area.
2. Click the [Delete...](#) button.

Adding Notes

1. Enter a note in the [Notes](#) field.
2. Select one or more alarms listed in the paging area.
3. Click the [Update](#) button.


Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Select All/Unselect All









Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Alarm ID

Lists a system-generated and unique ID for each alarm. The expand icon  can be clicked to display specific alarm information.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (*page 16*) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (*page 556*) displayed is based on the [Machine ID / Group ID filter](#) (*page 23*) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (*page 369*). Each dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Alarm Date

The date and time the alarm was created.

Type

The type of monitor object: Counter, Process, Service, SNMP, Alert, System Check, Security and Log Monitoring.

Ticket

If a ticket has been generated for an alarm a [Ticket ID](#) link displays. Clicking this link displays the ticket

in the Ticketing > [View Ticket](#) (page 403) page. If no ticket has been generated for an alarm a [New Ticket...](#) link displays. Click this link to create a ticket for this alarm.

Name

The name of the monitoring object.

Suspend Alarm

[Monitor](#) > [Status](#) > [Suspend Alarm](#)

The [Suspend Alarms](#) page suppresses [alarms](#) (page 550) for specified time periods, including recurring time periods. This allows upgrade and maintenance activity to take place without generating alarms. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms*. The list of machine IDs you can select depends on the [machine ID / group ID filter](#) (page 23) and the [scope](#) (page 369) you are using.

Clear All

Clears all time periods scheduled for suspending alarms for all selected machine IDs.

Add / Replace

Click [Add](#) to add a schedule time period when alarms will be suspended for selected machine IDs. Click [Replace](#) to remove suspend alarm time periods currently assigned to selected machine IDs and assign them a new single time period to suspend alarms.

Schedule

Click [Schedule](#) to schedule this task on selected machine IDs using the schedule options previously selected.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Clears a time period matching the date/time parameters for suspending alarms on selected machine IDs.

Run recurring

Check the box to make this task a recurring task. Enter the number of periods to wait before running this task again.

Suspend alarms




Select the duration of time during which alarms will be suspended.

Select All/Unselect All






Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.

Monitor

-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Next Suspend

Lists the start times when machine ID alarms are scheduled to be suspended.

Duration

Lists the duration of the time periods alarms are scheduled to be suspended.

Recur

If recurring, displays the interval to wait before running the task again.

Live Counter

Monitor > Status > Live Counter

The **Live Counter** page displays live **performance counter** (page 560) data for a selected machine ID. Only machines IDs assigned one or more monitor sets using **Assign Monitoring** (page 286) are listed on this page. The list of machine IDs you can select depends on the **machine ID / group ID filter** (page 23) and the **scope** (page 369) you are using.









Each specific **Live Counter** displays in a new window. Each window displays a bar chart with 75 data points containing the value of the counter object for the **Refresh Rate** specified. The chart refresh rate can be set between 3 and 60 seconds. The new data displays on the far right of the chart and the data moves from right to left as it ages.

Each bar within the chart displays in a specific color, which is determined by the alarm and warning thresholds of the monitor set counter object.

- **Red** - if alarming
- **Yellow** - if within warning threshold
- **Green** - if not alarming or not in warning threshold

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

(Machine.Group ID)

Lists the **Machine.Group IDs** (page 556) currently matching the **Machine ID / Group ID filter** (page 23) and that has been assigned one or more monitor sets. Click a machine ID to select a monitor set, refresh rate and one or more counters.

Select Monitor Set

Select a monitor set.

Refresh Rate

Enter a value from 3 to 60. This is the interval **Live Counter** uses to gather data.

Select Counter

Lists the counters included in a selected monitor set. Click a counter link to display a **Live Counter** window for that counter.

Monitor Lists

[Monitor](#) > [Edit](#) > [Monitor Lists](#)

The **Monitor Lists** page maintains the complete list of all objects, services and processes loaded on the Kaseya Server that are used to create **Monitor Sets** (page 234) and **SNMP Sets** (page 241). The **Monitor List** page also maintains user-defined **group alarms** (page 555).

Note: The **Counter Objects**, **Counters**, **Instances** and **Services** lists are populated by **Update Lists by Scan** (page 232). For most Windows machines **Update Lists by Scan** is run automatically. Additionally these lists, as well as **Services** and **Processes**, can be populated with the import of a **Monitor Set** (page 234). **MIB OIDs** can be populated by using the **Add SNMP Object** (page 246) page or by the import of a **SNMP Set** (page 241).

Counter Objects

This tab lists **counter objects** you can include in a **Monitor Set** (page 234). Monitor Set uses the **PerfMon** combination of **object/counter/instance** (page 560) to collect counter information.

Note: Counter Objects are the primary reference. The user needs to add a record of the counter object first, before adding records of the corresponding counters or instances.

Counters

This tab lists **counters** you can include in a **Monitor Set** (page 234). Monitor Set uses the **PerfMon** combination of object/counter/instance to collect counter information.

Counter Instances

This tab lists **counter instances** you can include in a **Monitor Set** (page 234). Monitor Set uses the **PerfMon** combination of object/counter/instance to collect counter information.

Note: Windows **PerfMon** requires that a counter object have at least one counter, but does not require an instance be available.

Services

This tab lists Windows **services** you can include in a **Monitor Set** (page 234) to monitor the activity of Windows Services. This list can also be populated by **Update Lists By Scan** (page 232) or the import of a **Monitor Set** (page 234).

Monitor

Processes

This tab lists Windows **processes** you can include in a **Monitor Set** (page 234) to monitor the transition of a process to or from a running state. A process is equivalent to an application. The processes list is *not* populated via **Update Lists by Scan** (page 232). This list can be populated by the import of a **Monitor Set** (page 234).

CMIB OIDs

This tab lists SNMP **MIB objects** you can include in **SNMP Sets** (page 241). SNMP sets monitor the activity of SNMP devices. This list can be populated with the import of a **SNMP Set** (page 241) or the execution of the **Add SNMP Object** (page 246) page. MIB objects are references to values that can be monitored on SNMP devices. Example: the MIB object `sysUptime` returns how much time has passed since the device was powered-up.

SNMP Devices

This tab defines broad categories of SNMP devices called **Set SNMP Types** (page 308). This enables the convenient assignment of SNMP sets to multiple SNMP devices, based on their SNMP type. Assignment can be either automatic or manual. See **SNMP Services** below for more information.



SNMP Services

This tab associates a `sysServicesNumber` with a SNMP type. A SNMP type is associated with a SNMP set using the **Automatic Deployment to** drop-down list in Monitor > SNMP Sets > **Define SNMP Set** (page 243). During a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) SNMP devices are automatically assigned to be monitored by SNMP sets if the SNMP device returns a `sysServicesNumber` associated with a SNMP type used by those SNMP sets. This table comes with pre-defined SNMP types and `sysServicesNumbers` for basic devices. System updates and updates provided by customers themselves can update this table.


Group Alarm Column Names

This tab maintains *user defined* **Group Alarm Column Names**. Pre-defined **group alarm** (page 555) column names do not display here. Use **Monitor Sets** (page 234) and **Define Monitor Sets** (page 235) to assign a monitor set to any group alarm column name. Group alarms are displayed using the **Dashboard List** (page 219) page.

Page Select

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Edit Icon

Click the edit icon  to edit the text of a list item.

Delete Icon

Click the delete icon  to delete a list item.

Update Lists By Scan

Monitor > Edit > Update Lists By Scan

The **Update Lists by Scan** page scans one or more machine IDs and returns lists of counter objects, counters, instances and services to select from when creating or editing a monitor set. A consolidated list of all scanned objects displays on the Monitor > **Monitor Lists** (page 231) page. Typically only a handful of machines of each operating system type needs to be scanned to provide a set of comprehensive lists on the **Monitor Lists** page. **Update Lists by Scan** also updates the list of event types available for

monitoring using Monitoring > [Event Log Alerts](#) (page 276). You can see the list of event types available by displaying the Agent > [Event Log Settings](#) (page 34) page. For newer Windows machines [Update Lists by Scan](#) need not be run more than once.

- **For Windows Machines Later than Windows 2000** - The discovery of new counter instances is managed entirely by the agent. For example, removable disks may be added to a machine. A new counter instance for a new removable disk will be discovered by the agent within a few hours. If a monitor set specifies the monitoring of that disk—either by specifying the letter of that drive or by using the *ALL counter instance—then data will start to be returned for that newly added disk. Any counters being monitored that stop are automatically restarted within the same discovery time period. All of this occurs independently of [Update Lists by Scan](#).
- **For Windows 2000 and Earlier Windows Machines** - Users may elect to run [Update Lists by Scan](#) to discover new counter objects on those machines. This is the only reason to run [Update Lists by Scan](#).

Run Now

Runs a scan immediately.

Cancel









Click [Cancel](#) to cancel execution of this task on selected managed machines.

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended


Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Last Scan

This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

Next Scan

This timestamp shows the next scheduled scan. Overdue date/time stamps display as **red text with yellow highlight**. A green  checkmark indicates the scan is recurring.

Monitor Sets

Monitor > Edit > Monitor Sets

The **Monitor Sets** page adds, imports or modifies monitor sets. Sample monitor sets are provided.

A monitor set is a set of **counter objects**, **counters**, **counter instances**, **services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter** (page 560), service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** (page 231).
2. Create and maintain monitor sets using Monitor > **Monitor Sets** (page 234).
3. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** (page 286).
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.
6. Review monitor set results using:
 - Monitor > **Monitor Log** (page 291)
 - Monitor > **Live Counter** (page 230)
 - Monitor > Dashboard > **Network Status** (page 223)
 - Monitor > Dashboard > **Group Alarm Status** (page 223)
 - Monitor > Dashboard > **Monitoring Set Status** (page 224)
 - Info Center > Reporting > Reports > Monitor > Monitor Set Report
 - Info Center > Reporting > Reports > Monitor > Monitor Action Log

Sample Monitor Sets

The VSA provides a growing list of sample monitor sets. The names of sample monitor sets begin with ZC. You can modify sample monitor sets, but its better practice to copy a sample monitor set and customize the copy. Sample monitor sets are subject to being overwritten every time the sample sets are updated during a maintenance cycle.


Monitoring using Apple OS X

Apple OS X supports process monitoring only. See **System Requirements** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm>).

Folder Trees

Monitor sets are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

Always Available

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

When a Folder is Selected

- **Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.

Note: See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 108) topic.

- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.
- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **New Monitor Set** - Opens the **Define Monitor Set** (page 235) window to create a new monitor set in the selected folder of the folder tree.
- **Import Monitor Set** - Imports a monitor set.

When a Monitor Set is Selected

- **Copy Monitor Set** - Copies the selected monitor set.
- **Export Monitor Set** - Exports the selected procedure.
- **Delete Monitor Set** - Deletes the selected procedure.

Creating Monitor Sets

1. Select a folder in the middle pane.
2. Click the **New Monitor Set** button.
3. Enter a name.
4. Enter a description.
5. Select a **group alarm** (page 555) category from the **Group Alarm Column Name** drop-down list. User defined group alarm column names are maintained using the **Monitor Lists** (page 231) page. Group alarms display on the **Dashboard List** (page 219) page.
6. Click **Save**. The **Define Monitor Sets** (page 235) window displays.

Note: Sample monitor sets do not display in the **Assign Monitoring** (page 286) > **Select Monitor Set** drop-down list. Create a copy of a sample monitor set by selecting the sample set in **Monitor Sets** (page 234) and clicking the **Save As** button. Your copy of the sample monitor set will display in the drop-down list. In a **SaaS** (page 564)-based VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

Define Monitor Sets

Monitor > Edit > Monitor Sets

- Select a monitor set in a folder.

The **Define Monitor Sets** window maintains a set of counter objects, counters, counter instances, services and processes included in a monitor set. This collection is drawn from a "master list" maintained using **Monitor Lists** (page 231). Sample monitor sets are provided.

Monitor Sets

A monitor set is a set of **counter objects**, **counters**, **counter instances**, **services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter** (page 560), service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

Monitor

The general procedure for working with monitor sets is as follows:

1. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** (page 231).
2. Create and maintain monitor sets using Monitor > **Monitor Sets** (page 234).
3. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** (page 286).
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.
6. Review monitor set results using:
 - Monitor > **Monitor Log** (page 291)
 - Monitor > **Live Counter** (page 230)
 - Monitor > Dashboard > **Network Status** (page 223)
 - Monitor > Dashboard > **Group Alarm Status** (page 223)
 - Monitor > Dashboard > **Monitoring Set Status** (page 224)
 - Info Center > Reporting > Reports > Monitor > Monitor Set Report
 - Info Center > Reporting > Reports > Monitor > Monitor Action Log

Click the following tabs to define monitor set details.

- **Counter Thresholds** (page 236)
- **Services Check** (page 239)
- **Process Status** (page 240)

Monitor Set Name

Enter a descriptive name for the monitor set that helps you identify it in monitor set lists.

Monitor Set Description

Describe the monitor set in more detail. The rationale for the creation of the set is meaningful here; the reason for the creation of the set is sometimes lost over time.

Group Alarm Column Name

Assign this monitor set to a **Group Alarm Column Name**. If a monitor set alarm is triggered, the **group alarm** (page 555) it belongs to is triggered as well. Group alarms display in the **Group Alarm Status** (page 223) pane of the Monitor > **Dashboard List** page.

Note: The **Enable Matching** (page 239) option applies to counters, services and processes.

Save

Saves changes to a record.

Save As

Saves a record using a new name.

Export Monitor Set...

Click the **Export Monitor Set...** link to display the procedure in XML format in the **Export Monitor Sets** popup window. You can copy it to the clipboard or download it to a text file.

Counter Thresholds

Monitor > Edit > Monitor Sets

- Select a monitor set in a folder, then Counter Thresholds

The **Counter Thresholds** tab defines alert conditions for all performance objects/instances/counters

associated with a monitor set. These are the same performance objects, instances and counters displayed when you run PerfMon.exe on a Windows machine.



Note: The **Enable Matching** (page 239) option applies to counters, services and processes.

Performance Objects, Instances and Counters

When setting up counter thresholds in **monitor sets** (page 558), it's helpful to keep in mind exactly how both Windows and the VSA identify the components you can monitor:

- **Performance Object** - A logical collection of counters that is associated with a resource or service that can be monitored. For example: processors, memory, physical disks, servers each have their own sets of predefined counters.
- **Performance Object Instance** - A term used to distinguish between multiple performance objects of the same type on a computer. For example: multiple processors or multiple physical disks. The VSA lets you skip this field if there is only one instance of an object.
- **Performance Counter** - A data item that is associated with a performance object, and if necessary, the instance. Each selected counter presents a value corresponding to a particular aspect of the performance that is defined for the performance object and instance.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.


Edit icon

Click the edit icon  next to row to edit the row.

Delete Icon

Click the delete icon  to delete this record.

Add / Edit

Click **Add** or the edit icon  to use a wizard that leads you through the six steps required to add or edit a performance counter.

1. Select a **Object**, **Counter** and, if necessary, an **Instance** using their respective drop-down lists.
 - If only one instance of a performance object exists, the **Instance** field can usually be skipped.
 - The drop-down lists used to select performance objects, counters, and instances are based on the "master list" maintained using the **Monitor Lists** (page 231) page. If an object/instance/counter does not display in its respective drop-down list, you can add it manually using **Add Object**, **Add Counter**, and **Add Instance**.
 - Whatever the range of counter instances specified by a monitor set, the **Monitor Log** (page 291) page only displays instances that exist on a specific machine. Newly added counter instances—for example, adding a removable disk to a machine—will start being displayed on the **Monitor Log** page soon after they are discovered, if included in the range specified for monitoring by a monitor set.
 - When multiple instances exist, you can add an instance called **_Total**. The **_Total** instance means you want to monitor the *combined* value of all the other instances of a performance object as a *single counter*.
 - When multiple instances exist, you can add a counter instance called ***ALL** to the list of instances supported using the **Monitor Lists** (page 231) > **Counter Instance** tab. Once added to the counter you want to work with, the ***ALL** value will display in the drop-down list of instances associated with that counter. The ***ALL** instance means you want to monitor all instances for the same performance object *using individual counters*.
2. Optionally change the default counter object **Name** and **Description**.

Monitor

3. Select the log data collected. If the returned value is numeric, you can minimize unwanted log data by setting a collection operator just over or just under the collection threshold.
 - **Collection Operator** - For character string return values, the options are **Changed**, **Equal** or **NotEqual**. For numeric return values, the options are **Equal**, **NotEqual**, **Over**, or **Under**.
 - **Collection Threshold** - Set a fixed value that the returned value is compared to, using the selected **Collection Operator**, to determine what log data is collected.
 - **Sample Interval** - Defines how frequently the data is sent by the agent to the Kaseya Server.
4. Specify when an alert condition is encountered.
 - **Alarm Operator** - For character string return values, the options are **Changed**, **Equal** or **NotEqual**. For numeric return values, the options are **Equal**, **NotEqual**, **Over** or **Under**.
 - **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alert condition is encountered.
 - **Duration** - Specify the time the returned values must continuously exceed the alarm threshold to generate the alert condition. Many alert conditions are only alarming if the level is sustained over a long period of time.
 - **Ignore additional alarms for** - Suppress additional alert conditions for this same issue for this time period. This reduces the confusion of many alert conditions for the same issue.
5. **Warn when within X% of alarm threshold** - Optionally display a warning alert condition when the returned value is within a specified percentage of the **Alarm Threshold**. The warning icon is a yellow traffic light icon 🚦.
6. Optionally activate a **trending alarm**. Trending alarms use historical data to predict when the next alert condition will occur.
 - **Trending Activated?** - If yes, a linear regression trendline is calculated based on the last 2500 data points logged.
 - **Trending Window** - The time period used to extend the calculated trendline into the future. If the predicted trendline exceeds the alarm threshold within the future time period specified, a trending alert condition is generated. Typically a trending window should be set to the amount of time you need to prepare for an alert condition, if it occurs. Example: a user may want 10 days notice before a hard drive reaches the alert condition, to accommodate ordering, shipping and installing a larger hard drive.
 - **Ignore additional trending alarms for** - Suppress additional trending alert conditions for this same issue for this time period.
 - Trending alarms display as an orange icon 🟡.

Warning status alert conditions and trending status alert conditions don't create alarm entries in the alarm log, but they change the image of the alarm icon in various display windows. You can generate a trending alarm report using Reports > Monitor.

Next

Moves to the next wizard page.

Previous

Moves back to the previous wizard page.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Enable Matching

The **Enable Matching** checkbox applies to services, counters and processes as follows:

- **Services** (page 236) - If checked, no alarms are created if a service specified in the monitor set does not exist on an assigned machine. If unchecked, creates a "does not exist" alarm.

Note: Specifying a range of services using the * wildcard character requires **Enable Matching** (page 239) be checked.

- **Counters** (page 236) - If checked, no alarms are created if a counter specified in the monitor set does not exist on an assigned machine. If unchecked, the counter displays on the **Monitor Log** (page 291) page with a **Last Value** of Not Responding. No alarm is created.
- **Processes** (page 240) - Does not apply to processes. Checked or unchecked, no alarms are created if a process specified in the monitor set does not exist on an assigned machine.

Note: This change does not take effect on machines already assigned the monitor set until the monitor set is reassigned.



Services Check

Monitor > Edit > Monitor Sets

- Select a monitor set in a folder, then **Services Check**

The **Services Check** tab defines alarms conditions for a service if the service on a machine ID has stopped, and optionally attempts to restart the stopped service. *The service must be set to automatic to be restarted by a monitor set.*

Select Pages

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.


Edit icon

Click the edit icon  next to row to edit the row.

Delete Icon

Click the delete icon  to delete this record.

Add / Edit

Click **Add** or the edit icon  to maintain a **Services Check** record.

1. **Service** - Selects the service to be monitored from the drop-down list.
 - The drop-down list is based on the "master list" maintained using the **Monitor Lists** (page 231) page. If a service does not display in the drop-down list, you can add it manually using **Add Service**.
 - You can add an asterisk (*) wildcard service to the **Name** or **Description** columns in the list of services supported using the **Monitor Lists** (page 231) > **Service** tab. Once added, the wildcard service will display in the drop-down list of services. For example specifying the service *SQL SERVER* will monitor all services that include the string SQL SERVER in the name of the service.
 - You can add a service called *ALL to the **Name** or **Description** columns in the list of services supported using the **Monitor Lists** (page 231) > **Service** tab. Once added, the *ALL value will

Monitor

display in the drop-down list of services. Selecting the ***ALL** service means you want to monitor all services.

Note: Specifying a range of services using the ***** wildcard character requires **Enable Matching** (page 239) be checked.

2. **Description** - Describes the service and the reason for monitoring.
3. **Restart Attempts** - The number of times the system should attempt to restart the service.
4. **Restart Interval** - The time period to wait between restart attempts. Certain services need more time.
5. **Ignore additional alarms for** - Suppresses additional alert conditions for the specified time period.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Process Status



Monitor > Edit > Monitor Sets

- Select a monitor set in a folder, then **Process Status**

The **Process Status** tab defines alert conditions based on whether a process has started or stopped on a machine ID.

Note: The **Enable Matching** (page 239) option applies to services, counters and processes.

Select Pages

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.


Edit icon

Click the edit icon  next to row to edit the row.

Delete Icon

Click the delete icon  to delete this record.

Add / Edit

Click **Add** or the edit icon  to maintain a **Process Status** record.

1. **Process** - Selects the process to be monitored from the drop-down list. The drop-down list is based on the "master list" maintained using the **Monitor Lists** (page 231) page. If a process does not display in the drop-down list, you can add it manually using **Add Process**.
2. **Description** - Describes the process and the reason for monitoring.
3. **Alarm on Transition** - Triggers an alert condition when a process (application) is started or stopped.
4. **Ignore additional alarms for** - Suppresses additional alert conditions for the specified time period.

Save

Saves changes to a record.

Cancel






Ignores changes and returns to the list of records.

Monitor Icons

Monitor > Edit > Monitor Sets

- Select a monitor set in a folder, then Monitor Icons

The **Monitor Icons** tab selects the monitor icons that display in the **Monitor Log** (page 291) page when various alarm states occur.

- **Select Image for OK Status** - The default icon is a green traffic light .
- **Select the Image for Alarm Status** - The default icon is a red traffic light .
- **Select Image for Warning Status** - The default icon is a yellow traffic light .
- **Select the Image for Trending Status** - The default icon is an orange traffic light .
- **Select the Image for Not Deployed Status** - The default icon is a grey traffic light .

Save

Saves changes to a record.

Upload additional monitoring icons

Select the **Upload additional monitoring icons** link to upload your own icons to the status icon drop-down lists.

Restore

Sets all monitor icons back to their defaults.

SNMP Sets

Monitor > Edit > SNMP Sets

SNMP Sets adds, imports or modifies a SNMP set. A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** (page 562). The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 562) are the easiest method of implementing SNMP monitoring on a device.
- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.
- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.
- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** (page 563) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Discovery > **LAN Watch**
(<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 297). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 305) or **Dashboard List** (page 219).

The following additional SNMP functions are available and can be used in any order.

- Optionally review the list of all imported SNMP objects using Monitor > **Monitor Lists** (page 231).

Monitor

- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 241).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 246).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** (page 308).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 306).

Note: Certain command line functions from the Net-SNMP suite of applications are used to implement SNMP v1 and SNMP v2c retrieval of information from SNMP capable devices in accordance with all pertinent copyright requirements.


Monitoring using Apple OS X

Apple OS X supports SNMP monitoring. See **System Requirements** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm>).

Folder Trees

SNMP sets are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

Always Available

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon  to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

When a Folder is Selected

- **Share Folder** - Shares a folder with user roles and individual users. Applies to shared cabinet folders only.

Note: See guidelines for share rights to objects within folder trees in the **Folder Rights** (page 108) topic.

- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.
- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **New SNMP Set** - Opens the **Define SNMP Set** (page 243) window to create a new monitor set in the selected folder of the folder tree.
- **Import SNMP Set** - Imports a monitor set.

When a Monitor Set is Selected

- **Delete Monitor Set** - Deletes the selected procedure.

Creating SNMP Sets

1. Select a folder in the middle pane.
2. Click the **New SNMP Set** button.
3. Enter a name.
4. Enter a description.
5. Select an **SNMP type** (page 308) from the **Automatic deployment to** drop-down list. If a LAN Watch detects this type of SNMP device the system automatically begins monitoring the SNMP device using this SNMP set.

6. Select a **group alarm** (page 555) category from the **Group Alarm Column Name** drop-down list. User defined group alarm column names are maintained using the **Monitor Lists** (page 231) page. Group alarms display on the **Dashboard List** (page 219) page.
7. Click **Save**. The **Define SNMP Set** (page 243) window displays.

Note: Sample SNMP sets do not display in the **Assign SNMP** (page 297) > **Select SNMP Set** drop-down list. Create a copy of a sample SNMP set by selecting the sample set in **SNMP Sets** (page 241) and clicking the **Save As** button. Your copy of the sample SNMP set will display in the drop-down list. In a SaaS (page 564)-based VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

Define SNMP Set

Monitor > Edit > SNMP Sets > Define SNMP Set

- Select a SNMP set in a folder.

The **Define SNMP Set** page maintains a collection of MIB objects included in a SNMP set.

A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** (page 562). The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 562) are the easiest method of implementing SNMP monitoring on a device.
- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.
- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.
- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** (page 563) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Discovery > **LAN Watch**
(<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 297). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 305) or **Dashboard List** (page 219).

The following additional SNMP functions are available and can be used in any order.

- Optionally review the list of all imported SNMP objects using Monitor > **Monitor Lists** (page 231).
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 241).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 246).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** (page 308).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 306).

Note: Certain command line functions from the Net-SNMP suite of applications are used to implement SNMP v1 and SNMP v2c retrieval of information from SNMP capable devices in accordance with all pertinent copyright requirements.

Monitor

Click the following tabs to define SNMP set details.

- [SNMP Sets](#) (page 244)
- [SNMP Icons](#) (page 247)

SNMP Monitor Set Name

Enter a descriptive name for the SNMP set that helps you identify it in SNMP set lists.

SNMP Monitor Set Description

Describe the SNMP set in more detail. The rationale for the creation of the set is meaningful here; the reason for the creation of the set is sometimes lost over time.

Automatic Deployment to

Selecting a type automatically assigns a newly discovered SNMP device to a [Set SNMP Type](#) (page 308) when performing a [LAN Watch](#) (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) function.

Group Alarm Column Name

Assign this SNMP set to a [Group Alarm Column Name](#). If a SNMP set alarm is triggered, the group alarm it belongs to is triggered as well. Group alarms display in the Group Alarm Status pane of the [Dashboard List](#) (page 219) page.

Save

Saves changes to a record.

Save As

Saves a record using a new name.

Export SNMP Set...

Click the [Export SNMP Set...](#) link to display the procedure in XML format in the [Export Monitor Sets](#) popup window. You can copy it to the clipboard or download it to a text file. SNMP sets can be *imported* using the [SNMP Sets](#) (page 241) page.



SNMP Set Details

[Monitor](#) > [Edit](#) > [SNMP Sets](#) > [Define SNMP Set](#)

- [Select a SNMP set in a folder, then SNMP Sets](#)

The [SNMP Sets](#) tab enables you to maintain all MIB objects associated with a SNMP set.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.


Edit icon

Click the edit icon  next to row to edit the row.


Delete Icon

Click the delete icon  to delete this record.

Add / Edit

Click [Add](#) or the edit icon  to use a wizard that leads you through the six steps required to add or edit the monitoring of a MIB object.

1. Add the object/version/instance combination required to retrieve information from a SNMP device.

- **MIB Object** - Select the **MIB object** (page 562). Click **Add Object** (page 246) to add a MIB object that currently does not exist on the **Monitor Lists** (page 231) page.
 - **SNMP Version** - Select a SNMP version. Version 1 is supported by all devices and is the default. Version 2c defines more attributes and encrypts the packets to and from the SNMP agent. Only select version 2c if you know the device supports version 2c.
 - **SNMP Instance** - The last number of an object ID may be expressed as a table of values instead of as a single value. If the instance is a single value, enter 0. If the instance is a table of values, enter a range of numbers, such as 1-5,6 or 1,3,7.
- Note:** If you're not sure what numbers are valid for a particular SNMP instance, select a machine ID that has performed a LAN Watch using **Monitoring > Assign SNMP** (page 297). Click the **SNMP Info** hyperlink for the device you're interested in. This displays all MIB object IDs and the SNMP instances available for the device.
- **Value Returned as** - If the MIB object returns a numeric value, you can choose to return this value as a **Total** or a **Rate Per Second**.
2. Optionally change the default MIB object **Name** and **Description**.
 3. Select the log data collected. If the returned value is numeric, you can minimize the collection of unwanted log data by setting a collection operator just over or just under the collection threshold.
 - **Collection Operator** - For character string return values, the options are **Changed**, **Equal** or **NotEqual**. For numeric return values, the options are **Equal**, **NotEqual**, **Over** or **Under**.
 - **Collection Threshold** - Set a fixed value that the returned value is compare to, using the selected **Collection Operator**, to determine what log data is collected.
 - **SNMP Timeout** - Specify the number of periods the agent waits for a reply from the SNMP device before giving up. Two seconds is the default.
 4. Specify when a SNMP alert condition is triggered.
 - **Alarm Operator** - For character string return values, the options are **Changed**, **Equal** or **NotEqual**. For numeric return values, the options are **Equal**, **NotEqual**, **Over**, **Under** or **Percent Of**.
 - **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alert condition is triggered.
 - **Percent Object** - Selecting the **Percent Of** option for **Alarm Operator** causes this field to display. Enter another object/version/instance in this field whose value can serve as a 100% benchmark for comparison purposes.
 - **Duration** - Specify the time the returned values must continuously exceed the alarm threshold to generate the alert condition. Many alert conditions are only alarming if the level is sustained over a long period of time.
 - **Ignore additional alarms for** - Suppress additional alert conditions for this same issue for this time period. This reduces the confusion of many alert conditions for the same issue.
 5. **Warn when within X% of alarm threshold** - Optionally display a warning alert condition in the **Dashboard List** (page 219) page when the returned value is within a specified percentage of the **Alarm Threshold**. The default warning icon is a yellow traffic light icon . See **SNMP Icons** (page 247).
 6. Optionally activate a **trending alarm**. Trending alarms use historical data to predict when the next alert condition will occur.
 - **Trending Activated?** - If yes, a linear regression trendline is calculated based on the last 2500 data points logged.
 - **Trending Window** - The time period used to extend the calculated trendline into the future. If the predicted trendline exceeds the alarm threshold within the future time period specified, a trending alert condition is generated. Typically a trending window should be set to the amount of time you need to prepare for an alert condition, if it occurs.

Monitor

- **Ignore additional trending alarms for** - Suppresses additional trending alert conditions for this same issue during this time period.
- By default, trending alarms display as an orange icon 🟡 in the **Dashboard List** (page 219) page. You can change this icon using the **SNMP Icons** (page 247) tab.
- Warning status alarms and trending status alarms don't create alarm entries in the alarm log, but they change the image of the alarm icon in various display windows. You can generate a trending alarm report using Reports > Monitor.

Next

Moves to the next wizard page.

Previous

Moves back to the previous wizard page.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Add SNMP Object

Monitor > Edit > Add SNMP Object

Monitor > Edit > SNMP Sets > Define SNMP Set


- Select a SNMP set in a folder, then SNMP Sets > Add Object

When you select objects to include in an SNMP set you're given the opportunity of adding a new SNMP object. This should not be necessary for the most part, because a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) retrieves the objects you typically require. But if you do need to add an SNMP object from a MIB file manually you can do so using Monitor > **Add SNMP Object** (page 246) or by clicking the **Add Object...** button while configuring an SNMP set.

The **SNMP MIB Tree** page loads a Management Information Base (MIB) file and displays it as an expandable *tree* of MIB objects. All **MIB objects** (page 562) are classified by their location on the MIB tree. Once loaded you can select the MIB objects you want to install on your VSA. SNMP device manufacturers typically provide MIB files on their websites for the devices they manufacture.

Note: You can review the complete list of MIB objects already installed, by selecting the **MIB OIDs** tab in **Monitoring > Monitor Lists** (page 231). This is the list of MIB objects you currently can include in an SNMP set.

If a vendor has supplied you with a MIB file, you can follow these steps:

1. Load the vendor's MIB file by clicking **Load MIB** There may be a message stating there are dependent files that need to be loaded first. The vendor may need to provide those also.
2. Click the  expand icons in the MIB tree—see *the sample graphic below*—and find the desired items to monitor. Select each corresponding check box.
3. Click **Add MIB Objects** to move the selected items from Step 2 into the MIB object list.
4. Configure the settings for monitoring the new SNMP object within an SNMP set as you normally would.
5. The number of MIB objects in the tree can soon become unwieldy. Once the desired MIB objects have been added, the MIB file can be removed.

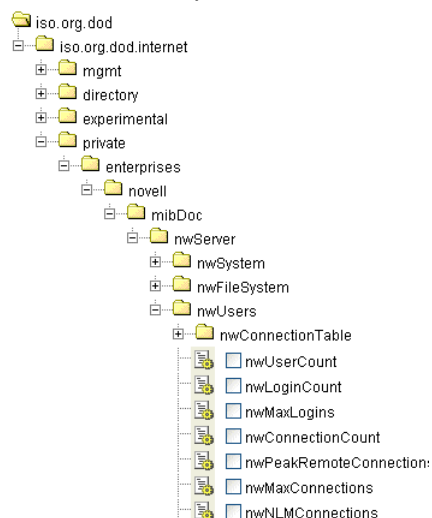
Load MIB

Click **Load MIB...** to browse for and upload a MIB file. When a MIB object is added, if the system does not already have the following standard MIB II files—required by most MIBs—it loads them automatically: `snmp-tc`, `snmp-smi`, `snmp-conf`, `rfc1213`, `rfc1759`. Once these files are loaded, the MIB tree located at the bottom of the **Add SNMP Object** page can be opened and navigated to find the new objects that the user can select. Most private vendor MIBs are installed under the `Private` folder. See *the sample graphic below*.

Note: The MIB file can be loaded and removed at any time and does *not* affect any MIB objects that are used in SNMP sets.

MIB Tree

The MIB tree represents all MIB file objects that are currently loaded for the user to select from.



Add MIB Objects

Click **Add MIB Objects** to add selected objects to the VSA's list of MIB objects that can be monitored using **Define SNMP Set** (page 243).

Remove MIB






After selections have been made the MIB file can be removed. The size of the MIB tree can become so large that it is hard to navigate. Click **Remove MIB** to clean that process up.

SNMP Icons

Monitor > SNMP Sets

- Select a SNMP set in a folder, then **SNMP Icons**

The **SNMP Icons** tab selects the SNMP icons that display in the **Dashboard List** (page 219) page when the following alarm states occur:

- **Select Image for OK Status** - The default icon is a green traffic light .
- **Select the Image for Alarm Status** - The default icon is a red traffic light .
- **Select Image for Warning Status** - The default icon is a yellow traffic light .
- **Select the Image for Trending Status** - The default icon is an orange traffic light .
- **Select the Image for Not Deployed Status** - The default icon is a grey traffic light .

Monitor

Save

Saves changes to a record.

Upload additional monitoring icons

Select the [Upload additional monitoring icons](#) link to upload your own icons to the status icon drop-down lists.

Restore

Sets all SNMP icons back to their defaults.

Alerts

Monitor > Agent Monitoring > Alerts

The **Alerts** page enables you to quickly define alerts for typical **alert conditions** (page 551) found in an IT environment. For example, low disk space is frequently a problem on managed machines. Selecting the **Low Disk** type of alert displays a single additional field that lets you define the % free space threshold. Once defined, you can apply this alert immediately to any machine ID displayed on the **Alerts** page and specify actions to take in response to the alert.

Note: **Monitor Sets** (page 558) represent a more complex method for monitoring alert conditions. Typical alert conditions should be defined using the **Alerts** page.

Select Alert Function

Select an alert type using the **Select Alert Function** drop-down list.

- **Summary** (page 248)
- **Agent Status** (page 250)
- **Application Changes** (page 253)
- **Get Files** (page 255)
- **Hardware Changes** (page 258)
- **Low Disk** (page 260)
- **Agent Procedure Failure** (page 262)
- **Protection Violation** (page 264)
- **New Agent Installed** (page 266)
- **Patch Alert** (page 268)
- **Backup Alert** (page 271)
- **System** (page 275)

Alerts - Summary

Monitor > Agent Monitoring > Alerts (page 248)

- Select **Summary** from the **Select Alert Function** drop-down list

The **Alerts - Summary** (page 248) page shows what alerts are enabled for each machine. You can apply or clear settings or copy enabled alerts settings. Specifically you can:

- Apply or clear settings for alarm, ticket and email notification *for all enabled alert types at one time* on selected machines.
- **Copy** all the enabled alert settings from a selected machine ID or machine ID template and apply them to multiple machine IDs.

Note: You can only modify or clear alerts initially enabled using the Copy option or else by using the other alerts pages.

Although you can not assign agent procedures using this page, agent procedure assignments are displayed in the paging area.

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 219), Monitor > **Alarm Summary** (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Copy








Only active when **Summary** is selected. **Copy** takes all the alert type settings for a single machine ID, selected by clicking **Copy alert settings from <machine_ID> to all selected machine IDs**, and applies these same settings to all other checked machine IDs.

Select All/Unselect All


Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled

Monitor

-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Alert Type

Lists all alert types you can assign to a machine ID using the Monitor > **Alerts** (page 248) page. Displays any agent procedure assignments for this machine ID.

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure
- E = **Email Recipients**

Email Address

A comma separated list of email addresses where notifications are sent. The word **disabled** displays here if no alerts of this alert type are assigned to this machine ID.

Alerts - Agent Status

Monitor > **Agent Monitoring** > **Alerts** (page 248)

- **Select Agent Status** from the **Select Alert Function** drop-down list

The **Alerts - Agent Status** (page 250) page alerts when an agent is offline, first goes online, or someone has disabled remote control on the selected machine.

Agent Online/Offline Alerts

Online and offline alerts are not triggered by powering up and powering down the machine. Rather they only occur when the machine is powered up and the agent process is prevented from checking in. For example, the agent process may have been terminated or the agent may not be able to connect to the network.

Note: When ever the Kaseya Server service stops, the system suspends all agent online/offline alerts. If the Kaseya Server stops for more than 30 seconds, then agent online/offline alerts are suspended for one hour after the Kaseya Server starts up again. Rather than continuously try to connect to the Kaseya Server when the Kaseya Server is down, agents go to sleep for one hour after first trying to connect a couple times. The one hour alert suspension prevents false agent offline alerts when the Kaseya Server starts back up.

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- **1 - Alert when single agent goes off-line**
- **2 - Alert when users disable remote control**
- **3 - Alert when agent first goes online** - The agent online alert only occurs if an agent offline alert has also been set for the same machine.
- **4 - Alert when multiple agents in the same group go off-line** - If more than one offline alert is triggered at the same time, email notification is consolidated by group.

Note: Changing this email alarm format changes the format for all Agent Status alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🟡 in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3	4
<at>	#at#	alert time	🟡	🟡	🟡	🟡
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🟡	🟡	🟡	🟡
<gr>	#gr#	group ID	🟡	🟡	🟡	🟡
<id>	#id#	machine ID	🟡	🟡	🟡	
<mc>	#mc#	number of machines going offline				🟡
<ml>	#ml#	list of multiple machines going offline				🟡
<qt>	#qt#	offline time / online time / time remote disabled	🟡	🟡	🟡	🟡
	#subject#	subject text of the email message, if an email was sent in response to an alert	🟡	🟡	🟡	🟡
	#body#	body text of the email message, if an email was sent in response to an alert	🟡	🟡	🟡	🟡

Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an [alert condition](#) (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

Monitor

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Agent has not checked in for <N> <periods>

If checked, an alert is triggered if the agent has not checked in for the specified number of periods.

Alert when agent goes online

If checked, an alert is triggered if the agent goes online

Alert when user disables remote control









If checked, an alert is triggered if the user disables remote control

Select All/Unselect All


Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure

- E = Email Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Time Offline

Displays the number of periods a machine ID must be off-line before an alert condition occurs.

Rearm Time

The number of periods to ignore additional alert conditions after the first one is reported. This prevents creating multiple alarms for the same problem.

Agent Goes Online

Displays a checkmark ✓ if an alert is sent when an agent goes online.

RC Disabled

Displays a checkmark ✓ if an alert is sent when the user disables remote control.

Alerts - Application Changes

Monitor > Agent Monitoring > Alerts (page 248)

- Select Application Changes from the Select Alert Function drop-down list.
- Similar information is provided using Audit > Add/Remove (page 137) and Reports > Software.

The Alerts Application Changes (page 253) page alerts when a new application is installed or removed on selected machines. You can specify the directories to exclude from triggering an alert. This alert is based on the latest audit (page 551).

Passing Alert Information to Emails and Procedures

The following type of monitoring alert emails can be sent and formatted:

- Alert when application list change

Note: Changing this email alarm format changes the format for all Application Changes alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<il>	#il#	list of newly installed applications
<rl>	#rl#	list of newly removed applications
	#subject#	subject text of the email message, if an email was sent in response to an alert

Monitor

	#body#	body text of the email message, if an email was sent in response to an alert
--	--------	--

Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an [alert condition](#) (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Procedure after alert

If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 353).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for [master role users](#) (page 564).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 392).

Alert when audit detects New application installed

If checked, an alert condition is encountered when a new application is installed.

Alert when audit detects Existing application deleted

If checked, an alert condition is encountered when a new application is removed.

Exclude directories

You can specify the directories to exclude from triggering an alert. The exclude path may contain the wildcard asterisk (*) character. Excluding a folder excludes all subfolders. For example, if you exclude [*\windows*](#), c:\Windows and all subfolders are excluded. You can add to the current list of applications, replace the current application list or remove the existing application list.









Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the


page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

ATSE


The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients


Email Address

A comma separated list of email addresses where notifications are sent.

Installed Apps

Displays a checkmark  if an alert is sent when an application is installed.

Removed Apps

Displays a checkmark  if an alert is sent when an application is removed.

(Exclude)

Lists directories excluded from sending an alert when an application is installed or removed.

Alerts - Get Files

Monitor > Agent Monitoring > Alerts (page 248)

- Select **Get Files** from the **Select Alert Function** drop-down list

The **Alerts - Get File** (page 255) page alerts when a procedure's **getFile()** or **getFileInDirectoryPath()** command executes, uploads the file, and the file is now different from the copy previously stored on the Kaseya Server. If there was no previous copy on the Kaseya Server, the alert is created. Once defined for a machine ID, the same **Get File** alert is *active for any agent procedure* that uses a **Get File** command and is run on that machine ID.

Monitor

Note: The VSA issues the alert only if the **send alert if file changed** option has been selected in the procedure. Turn off alerts for specific files in the agent procedure editor by selecting one of the without alerts options.

Passing Alert Information to Emails and Procedures

The following type of monitoring alert emails can be sent and formatted:

- Alert when file fetched with **Get File** changes from the last fetch
- Alert when file fetched with **Get File** is unchanged from last fetch

Note: Changing this email alarm format changes the format for all Get Files alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<fn>	#fn#	filename
<gr>	#gr#	group ID
<id>	#id#	machine ID
<sn>	#sn#	procedure name that fetched the file
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 219), Monitor > **Alarm Summary** (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Procedure after alert

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified

machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.









- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Select All/Unselect All


Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure
- E = **Email Recipients**

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Hardware Changes

Monitor > Agent Monitoring > Alerts (page 248)

- Select **Hardware Changes** from the **Select Alert Function** drop-down list

The **Alerts - Hardware Changes** (page 258) page alerts when a hardware configuration changes on the selected machines. Detected hardware changes include the addition or removal of RAM, PCI devices, and disk drives. This alert is based on the **latest audit** (page 551).

Passing Alert Information to Emails and Procedures

The following type of monitoring alert emails can be sent and formatted:

- **1 - Alert when disk drive or PCI card is added or removed**
- **2 - Alert when the amount of installed RAM changes**

Note: Changing this email alarm format changes the format for all Hardware Changes alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🟡 in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2
<at>	#at#	alert time	🟡	🟡
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🟡	🟡
<gr>	#gr#	group ID	🟡	🟡
<ha>	#ha#	list of hardware additions	🟡	
<hr>	#hr#	list of hardware removals	🟡	
<id>	#id#	machine ID	🟡	🟡
<rn>	#rn#	new RAM size		🟡
<ro>	#ro#	old RAM size		🟡
	#subject#	subject text of the email message, if an email was sent in response to an alert	🟡	🟡
	#body#	body text of the email message, if an email was sent in response to an alert	🟡	🟡

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in

Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.









- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 353).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for [master role users](#) (page 564).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 392).

Select All/Unselect All


Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Monitor

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Low Disk

Monitor > **Agent Monitoring** > **Alerts** (page 248)

- Select **Low Disk** from the **Select Alert Function** drop-down list

The **Alerts - Low Disk** (page 260) page alerts when available disk space falls below a specified percentage of free disk space. A subsequent low disk alert is not created unless the target machine's low disk space is corrected, or unless the alert is cleared, then re-applied. This alert is based on the **latest audit** (page 551).

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- **Alert when disk drive free space drops below a set percent**

Note: Changing this email alarm format changes the format for all Low Disk alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<df>	#df#	free disk space
<dl>	#dl#	drive letter
<dt>	#dt#	total disk space
<gr>	#gr#	group ID
<id>	#id#	machine ID
<pf>	#pf#	percent free space
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 219), Monitor > **Alarm Summary** (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Send alert when selected machines have less than <N> % free space on any fixed disk partition









An alert is triggered if a machine's free disk space is less than the specified percentage.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.


Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Monitor

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Agent Procedure Failure

Monitor > **Agent Monitoring** > **Alerts** (page 248)

- Select **Agent Procedure Failure** from the **Select Alert Function** drop-down list

The **Alerts - Agent Procedure Failure** (page 262) page alerts when an agent procedure fails to execute on a managed machine. For example, if you specify a file name, directory path or registry key in an agent procedure, then run the agent procedure on a machine ID for which these values are invalid, you can be notified about the agent procedure failure using this alerts page.

Passing Alert Information to Emails and Procedures

The following type of alert emails can be sent and formatted:

- **Format email message generated by Agent Procedure Failure alerts**

Note: Changing this email alarm format changes the format for all Agent Procedure Failure alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
	#em#	procedure error message
<en>	#en#	procedure name that fetched the file
<gr>	#gr#	group ID
<id>	#id#	machine ID
	#subject#	subject text of the email message, if an email was sent in response to an alert

	#body#	body text of the email message, if an email was sent in response to an alert
--	--------	--

Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an [alert condition](#) (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.







- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 353).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for [master role users](#) (page 564).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 392).

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in

Monitor




Agent is online but remote control has been disabled



The agent has been suspended

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure
- E = **Email Recipients**

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Protection Violation

Monitor > **Agent Monitoring** > **Alerts** (page 248)

- Select **Protection Violation** from the **Select Alert Function** drop-down list

The **Alerts - Protection Violation** (page 264) page alerts when a file is changed or access violation detected on a managed machine. Options include **Distributed file changed on agent and was updated**, **File access violation detected**, and **Network access violation detected**.

Prerequisites

- Agent Procedures > **Distribute File** (page 118)
- Audit > **File Access** (page 74)
- Audit > **Network Access** (page 75)

Passing Alert Information to Emails and Procedures

The following type of alert emails can be sent and formatted:

- **Format email message generated by Protection Violations alerts.**

Note: Changing this email alarm format changes the format for all Protection Violation alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID

<id>	#id#	machine ID
<pv>	#pv#	violation description from Agent Log
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 219), Monitor > **Alarm Summary** (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Distributed file changed on agent and was updated

If checked, an alert is triggered when a file distributed using Procedure > **Distributed File** (page 118) is changed on the managed machine. The agent verifies the distributed file at every **full check-in** (page 552).

File access violation detected

If checked, an alert is triggered when an attempt is made to access a file specified as blocked using Audit > **File Access** (page 74).

Monitor

Network access violation detected









If checked, an alert is triggered when an attempt is made to access either an internal or external internet site using an application specified as blocked using Audit > [Network Access](#) (page 75).

Select All/Unselect All


Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 562):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - New Agent Installed

[Monitor](#) > [Agent Monitoring](#) > [Alerts](#) (page 248)

- [Select New Agent Installed](#) from the [Select Alert Function](#) drop-down list

The [Alerts - New Agent Installed](#) (page 266) page alerts when a new agent is installed on a managed machine by selected *machine groups*.

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- [Agent checked in for the first time](#)

Note: Changing this email alarm format changes the format for all New Agent Installed emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<ct>	#ct#	time the agent checked in for the first time
<gr>	#gr#	group ID
<id>	#id#	machine ID
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an [alert condition](#) (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 353).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for [master role users](#) (page 564).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.

Monitor

- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Machine Group

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Patch Alert

Patch Management > Configure > Patch Alert

Monitor > Agent Monitoring > Alerts (page 248)

- Select **Patch Alert** from the **Select Alert Function** drop-down list.

The **Alerts - Patch Alert** (page 268) page alerts for patch management events on managed machines.

- A new patch is available for the selected machine ID.
- A patch installation failed on the selected machine ID.
- The agent credential is invalid or missing for the selected machine ID.
- Windows Auto Update changed.

To Create a Patch Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
 - Create **Alarm**
 - Create **Ticket**
 - Run **Script**
 - **Email Recipients**
2. Set additional email parameters.
3. Set additional patch alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.

The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

The following types of patch alert emails can be sent and formatted:

- **1 - New Patch Available**
- **2 - Patch Install Failed**
- **3 - Patch Approval Policies Updated**
- **4 - Agent Credential Invalid**
- **5 - Windows Auto Update Configuration Changed**

Note: Changing the email alarm format changes the format for all **Patch Alert** emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🟡 in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3	4	5
<at>	#at#	alert time	🟡	🟡	🟡	🟡	🟡
<au>	#au#	auto update change					🟡
<bl>	#bl#	new bulletin list			🟡		
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🟡	🟡	🟡	🟡	🟡
<fi>	#fi#	failed bulletin ID		🟡			
<gr>	#gr#	group ID	🟡	🟡		🟡	🟡
<ic>	#ic#	invalid credential type				🟡	
<id>	#id#	machine ID	🟡	🟡		🟡	🟡
<pl>	#pl#	new patch list	🟡				
	#subject#	subject text of the email message, if an email was sent in response to an alert	🟡	🟡	🟡	🟡	🟡
	#body#	body text of the email message, if an email was sent in response to an alert	🟡	🟡	🟡	🟡	🟡

Create Alarm

If checked and an [alert condition](#) (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 353).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for [master role users](#) (page 564).

Monitor

- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Patch Alert Parameters

The system can trigger an alert for the following alert conditions for a selected machine ID:

- **New patch is available**
- **Patch install fails**
- **Agent credential is invalid or missing**

Note: An agent credential (page 553) is not required to install patches unless the machine's File Source is configured as Pulled from file server using UNC path. If an agent credential is assigned, it will be validated as a local machine credential without regard to the File Source configuration. If this validation fails, the alert will be raised. If the machine's File Source is configured as Pulled from file server using UNC path, a credential is required. If it is missing, the alert will be raised. If it is not missing, it will be validated as a local machine credential and as a network credential. If either of these validations fails, the alert will be raised.









- **Windows Auto Update changed**

Select All/Unselect All


Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Edit icon

Click the edit icon  next to a machine ID to automatically set header parameters to those matching the selected machine ID.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Approval Policy Updated

Displays as the first row of data. This is a system alert and not associated with any machines. An alert is generated when a new patch is added to all patch policies. An **NN--** in the **ATSE** column indicates you cannot set an alert or a ticket for this row. You can specify an email recipient. You can also run an agent procedure on a specified machine. See Approval by Policy.

ATSE

The ATSE response code assigned to machine IDs:

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Procedure
- E = **Email Recipients**

Email Address

A comma separated list of email addresses where notifications are sent.

New Patch

If checked, an alarm is triggered when a new patch is available for this machine ID.

Install Failed

If checked, an alarm is triggered when a patch installation has failed for this machine ID.

Invalid Credential

If checked, an alarm is triggered when the credential is invalid for this machine ID.

Win AU Changed

If checked, an alarm is triggered if the group policy for **Windows Automatic Update** on the managed machine is changed from the setting specified by Patch Management > Windows Auto Update.

Note: A log entry in the machine's Configuration Changes log is made regardless of this alert setting.

Alerts - Backup Alert

Backup > Backup Alert

Monitor > Agent Monitoring > Alerts (page 248)

- Select **Backup Alert** from the **Select Alert Function** drop-down list

The **Alerts - Backup Alert** (page 271) page alerts for backup events on managed machines.

The list of machine IDs you can select depends on the **machine ID / group ID filter** (page 23) and the **scope** (page 369) you are using. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove page.

To Create a Backup Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
 - Create **Alarm**
 - Create **Ticket**

Monitor

- Run **Script**
 - **Email Recipients**
2. Set additional email parameters.
 3. Set additional backup alert specific parameters.
 4. Check the machine IDs to apply the alert to.
 5. Click the **Apply** button.

To Cancel a Patch Alert

1. Select the machine ID checkbox.
 2. Click the **Clear** button.
- The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

The following types of backup alert emails can be sent and formatted:

- **Backup failed**
- **Recurring backup skipped if machine offline**
- **Backup Completed Successfully**
- **Full Backup Completed Successfully**
- **Image Location free space below**
- **Verify backup failed**

Note: Changing the email alarm format changes the format for all Backup Alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<be>	#be#	backup failed error message
<bt>	#bt#	backup type
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<im>	#im#	backup image location
<mf>	#mf#	megabytes free space remaining
<sk>	#sk#	backup skip count
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Create Alarm

If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 219), Monitor > **Alarm Summary** (page 227) and Info Center > Reporting >

Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 353).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for [master role users](#) (page 564).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 392).

Apply

Click [Apply](#) to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

Backup Alert Parameters


The system triggers an alarm whenever the system discovers one of four different backup alert conditions for a selected machine ID:

- [Any Backup Completed](#) - Alerts when any volume or folder backup completes successfully.
- [Full Backup Completed](#) - Alerts when a full volume or folder backup completes successfully.
- [Backup Fails](#) - Alerts when a volume or folder backup stops prior to completion for any reason. Typically, backup fails because the machine is turned off mid-backup or because the network connection to the file server referenced by Image Location is lost.
- [Recurring backup skipped if machine offline <N> times](#) - Alerts when [Skip if machine offline](#) is set in Schedule Volumes and the backup is rescheduled the specified number of times because the machine is offline. Use this alert to notify you that backups are not even starting because the machine is turned off at the scheduled volume backup time.
- [Image location free space below <N> MB](#) - Alerts when the hard disk being used to store the backups is less than a specified number of megabytes.

Three additional parameters can be set:

- [Add](#) - Adds alert parameters to selected machine IDs when [Apply](#) is selected without clearing existing parameters.
- [Replace](#) - Replaces alert parameters on selected machine IDs when [Apply](#) is selected.

Monitor

- **Remove** - Clear alert parameters from selected machine IDs. Click the edit icon  next to a machine ID group *first* to select the alert parameters you want to clear.









Note: You may specify different alert email addresses for each backup alert type. This lets you send backup complete alerts to the user and only send failures to the user.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 16).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Any Complete

If checked, an alarm is triggered when any backup is completed for this machine ID.

Full Complete

If checked, an alarm is triggered when a full backup is completed for this machine ID.

Backup Fails

If checked, an alarm is triggered when any backup fails for this machine ID.

Backup Skipped

If checked, an alarm is triggered when any backup is skipped for this machine ID.

Alerts - System

Monitor > Agent Monitoring > Alerts (page 248)

- Select **System** from the **Select Alert Function** drop-down list

The **Alerts - System** (page 275) page alerts for selected events occurring on the *Kaseya Server*. Selecting the **Alerts - System** page does not display a managed machine list. The events listed only apply to the Kaseya Server. This option only displays for **master role users** (page 564).

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- **1 - Admin account disabled manually by a Master admin**
- **2 - Admin account disabled because logon failed count exceeded threshold**
- **3 - KServer has stopped**
- **4 - Database backup failed**
- **5 - Email reader failed (Ticketing module only)**

Note: Changing this email alarm format changes the format for all System alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🟡 in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3	4	5
<an>	#an#	disabled VSA user name	🟡	🟡			
<at>	#at#	alert time	🟡	🟡	🟡	🟡	🟡
<bf>	#bf#	database backup error data				🟡	
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🟡	🟡	🟡	🟡	🟡
<el>	#el#	email reader error message					🟡
<fc>	#fc#	value that tripped the failed logon attempt counter	🟡	🟡			
<fe>	#fe#	time account re-enables	🟡	🟡			
<kn>	#kn#	Kaseya Server IP/name	🟡	🟡	🟡		
<ms>	#ms#	disabled VSA user type (master or standard)	🟡	🟡			
	#subject#	subject text of the email message, if an email was sent in response to an alert	🟡	🟡			
	#body#	body text of the email message, if an email was sent in response to an alert	🟡	🟡			

Apply

Click **Apply** to apply alert parameters to the system.

Monitor

Clear

Click **Clear** to remove all alert parameters from the system.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Admin account disabled

If checked, an alert is triggered when a VSA user account is disabled, whether manually or automatically.

KServer stopped

If checked, an email notification is triggered when the Kaseya Server stops.

System database backup failed

If checked, an email notification is triggered when the Kaseya Server's database backup fails

Email reader in ticketing failed

If checked, an email notification is triggered if the Ticketing > **Email Reader** (page 414) fails.

System alerts sent to

Displays the email recipients who are sent system alerts.

Event Log Alerts

Monitor > Agent Monitoring > Event Log Alerts

The **Event Log Alerts** page alerts when an event log entry for a selected machine matches a specified criteria. After selecting the **event log type**, you can filter the alert conditions specified by **event set** and by **event category**. You then set the alert action to take in response to the alert condition specified.

Note: You can display event logs directly. On a Windows machine click **Start**, then click **Control Panel**, then click **Administrative Tools**, then click **Event Viewer**. Click **Application**, **Security** or **System** to display the events in each log.

Event Sets

Because the number of events in Windows **events logs** (page 554) is enormous the VSA uses a record type called an **event set** to filter an alert condition. Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** (page 554) entry has to match all the field filters of a condition to be

considered a match. A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to. For details on how to configure event sets, see Monitor > Event Log Alerts > [Edit Event Sets](#) (page 280).

Sample Event Sets

A growing list of sample event sets are provided. The names of sample event sets begin with ZC. You can modify sample event sets, but its better practice to copy a sample event set and customize the copy. Sample event sets are subject to being overwritten every time the sample sets are updated during a maintenance cycle.


Global Event Log Black List

Each agent processes all events, however events listed on a "black list" are *not* uploaded to the VSA server. There are two black lists. One is updated periodically by Kaseya and is named `EvLogBlkList.xml`. The second one, named `EvLogBlkListEx.xml`, can be maintained by the service provider and is not updated by Kaseya. Both are located in the `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles` directory. Alarm detection and processing operates regardless of whether entries are on the collection blacklist.

Flood Detection

If 1000 events—not counting [black list events](#) (page 555)—are uploaded to the Kaseya Server by an agent *within one hour*, further collection of events of that log type are stopped for the remainder of that hour. A new event is inserted into the event log to record that collection was suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your Kaseya Server. Alarm detection and processing operates regardless of whether collection is suspended.

Monitor Wizard Icon for Event Sets

A monitor wizard  icon displays next to event log entries in the VSA and in [Live Connect](#). Hovering the cursor over the monitor wizard icon of a log entry displays a wizard. The wizard enables you to create a new event set criteria based on that log entry. The new event set criteria can be added to any new or existing event set. The new or changed event set is immediately applied to the machine that served as the source of the log entry. Changing an existing event set affects all machines assigned to use that event set. The monitor wizard icon displays in:

- Agent > [Agent Logs](#) (page 31)
- Live Connect > Event Viewer
- Live Connect > Agent Data > Event Log

See Monitor > [Event Log Alerts](#) (page 276) for a description of each field shown in the wizard.

Configuring and Assigning Event Log Alerts

1. Optionally enable event logging for the machines you want to monitor using Agent > [Event Log Settings](#) (page 34). [Event categories](#) highlighted in red (EWISFCV) indicate these event categories are not collected by the VSA. [Event log alerts are still generated even if event logs are not collected by the VSA.](#)
2. Select the [event set](#), the [event log type](#) and other parameters using the Event Log Alerts > [Assign Event Set](#) (page 279) header tab.
3. Optionally click the [Edit](#) button on the [Assign Event Set](#) header tab to [create or change the alert conditions for the event sets](#) (page 280) you assign.
4. Specify the actions to take in response to an alert condition using the Event Log Alerts > [Set Alert Actions](#) (page 279) header tab.
5. Optionally click the [Format Email](#) button on [Set Alert Actions](#) header tab to [change the format of mail alerts for event sets](#) (page 280).
6. Select the machines an event set should be applied to.

Monitor


7. Click the **Apply** button.

Actions

- **Apply** - Applies a selected events set to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.
- **Clear** - Removes selected event set from selected machine IDs.
- **Clear All** - Removes all event set settings from selected machine IDs.

Paging Area

The paging area displays the same columns whichever header tab is selected.

- **Select All/Unselect All** - Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.
- **Check-in status** - These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the **agent quick view window** (page 16).
 - 🟢 Online but waiting for first audit to complete
 - 🟢 Agent online
 - 🟢 Agent online and user currently logged on.
 - 🟡 Agent online and user currently logged on, but user not active for 10 minutes
 - ⚪ Agent is currently offline
 - 🟡 Agent has never checked in
 - 🔒 Agent is online but remote control has been disabled
 - 🔴 The agent has been suspended
- **Machine.Group ID** - The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).
- **Edit Icon** - Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.
- **Log Type** - The type of event log being monitored.
- **ATSE** - The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):
 - A = Create **Alarm**
 - T = Create **Ticket**
 - S = Run Agent Procedure
 - E = **Email Recipients**
- **EWISFCV** - The event category being monitored.
- **Email Address** - A comma separated list of email addresses where notifications are sent.
- **Event Set** - The event set assigned to this machine ID. Multiple events sets can be assigned to the same machine ID.
- **Interval** - The number of times an event occurs within a specified number of periods. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** option is selected. Displays **Missing** if the **Alert when this event doesn't occur within <N> <periods>** option is selected. Displays **1** if the **Alert when this event occurs once** is selected.
- **Duration** - The number of periods an event must occur to trigger an alert condition. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** or **Alert when this event doesn't occur within <N> <periods>** options are selected.
- **Re-Arm** - Displays the number of periods to wait before triggering any new alert conditions for the same combination of event set and event category. Applies only if a re-arm period greater than zero is specified using **Ignore additional alarms for <N> <periods>**.

Assign Event Set tab

Monitor > Agent Monitoring > Event Log Alerts > Assign Event Set tab

Use the **Assign Event Set** header tab to select the event set, the event log type and other parameters for an event set. You can also select machines and assign events sets when this header tab is selected.

Creating an Event Log Alert

1. On the Monitor > **Event Log Alerts** page select the **Assign Event Set** tab.
2. Select an item from the **Select event log type** drop-down list.
3. Select the **Event Set** (*page 280*) filter used to filter the events that trigger alerts. By default **<All Events>** is selected.

Note: You can create a new event set or edit an existing event set by clicking the **Edit** button.

4. Check the box next to any of the following **event category**:
 - Error
 - Warning
 - Information
 - Success Audit
 - Failure Audit
 - Critical - Applies only to Vista, Windows 7 and Windows Server 2008
 - Verbose - Applies only to Vista, Windows 7 and Windows Server 2008

Note: **Red letters indicate logging disabled.** Event log collection may be disabled by the VSA for a particular machine, based on settings defined using **Agent > Event Log Settings** (*page 34*). A particular event category (EWISFCV) may be not be available for certain machines, such as the **Critical** and **Verbose** event categories. Event log alerts are still generated even if event logs are not collected by the VSA.

5. Specify the *frequency* of the alert condition required to trigger an alert:
 - **Alert when this event occurs once.**
 - **Alert when this event occurs <N> times within <N> <periods>.**
 - **Alert when this event doesn't occur within <N> <periods>.**
 - **Ignore additional alarms for <N> <periods>.**
6. Click the **Add** or **Replace** radio options.
 - **Add** adds the selected event set to the list of event sets already assigned to selected machines.
 - **Replace** replaces the entire list of assigned events sets on selected machines with the selected event set.
7. Select the **Set Alert Actions** tab to select the actions to take in response to the alert condition specified.
8. Click **Apply** to assign selected event type alerts to selected machine IDs.

Note: Click **Remove** to remove all event set alerts from selected machine IDs immediately. You don't have to click the **Apply** button.

Set Alert Actions tab

Monitor > Agent Monitoring > Event Log Alerts > Set Alert Action tab

Use the **Set Alert Action** tab to specify the actions to take in response to an event set alert condition. You can also select machines and assign events sets when this header tab is selected.

Monitor

- **Create Alarm** - If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 219), Monitor > **Alarm Summary** (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.
- **Create Ticket** - If checked and an alert condition is encountered, a ticket is created.
- **Run Script** - If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.
- **Email Recipients** - If checked and an alert condition is encountered, an email is sent to the specified email addresses.
 - The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
 - Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
 - If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
 - If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
 - If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
 - Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Edit Event Sets

Monitor > Agent Monitoring > Event Log Alerts (page 276)

- Select <New Event Set> from the Define events to match or ignore drop-down list. The Edit Event Set popup window displays.

Edit Event Sets filters the triggering of alerts based on the monitoring of events in event logs maintained by the Windows OS of a managed machine. You can assign multiple event sets to a machine ID.

Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** (page 554) entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to.

Note: Normally, if two conditions are added to an event set, they are typically interpreted as an OR statement. If either one is a match, the alert is triggered. The exception is when the **Alert when this event doesn't occur within <N> <periods>** option is selected. In this case the two conditions should be interpreted as an AND statement. Both must *not* happen within the time period specified to trigger an alert.

Note: You can display event logs directly. On a Windows machine click **Start**, then click **Control Panel**, then click **Administrative Tools**, then click **Event Viewer**. Click **Application**, **Security** or **System** to display the events in that log. Double-click an event to display its **Properties** window. You can copy and paste text from the **Properties** window of any event into **Edit Event Set** fields.

To Create a New Event Set

1. Select the Monitor > **Events Logs Alerts** page.
2. Select an **Event Log Type** from the second drop-down list.

3. Select `<New Event Set>` from the **Define events to match or ignore** drop-down list. The **Edit Event Set** popup window displays. You can create a new event set by:
 - Entering a new name and clicking the **New** button.
 - Pasting event set data as text.
 - Importing event set data from a file.
4. If you enter a new name and click **New**, the **Edit Event Set** window displays the five properties used to filter events.
5. Click **Add** to add a new event to the event set.
6. Click **Ignore** to specify an event that should *not* trigger an alarm.
7. You can optionally **Rename**, **Delete** or **Export Event Set**.

Ignore Conditions

If an event log entry matches one more more **ignore conditions** in an event set, then no alert is triggered *by any event set*, even if multiple conditions in multiple event sets match an event log entry. Because ignored conditions override *all event sets*, it's a good idea to define just one event set for all ignored conditions, so you only have to look in one place if you suspect an ignored condition is affecting the behavior of all your alerts. You must assign the event set containing an ignored condition to a machine ID for it to override all other event sets applied to that same machine ID.

Ignore conditions only override events sharing the same log type. So if you create an "ignore set" for all ignore conditions, it must be applied multiple times to the same machine ID, *one for each log type*. For example, an ignore set applied only as a System log type will not override event conditions applied as Application and Security log type events.

1. Select the Monitor > **Event Log Alerts** page.
2. Check the **Error** checkbox and select `<All Events>` from the event set list. Click the **Apply** button to assign this setting to all selected machine IDs. This tells the system to generate an alert for every error event type. Note the assigned log type.
3. Create and assign an "ignore event set" to these same machine IDs that specifies all the events you wish to ignore. The log type must match the log type in step 2.

Using the Asterisk (*) Wildcard

Include an asterisk (*) wildcard with the text you enter to match multiple records. For example:

```
*yourFilterWord1*yourFilterWord2*
```

This would match and raise an alarm for an event with the following string:

```
"This is a test. yourFilterWord1 as well as yourFilterWord2 are in the description."
```

Exporting and Importing Edit Events

You can export and import event set records as XML files.

- You can *export* an existing event set record to an XML file using the **Edit Event Set** popup window.
- You can *import* an event set XML file by selecting the `<Import Event Set>` or `<New Event Set>` value from the event set drop-down list.

Example:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<event_sets>
<set_elements setName="Test Monitor Set" eventSetId="82096018">
  <element_data ignore="0" source="*SourceValue*"
    category="*CategoryValue*" eventId="12345"
    username="*UserValue*" description="*DescriptionValue*" />
</set_elements>
</event_sets>
```


Format Email Alerts for Event Sets

Monitor > Agent Monitoring > Event Log Alerts > Set Alert Action > Format Email

This **Format Email Alerts** window specifies the format of emails sent in response to *event set* alert conditions. The following types of alert emails can be formatted using this window:

- **1 - Single event log alert** - Same template applied to all event log types.
- **2 - Multiple event log alerts** - Same template applied to all event log types.
- **3 - Missing event log alert** - Same template applied to all event log types.

Note: Changing this email alarm format changes the format for all Event Logs Alerts alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🟡 in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3
<at>	#at#	alert time	🟡	🟡	🟡
<cg>	#cg#	Event category	🟡		
<cn>	#cn#	computer name	🟡		
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🟡	🟡	🟡
<ed>	#ed#	event description	🟡	🟡	
<ei>	#ei#	event id	🟡		
<es>	#es#	event source	🟡		
<et>	#et#	event time	🟡		
<eu>	#eu#	event user	🟡		
<ev>	#ev#	event set name	🟡	🟡	🟡
<gr>	#gr#	group ID	🟡	🟡	🟡
<id>	#id#	machine ID	🟡	🟡	🟡
<lt>	#lt#	log type (Application, Security, System)	🟡	🟡	🟡
<tp>	#tp#	event type - (Error, Warning, Informational, Success Audit, or Failure Audit)	🟡		
	#subject#	subject text of the email message, if an email was sent in response to an alert	🟡	🟡	🟡
	#body#	body text of the email message, if an email was sent in response to an alert	🟡	🟡	🟡

SNMP Traps Alert

Monitor > Agent Monitoring > SNMP Traps Alert

The **SNMP Traps Alert** page configures alerts for a managed machine, acting as a SNMP trap "listener", when it detects an **SNMP trap** message.

When **SNMP Traps Alert** is assigned to a managed machine, a service is started on the managed machine called Kaseya SNMP Trap Handler. This service listens for SNMP trap messages sent by SNMP-enabled devices on the same LAN. Each time an SNMP trap message is received by the service, an SNMP trap Warning entry is added to the managed machine's Application event log. The **source** of these Application event log entries is always KaseyaSNMPTrapHandler.

Note: Create an event set that includes KaseyaSNMPTrapHandler as the source. Use asterisks * for the other criteria if you don't want to filter the events any more than that.

Note: SNMP uses the default UDP port 162 for SNMP trap messages. Ensure this port is open if a firewall is enabled.

Event Sets

Because the number of events in Windows **events logs** (page 554) is enormous the VSA uses a record type called an **event set** to filter an alert condition. Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** (page 554) entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to. For details on how to configure event sets, see Monitor > Event Log Alerts > **Edit Event Sets** (page 280).

Creating an SNMP Traps Alert

1. Select the Monitor > **SNMP Traps Alert** page.
2. Select the **Event Set** filter used to filter the events that trigger alerts. Do not select an event set to include *all* SNMP Trap events.
3. Check the box next to the **Warning event category**. *No other event categories are used by SNMP Trap Alert.*

Note: Event categories highlighted in red (EWISFCV) indicate these event categories are not collected by the VSA. Event log alerts are still generated even if event logs are not collected by the VSA.

4. Specify the *frequency* of the alert condition required to trigger an alert:
 - **Alert when this event occurs once.**
 - **Alert when this event occurs <N> times within <N> <periods>.**
 - **Alert when this event doesn't occur within <N> <periods>.**
 - **Ignore additional alarms for <N> <periods>.**
5. Click the **Add** or **Replace** radio options, then click **Apply** to assign selected event type alerts to selected machine IDs.
6. Click **Remove** to remove all event based alerts from selected machine IDs.
7. Ignore the **SNMP Community** field. *This option is not yet implemented.*

Monitor

Passing Alert Information to Emails and Procedures

Note: SNMP Traps Alert shares the same Format Email window with Monitor > Event Log Alerts (page 276).

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 219), Monitor > **Alarm Summary** (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.






- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).




Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.


-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline

-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Log Type

The type of event log being monitored.

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

EWISFCV

The event category being monitored.

Email Address

A comma separated list of email addresses where notifications are sent.

Event Set

Displays **All Events** if no *SNMP trap event set* was selected, meaning all SNMP trap events are included.

Interval

The number of times an event occurs within a specified number of periods. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** option is selected. Displays **Missing** if the **Alert when this event doesn't occur within <N> <periods>** option is selected. Displays **1** if the **Alert when this event occurs once** is selected.

Duration

The number of periods and event must occur to trigger an alert. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** or **Alert when this event doesn't occur within <N> <periods>** options are selected.

Re-Arm

Displays the number of periods to wait before triggering any new alerts for the same combination of event set and event category. Applies only if a re-arm period greater than zero is specified using **Ignore additional alarms for <N> <periods>**.

Assign Monitoring

Monitor > Agent Monitoring > Assign Monitoring

The **Assign Monitoring** page creates monitor set alerts for managed machines. An alert is a response to an alert condition. An alert condition exists when a machine's performance succeeds or fails to meet a pre-defined criteria.

Monitor Sets

A monitor set is a set of **counter objects**, **counters**, **counter instances**, **services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter** (page 560), service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.


The general procedure for working with monitor sets is as follows:

1. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** (page 231).
2. Create and maintain monitor sets using Monitor > **Monitor Sets** (page 234).
3. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** (page 286).
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.
6. Review monitor set results using:
 - Monitor > **Monitor Log** (page 291)
 - Monitor > **Live Counter** (page 230)
 - Monitor > Dashboard > **Network Status** (page 223)
 - Monitor > Dashboard > **Group Alarm Status** (page 223)
 - Monitor > Dashboard > **Monitoring Set Status** (page 224)
 - Info Center > Reporting > Reports > Monitor > Monitor Set Report
 - Info Center > Reporting > Reports > Monitor > Monitor Action Log

Note: Changes made to a monitor set affect all machine IDs the monitor set is already assigned to, within a couple minutes of the change.

Individualized Monitor Sets

You can *individualize* monitor set settings for a single machine.

1. Using Monitor > **Assign Monitoring**, select a *standard* monitor set using the <Select Monitor Set> drop-down list.
2. Assign this standard monitor set to a machine ID. The monitor set name displays in the **Monitor Set** column.
3. Click the individualized monitor set icon  in the **Monitor Set** column to display the same options you see when defining a **standard monitor set** (page 234). *An individualized monitor set adds an (IND) prefix to the name of the monitor set.*
4. Optionally change the name or description of the individualized monitor set, then click the **Save** button. Providing a unique name and description helps identify an individualized monitor set in reports and log files.
5. Make changes to the monitoring settings of the individualized monitor set and click the **Commit** button. Changes apply only to the single machine the individualized monitor set is assigned to.

Note: Changes to a standard monitor set have no effect on individualized monitor sets copied from it.

Auto Learn Alarm Thresholds for Monitor Sets


You can enable **Auto Learn** alarm thresholds for any standard monitor set you assign to selected machine IDs. This automatically fine-tunes alarm thresholds based on actual performance data on a per machine basis.

Each assigned machine collects performance data for a specified time period. During that time period no alarms are triggered. At the end of the auto learn session, the alarm threshold for each assigned machine is adjusted automatically based on the actual performance of the machine. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized monitor sets.

To apply **Auto Learn** settings to selected machine IDs:

1. Using Monitor > **Assign Monitoring**, select a *standard* monitor set using the <Select Monitor Set> drop-down list.
2. Click **Auto Learn** to display the **Auto Learn** (page 290) popup window. Use a wizard to define parameters used to calculate alarm threshold values.
3. Assign this standard monitor set, modified by your Auto Learn parameters, to selected machine IDs.

Note: You cannot apply Auto Learn settings to a monitor set that is already assigned to a machine ID. If necessary, clear the existing assignment of the monitor set to the machine ID, then perform steps 1 through 3 above.

Once auto learn is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon  for a specific machine ID and manually adjust the calculated alarm thresholds values. You can also re-run Auto Learn again, using a new session of actual performance data to re-calculate alarm threshold values.

To Create a Monitor Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
 - Create **Alarm**
 - Create **Ticket**
 - Run **Script**
 - **Email Recipients**
2. Set additional email parameters.
3. Select the monitor set to add or replace.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

To Cancel a Monitor Set Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.
The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Monitoring threshold alarm

Monitor

- Monitoring trending threshold alarm
- Monitoring exit alarm state notification

Note: Changing this email alarm format changes the format for *all* monitor set and SNMP set emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<ad>	#ad#	alarm duration
<ao>	#ao#	alarm operator
<at>	#at#	alert time
<av>	#av#	alarm threshold
<cg>	#cg#	event category
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<dv>	#dv#	SNMP device name
<gr>	#gr#	group ID
<id>	#id#	machine ID
<ln>	#ln#	monitoring log object name
<lo>	#lo#	monitoring log object type: counter, process, object
<lv>	#lv#	monitoring log value
<mn>	#mn#	monitor set name
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Create Alarm

If checked and an [alert condition](#) (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script


If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

(Apply Filter)

Enter text in the filter edit box, then click the funnel icon  to apply filtering to the drop-down list displayed in **Select Monitor Set**. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the set name.

Select Monitor Set

Select monitor sets from the **Select Monitor Set** list, then click the **Apply** button to assign the monitor set to selected machine IDs. You may assign more than one monitor set to a machine ID. Add or edit monitor sets using Monitor > **Monitor Sets** (page 234).

Note: Sample monitor sets do not display in the **Assign Monitoring** (page 286) > **Select Monitor Set** drop-down list. Create a copy of a sample monitor set by selecting the sample set in **Monitor Sets** (page 234) and clicking the **Save As** button. Your copy of the sample monitor set will display in the drop-down list. In a SaaS (page 564)-based VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

Add Monitor Set

When a monitor set is assigned to machine IDs, the monitor set is added to the list of monitor sets currently assigned to those machine IDs.

Replace Monitor Set

When a monitor set is assigned to machine IDs, the monitor set replaces all monitor sets already assigned to those machine IDs.

Apply

Applies the selected monitor set to checked machine IDs.

Clear

Clears the assignment of a selected monitor set from selected machine IDs.

Clear All

Clears all monitor sets assigned to selected machine IDs.









Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Monitor

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Monitor Sets

Displays the list of all monitor sets assigned to machine IDs.



Edit - Always displays next to a monitor set. Click this icon to set header parameters to those matching the selected machine ID.



Override auto learn values - Displays if Auto Learn is applied to this standard monitor set. Click this icon to display or change the actual values calculated by **Auto Learn** (page 290) for this monitor set on this machine ID.



Individualized monitor set - Displays if Auto Learn is *not* applied to this standard monitor set. Click this icon to create or make changes to a copy of this **standard monitor set** (page 234) that is individualized for this machine ID. *An individualized monitor set adds an (IND) prefix to the name of the monitor set.*

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **Alarm**
- T = Create **Ticket**
- S = Run Agent Procedure
- E = **Email Recipients**

Email Address

A comma separated list of email addresses where notifications are sent.

Auto Learn - Monitor Sets



Monitor > Agent Monitoring > Assign Monitoring > Auto Learn

The **Auto Learn Alarm Thresholds** window maintains auto learn alarm thresholds for monitor sets.


You can enable **Auto Learn** alarm thresholds for any standard monitor set you assign to selected machine IDs. This automatically fine-tunes alarm thresholds based on actual performance data on a per machine basis.

Each assigned machine collects performance data for a specified time period. During that time period no alarms are triggered. At the end of the auto learn session, the alarm threshold for each assigned machine is adjusted automatically based on the actual performance of the machine. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized monitor sets.


Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Edit

A list of [objects/instance/counters](#) (page 560) displays for the selected monitor set you want to setup to "auto learn". Click the edit icon  to use a wizard that leads you through the three steps required to edit auto learn alarm thresholds.

1. Enable Auto Learn for this object/counter/instance combination, if appropriate, by selecting **Yes - Include**. If **No - Do not include** is selected, no other selections in this wizard are applicable.
 - **Time Span** - Enter the period of time performance data is collected and used to calculate alarm thresholds automatically. Alarms will not be reported during this time period.
2. Displays the **Object**, **Counter** and, if necessary, the counter **Instance** of the alarm threshold being modified. These options cannot be changed.
3. Enter calculated value parameters.
 - **Computation** - Select a calculated value parameter. Options include **MIN**, **MAX** or **AVG**. For example, selecting **MAX** means calculate the maximum value collected by an object/counter/instance during the **Time Span** specified above.
 - **% Increase** - Add this percentage to the **Computation** value calculated above, with the **Computation** value representing 100%. The resulting value represents the alarm threshold.
 - **Minimum** - Set a minimum value for the alarm threshold. The value is automatically calculated as *two standard deviations below* the calculated **Computation** value, but can be manually overridden.
 - **Maximum** - Set a maximum value for the alarm threshold. The value is automatically calculated as *two standard deviations above* the calculated **Computation** value, but can be manually overridden.

Note: Once auto learn is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon  for a specific machine ID and manually adjust the calculated alarm thresholds values. You can also re-run Auto Learn again, using a new session of actual performance data to re-calculate alarm threshold values.

Next

Moves to the next wizard page.

Previous

Moves back to the previous wizard page.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Monitor Log

Monitor > Agent Monitoring > Monitor Log

- Clicking the monitoring log icon  next to a single alarm for a specific machine ID in the [Monitoring Set Status](#) (page 224) dashlet of the [Dashboard List](#) page displays this same information as a popup window.

Monitor

The **Monitor Log** page displays the agent monitoring object logs in chart and table formats.

Machine ID.Group ID

Click a machine ID link to display log data for all monitor sets assigned to that machine ID. The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369). If no machine IDs display use Monitor > **Assign Monitoring** (page 286) to apply monitor sets to machine IDs.

Select monitoring object to display information


The page displays a list of monitoring objects assigned to the selected machine ID.

View


Select a counter object by clicking the **View** link. The selected row is **bolded**. A selected row displays either as a chart or table.

Note: If a monitoring object cannot be represented by a chart, only the table view is available.

Expand Icon

Click the expand icon  to display details about a monitoring object.

Refresh Data

Click the refresh icon  to refresh data when no values display. Applies to non-responsive monitoring.

If your monitor doesn't show any log values, verify the following:

1. Check the sample interval of the counter object. Once a monitor set is deployed counters return values to the monitor log using their specified sample interval. Wait for the sample interval plus the agent check-in interval for the first value to come back.
2. If there are no values returned, check **Counter Thresholds** (page 236) for the Monitor Counter commands. If no values on the monitored machine or device meet the collection threshold they will not be inserted into the monitor log.

If a monitor isn't responding, the log displays the message **Monitor Not Responding**. There can be several reasons for no response from the monitor:

- **Counters** - If your monitoring set includes a counter that does not exist on a managed machine, the log displays **Not Responding**. You can troubleshoot the monitoring of counters for a specific machine in two ways:
 - Use the Monitor > **Update Lists By Scan** (page 232) page to scan for all monitor counters and services *for that specific machine ID*.
 - Connect to the machine managed by this agent, select the **Run** command in the **Start** menu, enter `perfmon.exe`, click **OK**, create a new **Counter Log**, and check for the existence of the counter objects/counters/instances that aren't responding.
 - A counter value of -998 in the monitor logs indicates the monitor set is returning no data. Check that the **Performance Logs & Alerts** service in Windows is running. This is a pre-requisite for monitoring of performance counters.
- **Services** - If your monitoring set includes a service that does not exist on a managed machine, the log displays **Service Does Not Exist**.
- **Processes** - If your monitoring set includes a process that does not exist on a managed machine, the log displays **Process Stopped**.
- **Permissions** - Make sure that the permissions for the agent's **working directory** (page 64) are set to full access for SYSTEM and NETWORK SERVICE. This can happen if the agent working directory is placed in the `c:\program files\` or `c:\windows` directories. This is not recommended as these directories have special permissions set by the OS.

Type

The type of monitor object: counter, process or service.

Monitor Set Name

The name of the monitor set.

Object Name

The name of the monitor object.

Last Value

The last value reported.

Bar Chart / Table

Select the **Bar Chart** or **Table** radio option to display data in either format. Only monitor objects of type **Counters** can be displayed in bar chart format.

- A bar chart displays the last 2000 data points at the sample interval rate. The background of the chart displays in red for alarm threshold, yellow for warning threshold and green for no alarm.
- Table log data displays the most current values first and displays alarm and warning icons on log data that falls within these thresholds. See **Define Monitor Set** (page 243) for more information.

Start Date / Display Last

Display log data for the last number of intervals selected since the specified date. If no date is specified, the current date is used. For example, if you select **Display Last** 500 minutes, each bar in the chart represents 1 minute.

Save View

You can save the **Display Last** value for a specific monitor object.

Log rows per Page

These fields only display in **Table** format. Select the number of rows to display per page.

Display Value Over / Under Value

These fields only display in **Table** format. Filter the table rows displayed by filtering log data that is over or under the value specified.

Refresh

Click the refresh button after making filter changes.

Select Page

This buttons display only if **Table** format is selected. When more rows of data are selected than can be displayed on a single page, click the << and >> buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

System Check

Monitor > External Monitoring > System Check

The VSA can monitor machines that *don't have an agent installed on them*. This function is performed entirely within a single page called **System Check**. Machines without an agent are called **external systems**. A machine with an agent is assigned the task of performing the system check on the external system. A system check typically determines whether an external system is available or not. Types of system checks include: web server, DNS server, port connection, ping, and custom.

Monitor

To Create a System Check Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
 - Create **Alarm**
 - Create **Ticket**
 - Run **Script**
 - **Email Recipients**
2. Set additional email parameters.
3. Set additional system-check parameters. You may check multiple systems using the same machine ID.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

To Cancel a System Check Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.
The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

The following types of system check alert emails can be sent and formatted:

- System check alert

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<p1>	#p1#	address checked
<p2>	#p2#	additional parameter
<sc>	#sc#	system check type
<scn>	#scn#	system check custom name
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an **alert condition** (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 219), Monitor > **Alarm Summary** (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an **agent procedure** (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

System Check Parameters

Select a system check type:

- **Web Server** - Enter a URL to poll at a selected time interval.
- **DNS Server** - Enter a DNS address, either a name or IP, to poll at a selected time interval.
- **Port Connection** - Enter an address, either a name or IP, to connect to, and a port number to connect to, at a selected time interval.
- **Ping** - Enter an address, either a name or IP, to ping at a selected time interval.

Note: Do not include the scheme name of a URL in the address you want to ping. For example, do not enter `http://www.google.com`. Instead enter `www.google.com`.

- **Custom** - Enter a path to a custom program and output file to run at a selected time interval.
 - **Program, parameters and output file** - Enter program path. Optionally include a parameter that creates an output file, if applicable. For example: `c:\temp\customcheck.bat > c:\temp\mytest.out`.
 - **Output file path and name** - Enter the name and path of the created output file. For example: `c:\temp\mytest.out`.
 - **Alarm if output file contains / does not contain** - Alarm if output file contains / does not contain the specified text. For example: `Hello World`.

The following optional parameters display for all types of system checks:

- **Every N Period** - Enter the number of times to run this task each time period.
- **Add** - Add this system check to selected machine IDs.

Monitor









- **Replace** - Add this system check to selected machine IDs and remove all existing system checks.
- **Remove** - Remove this system check from selected machine IDs.
- **Custom Name** - Enter a custom name that displays in alarm messages and formatted emails.
- **Only alarm when service continues to not respond for N periods after first failure detected** - Suppresses the triggering of a system check alarm for a specified number of periods after the initial problem is *detected*, if N is greater than zero. This prevents triggering an alarm for a temporary problem.
- **Ignore additional alarms for N periods** - Suppresses the triggering of additional alarms for the same system check for a specified number of periods after the initial problem is *reported*, if N is greater than zero. This prevents reporting multiple alarms for the same problem.

Select All/Unselect All


Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status


These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (*page 16*) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Delete

Click the delete icon  to delete a system check.

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of **Machine.Group IDs** (*page 556*) displayed is based on the **Machine ID / Group ID filter** (*page 23*) and the machine groups the user is authorized to see using System > User Security > **Scopes** (*page 369*).

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (*page 562*):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Type

The type of system check:

- Web Server
- DNS Server

- Port Connection
- Ping
- Custom

Interval

The interval for the system check to recur.

Duration

The number of periods the system check alarm is suppressed, after the initial problem is *detected*. This prevents triggering an alarm for a temporary problem.

ReArm

The number of periods to ignore additional alert conditions after the first one is reported. This prevents creating multiple alarms for the same problem.

Assign SNMP

Monitor > SNMP Monitoring > Assign SNMP

The **Assign SNMP** page creates SNMP alerts for SNMP devices discovered using a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>). An **alert** (page 549) is a response to an alert condition.

A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** (page 562). The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 562) are the easiest method of implementing SNMP monitoring on a device.
- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.
- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.
- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** (page 563) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.


1. Discover SNMP devices using Discovery > **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 297). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 305) or **Dashboard List** (page 219).

The following additional SNMP functions are available and can be used in any order.

- Optionally review the list of all imported SNMP objects using Monitor > **Monitor Lists** (page 231).
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 241).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 246).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** (page 308).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 306).

Individualized SNMP Sets

You can *individualize* SNMP set settings for a single machine.

1. Select a *standard* SNMP set using the <Select Monitor Set> drop-down list.
2. Assign this standard SNMP set to a SNMP device. The SNMP set name displays in the **SNMP Info / SNMP Set** column.
3. Click the individualized monitor set icon  in the **SNMP Info / SNMP Set** column to display the same options you see when defining a **standard SNMP set** (page 241). *An individualized SNMP set adds an (IND) prefix to the name of the SNMP set.*
4. Make changes to your new individualized SNMP set. These changes apply only to the single SNMP device it is assigned to.

Note: Changes to a standard SNMP set have no affect on individualized SNMP sets copied from it.


Auto Learn Alarm Thresholds for SNMP Sets

You can enable **Auto Learn** alarm thresholds for any standard SNMP set or quick set you assign to selected SNMP devices. This automatically fine-tunes alarm thresholds based on actual performance data on a per SNMP device basis.

Each assigned SNMP device generates performance data for a specified time period. During that time period no alarms are triggered. At the end of the **Auto Learn** session, the alarm threshold for each assigned SNMP device is adjusted automatically based on the actual performance of the SNMP device. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized SNMP sets.

To apply **Auto Learn** settings to selected SNMP devices:

1. Select a *standard* SNMP set using the <Select SNMP Set> drop-down list. Or click the edit icon of an SNMP set already assigned to a device to populate the <Select SNMP Set> drop-down list with its identifier.
2. Click **Auto Learn** to display the **Auto Learn** (page 290) popup window. Use a wizard to define parameters used to calculate alarm threshold values.
3. Assign this standard SNMP set, modified by your **Auto Learn** parameters, to selected SNMP devices, if not already assigned.

Once **Auto Learn** is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon  for a specific SNMP device and manually adjust the calculated alarm threshold values. You can also re-run **Auto Learn** again, using a new session of actual performance data to re-calculate alarm threshold values.

Quick Sets

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) is performed. You can use the list of discover MIB objects to instantly create a device-specific SNMP set—called a **quick set**—and apply it to the device. Once created, quick sets are the same as any standard set. They display in your private folder in Monitor > **SNMP Sets** and in the drop-down list in Monitor > **Assign SNMP**. A (QS) prefix reminds you how the quick set was created. Like any other standard set, quick sets can be *individualized* for a single device, used with Auto Learn, shared with other users, and applied to similar devices throughout the VSA.

1. Discover SNMP devices using Monitor > **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 297).
3. Click the hyperlink underneath the name of the device, called the **SNMP info** (page 302) link, in the **Assign SNMP** page to display a dialog.

- Click **Discovered MIB Objects** and select one or more of the MIB objects that were discovered on the SNMP device you just selected.
 - Click **Quick Set Items** and, if necessary, edit the alarm thresholds for selected MIB objects.
 - Enter a name after the **(QS)** prefix in the header of the dialog.
 - Click the **Apply** button to apply the quickset to the device.
4. Display SNMP monitoring data returned by the quick set using Monitor > **SNMP Log** (page 305), the same as you would for any other standard SNMP set.
 5. Optionally maintain your new quick set using Monitor > **SNMP Sets** (page 562).

To Create a SNMP Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
 - Create **Alarm**
 - Create **Ticket**
 - Run **Script**
 - **Email Recipients**
2. Set additional email parameters.
3. Select the SNMP set to add or replace.
4. Check the SNMP device to apply the alert to.
5. Click the **Apply** button.

To Cancel a SNMP Alert

1. Select the SNMP device checkbox.
2. Click the **Clear** button.
The alert information listed next to the SNMP device is removed.

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Monitoring threshold alarm
- Monitoring trending threshold alarm
- Monitoring exit alarm state notification

Note: Changing this email alarm format changes the format for *all* monitor set and SNMP set emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<ad>	#ad#	alarm duration
<ao>	#ao#	alarm operator
<at>	#at#	alert time
<av>	#av#	alarm threshold
<cg>	#cg#	event category
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use

Monitor

		<db-vMachine.ComputerName>
<dv>	#dv#	SNMP device name
<gr>	#gr#	group ID
<id>	#id#	machine ID
<ln>	#ln#	monitoring log object name
<lo>	#lo#	monitoring log object type: counter, process, object
<lv>	#lv#	monitoring log value
<mn>	#mn#	monitor set name
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Create Alarm

If checked and an [alert condition](#) (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script


If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 353).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for [master role users](#) (page 564).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 392).

(Apply Filter)

Enter text in the filter edit box, then click the funnel icon  to apply filtering to the drop-down list displayed in [Select SNMP Set](#). Filtering is case-insensitive. Match occurs if filter text is found anywhere in the set name.

Select SNMP Set

Select SNMP sets from the **Select SNMP Set** list, then click the **Apply** button to assign the SNMP set to selected machine IDs. You may assign more than one SNMP set to a machine ID. Add or edit SNMP sets using Monitor > **SNMP Sets** (page 241).

Note: Sample SNMP sets do not display in the **Assign SNMP** (page 297) > **Select SNMP Set** drop-down list. Create a copy of a sample SNMP set by selecting the sample set in **SNMP Sets** (page 241) and clicking the **Save As** button. Your copy of the sample SNMP set will display in the drop-down list. In a SaaS (page 564)-based VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

Add Monitor Set

Adds the selected SNMP set to selected SNMP devices.

Replace Monitor Set(s)

Adds the selected SNMP set to selected SNMP devices and removes all other SNMP sets currently assigned to selected SNMP device.

Edit SNMP List

Manually add a new SNMP device or edit the information of existing SNMP devices. Enter the IP and MAC address, name and description for the SNMP device. You can also enter the `sysDescr`, `sysLocation` and `sysContact` values typically returned by polling.

Apply

Applies the selected SNMP set to selected SNMP devices.

Clear

Clears the assignment of a selected SNMP set from selected SNMP devices.

Clear All

Clears all SNMP sets assigned to selected SNMP devices.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Name / Type

The name returned by the ARP protocol when a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) is performed.

Device IP

The IP address of the SNMP device.

MAC Address

The MAC address of the SNMP device.

SNMP Info

Displays the name returned by the SNMP protocol when a LAN Watch is performed. Click the **SNMP Info** (page 302) link to display the SNMP objects for this SNMP device.

SNMP Sets

Displays the list of SNMP sets assigned to a SNMP device.

Monitor



- **Edit** - Always displays next to an SNMP set. Click this icon to set header parameters to those matching the selected SNMP device.



- **Override auto learn values** - Displays if Auto Learn is applied to this standard SNMP set. Click this icon to display or change the actual values calculated by **Auto Learn** (page 290) for this SNMP set on this SNMP device.



- **Individualized monitor set** - Displays if Auto Learn is *not* applied to this standard SNMP set. Click this icon to create or make changes to a copy of this **standard SNMP set** (page 241) that is individualized for this SNMP device. *An individualized SNMP set adds an (IND) prefix to the name of the SNMP set.*

ATSE

The ATSE response code assigned to machine IDs or **SNMP devices** (page 562):

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

SNMP Quick Sets

Monitor > SNMP Monitoring > Assign SNMP > SNMP Info link

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) is performed. You can use the list of discover MIB objects to instantly create a device-specific SNMP set—called a **quick set**—and apply it to the device. Once created, quick sets are the same as any standard set. They display in your private folder in Monitor > **SNMP Sets** and in the drop-down list in Monitor > **Assign SNMP**. A (QS) prefix reminds you how the quick set was created. Like any other standard set, quick sets can be *individualized* for a single device, used with Auto Learn, shared with other users, and applied to similar devices throughout the VSA.

1. Discover SNMP devices using Monitor > **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 297).
3. Click the hyperlink underneath the name of the device, called the **SNMP info** (page 302) link, in the **Assign SNMP** page to display a dialog.
 - Click **Discovered MIB Objects** and select one or more of the MIB objects that were discovered on the SNMP device you just selected.
 - Click **Quick Set Items** and, if necessary, edit the alarm thresholds for selected MIB objects.
 - Enter a name after the **(QS)** prefix in the header of the dialog.
 - Click the **Apply** button to apply the quickset to the device.
4. Display SNMP monitoring data returned by the quick set using Monitor > **SNMP Log** (page 305), the same as you would for any other standard SNMP set.
5. Optionally maintain your new quick set using Monitor > **SNMP Sets** (page 562).


Use the following tabs on the **SNMP Info link** page to configure an SNMP quick set.

Discovered MIB Objects tab

The **Discovered MIB Objects** tab lists all objects sets discovered by the last SNMP "walk" that apply to the selected SNMP device. You can use this tab to add objects and instances to an SNMP quick set for this device.

- **Add Instance** - Click to add this instance of this object to an SNMP "quick set" displays in the **SNMP Set** tab of this same window.
- **Add All Instances** - Click to add all instances of this object to an SNMP "quick set" displays in the **SNMP Set** tab of this same window.
- **SNMP Object** - The name of the SNMP object. If no name is provided for the object, the OID numerical designation displays.
- **Instance** - The instance of the object. Many objects have multiple instances, each of which have a different value. For example, the different instances could be ports on a router, or paper trays on a printer. The field is blank if the last number of an OID is zero, which indicates there can only be one member of this object. If an instance is not blank, or any number other than 0, than more than one "instance" of this same object exists for the device. You can specify monitoring of multiple instances of an object by entering a range of numbers, such as 1-5,6 or 1,3,7. You can also enter All.
- **Current SNMP Value** - The value returned by the object/instance combination by the latest SNMP "walk".

Quick Set Items tab



The **Quick Set Items** tab configures the objects and instances selected to be included in your SNMP quick set. Click the edit icon  to define SNMP monitoring attributes for the selected objects. You can also use the **Add** button to add a new object and set these same attributes.

- **SNMP Object** - The SNMP object name or OID number.
- **SNMP Instance** - The last number of an object ID may be expressed as a table of values instead of as a single value. If the instance is a single value, enter 0. If the instance is a table of values, enter a range of numbers, such as 1-5,6 or 1,3,7. You can also enter All.
- **Alarm Operator** - For character string return values, the options are Changed, Equal or NotEqual. For numeric return values, the options are Equal, NotEqual, Over, or Under.
- **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alarm is triggered.
- **Value Returned as** - If the MIB object returns a numeric value, you can choose to return this value as a **Total** or a **Rate Per Second**.
- **Current SNMP Value** - The value returned by the object/instance combination by the latest SNMP "walk".
- SNMP Sets tab

SNMP Icons tab

- Customize the alarm icons for this *specific SNMP quick set*. See **SNMP Icons** (page 247) for a general explanation of how to use this page.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Commit

Save changes made to this page.

Cancel

Ignore any changes made to this page and return to the SNMP Sets list.

Clear

Clears all SNMP objects from all tabs. The default list of objects repopulates the **Discover Objects Set** tab a few minutes later.

Auto Learn - SNMP Sets

Monitor > SNMP Monitoring > Assign SNMP > Auto Learn


The **Auto Learn Alarm Thresholds** window maintains auto learn alarm thresholds for SNMP sets.

You can enable **Auto Learn** alarm thresholds for any standard SNMP set or quick set you assign to selected SNMP devices. This automatically fine-tunes alarm thresholds based on actual performance data on a per SNMP device basis.



Each assigned SNMP device generates performance data for a specified time period. During that time period no alarms are triggered. At the end of the **Auto Learn** session, the alarm threshold for each assigned SNMP device is adjusted automatically based on the actual performance of the SNMP device. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized SNMP sets.

To apply **Auto Learn** settings to selected SNMP devices:


1. Select a *standard* SNMP set using the <Select SNMP Set> drop-down list. Or click the edit icon of an SNMP set already assigned to a device to populate the <Select SNMP Set> drop-down list with its identifier.
2. Click **Auto Learn** to display the **Auto Learn** (page 290) popup window. Use a wizard to define parameters used to calculate alarm threshold values.
3. Assign this standard SNMP set, modified by your **Auto Learn** parameters, to selected SNMP devices, if not already assigned.

Once **Auto Learn** is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon  for a specific SNMP device and manually adjust the calculated alarm threshold values. You can also re-run **Auto Learn** again, using a new session of actual performance data to re-calculate alarm threshold values.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Edit

Click the edit icon  to use a wizard that leads you through the three steps required to edit auto learn alarm thresholds.

1. Enable Auto Learn for this SNMP object, if appropriate, by selecting **Yes - Include**. If **No - Do not include** is selected, no other selections in this wizard are applicable.
 - **Time Span** - Enter the period of time performance data is collected and used to calculate alarm thresholds automatically. Alarms will not be reported during this time period.
2. Displays the **SNMP Object** of the alarm threshold being modified. This option cannot be changed.
 - **Interface**
3. Enter calculated value parameters.
 - **Computation** - Select a calculated value parameter. Options include **MIN**, **MAX** or **AVG**. For example, selecting **MAX** means calculate the maximum value collected by an SNMP object during the **Time Span** specified above.
 - **% Increase** - Add this percentage to the **Computation** value calculated above, with the **Computation** value representing 100%. The resulting value represents the alarm threshold.
 - **Minimum** - Set a minimum value for the alarm threshold. The value is automatically calculated as *two standard deviations below* the calculated **Computation** value, but can be manually overridden.
 - **Maximum** - Set a maximum value for the alarm threshold. The value is automatically calculated as *two standard deviations above* the calculated **Computation** value, but can be manually overridden.

Next

Move the user to the next wizard page.

Previous

Move the user back to the previous wizard page.

Cancel

Ignore any changes made to wizard pages and return to the [Counter Objects](#) list.



Save

Save changes made to the wizard pages.

SNMP Log

[Monitor](#) > [SNMP Monitoring](#) > [SNMP Log](#)

The [SNMP Log](#) page displays SNMP log data of [MIB objects](#) (page 562) in a [SNMP Set](#) (page 241) in chart or table formats.

1. Click a machine ID link to list all SNMP devices associated with a machine ID.
2. Click the IP address or name of an SNMP device to display all SNMP sets and MIB objects assigned to the SNMP device.
3. Click the expand icon  to display the collection and threshold settings for a MIB object.
4. Click the down arrow icon  to display MIB object log data in chart or table formats.
5. Click the [Bar Chart](#) or [Table](#) radio options to select the display format for log data.

SNMP monitor objects can contain multiple instances and be viewed together within one chart or table. For example, a network switch may have 12 ports. Each is an instance and can contain log data. All 12 instances can be combined in one chart or table. SNMP bar charts are in 3D format to allow for multiple instance viewing.

Machine ID.Group ID / SNMP Devices

All machines assigned to SNMP monitoring and currently matching the [Machine ID / Group ID filter](#) (page 23) are displayed. Clicking the machine ID link displays all SNMP devices associated with the machine ID. Click the SNMP device link to display all MIB objects associated with the SNMP device.

View

Click the [View](#) link to display log data for a MIB object in a chart or table.

Remove

Click [Remove](#) to remove log data from a chart or table.

View All

If the SNMP monitor object has multiple instances, clicking the [View All](#) link displays all data for every instance.

Remove All

If the SNMP monitor object has multiple instances, clicking the [Remove All](#) link removes all data displayed for each instance.

Monitor Set Name

The name of the SNMP set the MIB object belongs to.

Monitor

Get Object Name

The name of the MIB object used to monitor the SNMP device.

Description

The description of MIB object in the SNMP set.

Bar Chart / Table

Select the **Bar Chart** or **Table** radio button to display data in either format.

- A bar chart displays the last 2000 data points at the sample interval rate. The background of the chart **displays in red** for alarm threshold, **yellow for warning threshold** and **green for no alarm**.
- Table log data displays the most current values first and displays alarm and warning icons on log data that falls within these thresholds. See **Define SNMP Set** (page 243) for more information.

Display Last

Bar charts display log data for the last number of intervals selected. For example, if you select **Display Last** 500 minutes, each bar in the chart represents 1 minute.

Save View

You can save custom views for each MIB object. The next time this MIB object is selected the saved information is loaded.

Log rows per Page

These fields only display in **Table** format. Select the number of rows to display per page.

Display Value Over / Under Value

These fields only display in **Table** format. Filter the table rows displayed by filtering log data that is over or under the value specified.

Refresh

Click the refresh button to display the most current log data.

If your monitor doesn't show any log values, verify the following.

1. If there are no values returned, check the collection threshold for MIB objects in SNMP sets. If no values on the monitored device meet the collection threshold they are not included in the SNMP log.
2. The log value sample interval is determined by the total number of **SNMPGet** commands retrieving information from SNMP devices to the agent of the machine ID. The more **SNMPGet** commands the larger the sample interval. Check all SNMP devices associated with a machine ID. If some **SNMPGet** commands are returning values but others are not, the **SNMPGet** commands for the failed requests are not compatible.

If a monitor isn't responding, the log displays the message **Monitor Not Responding**. The **SNMPGet** command is incompatible with the device.

Set SNMP Values

Monitor > SNMP Monitoring > Set SNMP Values

The **Set SNMP Values** page enables you to write values to SNMP network devices. The SNMP objects must be **Read Write** capable and requires entering the Write Community password assigned to the SNMP device.

An SNMP community is a grouping of devices and management stations running SNMP. SNMP information is broadcast to all members of the same community on a network. SNMP default









communities are:

- Write = private
- Read = public

Note: This page only displays machines that have been previously identified using a LAN Watch (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** ([page 16](#)) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine ID.Group ID

Lists **Machine ID.Group IDs** ([page 556](#)) currently matching the **Machine ID / Group ID filter** ([page 23](#)) and assigned a **SNMP Community** ([page 562](#)) name. Click a machine ID to display SNMP devices associated with that machine ID.

SNMP Device

Select the specific SNMP device of interest. This displays a history of SNMPSet values written to an SNMP device by the agent of the machine ID.

Create a SNMPSet command

Click **Create a SNMPSet command** to write a new value to this SNMP device. The following fields display:

- **Description** - Enter an easy to remember description of this event. This displays in the history of SNMPSet values for this SNMP device.
- **MIBObject** - Select the MIB object. Click **Add Object** ([page 246](#)) to add a MIB object that currently does not exist on the **Monitor Lists** ([page 231](#)) page.
- **SNMP Version** - Select a SNMP version. Version 1 is supported by all devices and is the default. Version 2c defines more attributes and encrypts the packets to and from the SNMP agent. Only select version 2c if you know the device supports version 2c.
- **writeCommunity** - The write Community password for the SNMP device. The default write community password is private.
- **timeOutValue** - Enter the number of seconds to wait for the SNMP device to respond before the write command times out.
- **setValue** - Enter the value to set the selected MIB object on the SNMP device.
- **attempts** - Enter the number of times to try and write to the MIB object, if it fails to accept the write command.

Execute SNMPSet

Prepares a procedure that executes a SNMPSet command for the selected SNMP device.

Cancel

Ignores any data entered and re-displays the **Create a SNMP command** link and history.

Set SNMP Type

Monitor > SNMP Monitoring > Set SNMP Type

The **Set SNMP Type** page assigns types to SNMP devices *manually*. SNMP devices assigned to one of these types are monitored by SNMP sets of the same type. You can also give individual SNMP devices custom names and descriptions as well as remove the device from your database.

Most SNMP devices are classified as a certain type of SNMP device using the MIB object `system.sysServices.0`. For example, some routers identify themselves as routers generically by returning the value 77 for the `system.sysServices.0` MIB object. You can use the value returned by the `system.sysServices.0` MIB object to auto assign SNMP sets to devices, as soon as they are discovered by a LAN Watch.

Note: The entire OID for `system.sysServices.0` is `.1.3.6.1.2.1.1.7.0` or `.iso.org.dod.internet.mgmt.mib-2.system.sysServices.`

You can assign **SNMP sets** (page 562) to **devices** (page 562) *by type automatically* as follows:

1. Add or edit SNMP *types* using the **SNMP Device** tab in Monitor > **Monitor Lists** (page 231).
2. Add or edit the value returned by the MIB object `system.sysServices.0` *and associated with each SNMP type* using the **SNMP Services** tab in Monitor > **Monitor Lists**.
3. Associate a SNMP *type* with a SNMP *set* using the **Automatic Deployment to** drop-down list in Monitor > SNMP Sets > **Define SNMP Set** (page 243).
4. Perform a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>). During the LAN Watch SNMP devices are automatically assigned to be monitored by SNMP sets if the SNMP device returns a value for the `system.sysServices.0` MIB object that matches the SNMP type associated with those SNMP sets.

You can also assign **SNMP sets** (page 562) to **devices** (page 562) *manually* as follows:

1. Assign a SNMP type to an SNMP device using Monitor > **Set SNMP Type** (page 308). Doing so causes SNMP sets using that same type to start monitoring the SNMP device.

Assign

Applies the selected SNMP type to selected SNMP devices.

Delete

Removes selected SNMP devices from your database. If the device still exists the next time a LAN Watch is performed, the device will be re-added to the database. This is useful if a device's IP or MAC address changes.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Name

List of SNMP devices generated for the specific machine ID by a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).

Type

The SNMP type assigned to the SNMP device.

Custom Name

The custom name and custom description assigned to the SNMP device. If a device is given a custom name, the custom name displays instead of the SNMP name and IP address in alarms and in the

SNMP log. To change the custom name and description click the edit icon  next to the custom name.

Device IP

The IP address of the SNMP device.

MAC Address

The MAC address of the SNMP device.

SNMP Name

The name of the SNMP device.

Parser Summary

Monitor > Log Monitoring > Parser Summary

The **Parser Summary** page displays and optionally define alerts for all parser sets assigned to all machine IDs within the user's scope. **Parser Summary** can also copy parser sets assignments to multiple machine IDs.

Note: Copying a parser set to a machine ID on this page *activates* the log parser on the machine IDs it is copied to. Parsing occurs whenever the log file being parsed is updated.

Note: You can download a [Configuring Log Parsers Step-by-Step](http://help.kaseya.com/webhelp/EN/VSA/7000000/EN_logparsers70.pdf#zoom=70&navpanes=0) (http://help.kaseya.com/webhelp/EN/VSA/7000000/EN_logparsers70.pdf#zoom=70&navpanes=0) PDF from the first topic of online user assistance.

Log Monitoring Setup

1. **Log Parser** - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.
2. **Assign Parser Sets** - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. *Activate* parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.
3. **Parser Summary** - Quickly copy *active* parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

Notification

The agent collects log entries and creates an entry in the 'log monitoring' log based on the criteria defined by the parser set, *whether or not any of the notification methods are checked*. You don't have to be notified each time a new log monitoring entry is created. You can simply **review the 'Log Monitoring' log** (page 322) periodically at your convenience.

To Copy Parser Set Assignments

1. Select a source machine to copy parser set assignments from.
2. Select machine IDs to copy parser set assignments to.
3. Click **Copy**.

To Create a Parser Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
 - Create **Alarm**

Monitor

- Create **Ticket**
 - Run **Script**
 - **Email Recipients**
2. Set additional email parameters.
 3. Check the machine IDs to apply the alert to.
 4. Click the **Apply** button.

To Cancel a Parser Set Alert

1. Select the machine ID checkbox.
 2. Click the **Clear** button.
- The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- Log Monitoring parser alerts.
- Multiple log monitoring parser alerts.
- Missing log monitoring parser alert.

Note: Changing this email alarm format changes the format for both Assign Parser Sets and Parser Summary emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🟡 in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3
<ad>	#ad#	duration		🟡	
<at>	#at#	alert time	🟡	🟡	🟡
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🟡	🟡	🟡
<ec>	#ec#	event count		🟡	
<ed>	#ed#	event description	🟡	🟡	
<gr>	#gr#	group ID	🟡	🟡	🟡
<id>	#id#	machine ID	🟡	🟡	🟡
<lpm>	#lpm#	Log file set criteria	🟡	🟡	🟡
<lpn>	#lpn#	Log parser set name	🟡	🟡	🟡
<lsn>	#lsn#	Log file set name	🟡	🟡	🟡
	#subject#	subject text of the email message, if an email was sent in response to an alert	🟡	🟡	🟡
	#body#	body text of the email message, if an email was sent in response to an alert	🟡	🟡	🟡

Create Alarm

If checked and an alert condition (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List (page 219), Monitor > Alarm Summary (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 353).
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for **master role users** (page 564).
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > **Outbound Email** (page 392).

Copy

Click **Copy** to copy the parser sets of the machine ID selected using the **this machine ID** link to other machine IDs selected in the paging area.

Apply

Applies alert checkbox settings to selected machine IDs.

Clear All









Clears all alert checkbox settings from selected machine IDs.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Monitor

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Delete

Click the delete icon  next to a parser set to delete its assignment to a machine ID.

Log Set Names

Lists the names of parser sets assigned to this machine ID.

ATSE

The ATSE response code assigned to machine IDs:

- A = Create **A**larm
- T = Create **T**icket
- S = Run Procedure
- E = **E**mail Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Interval

The interval to wait for the alert event to occur or not occur.

Duration

Applies only if **Alert when this event occurs <N> times within <N> <periods>** is selected. Refers to **<N> <periods>**.

Re-Arm

Applies only if **Ignore additional alarms for <N> <periods>** is selected.

Log Parser

Monitor > Log Monitoring > Log Parser

The **Log Parser** page defines log parsers and assigns them to selected machine IDs.

Note: You can download a [Configuring Log Parsers Step-by-Step](http://help.kaseya.com/webhelp/EN/VSA/7000000/EN_logparsers70.pdf#zoom=70&navpanes=0)

(http://help.kaseya.com/webhelp/EN/VSA/7000000/EN_logparsers70.pdf#zoom=70&navpanes=0) PDF from the first topic of online user assistance.

Note: The log parsers are only *active* if they are subsequently assigned a log parser set using **Assign Parser Sets** (page 317).

Log Monitoring

The VSA is capable of monitoring data collected from many **standard log files** (page 556). **Log Monitoring** extends that capability by extracting data from the output of any text-based log file. Examples include application log files and **syslog** (page 564) files created for Unix, Linux, and Apple operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the Kaseya Server database, **Log Monitoring** uses **parser definitions and parser sets** (page 559) to parse each log file and select only the data you're interested in. Parsed messages are displayed in Log Monitoring, which can be accessed using the Agent Logs tab of **Live Connect** (page 344) > Agent Data or the **Machine**

[Summary](#) (page 131) page or by generating a report using the Agent > Logs - [Log Monitoring](#) (page 192) page. Users can optionally trigger alerts when a [Log Monitoring](#) record is generated, as defined using [Assign Parser Sets](#) (page 317) or [Parser Summary](#) (page 309).

Log Monitoring Setup

1. [Log Parser](#) - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.
2. [Assign Parser Sets](#) - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. *Activate* parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.
3. [Parser Summary](#) - Quickly copy *active* parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

The Log File Parsing Cycle

The parsing of a log file is triggered whenever the log file is changed. In most cases this involves appending new text to the end of the file. To avoid scanning the entire log file from the beginning each time the file is updated, the agent parses log files as follows:

- After each update the agent stores a "bookmark" of the last 512 bytes of a log file.
- When the log file is updated again, the agent compares the bookmark from the old update with the *same byte position* in the new update.
- Since log files may be archived before the log parser is run, parsing can include archive files if they exist.
- You can specify sets of log files and sets of archive files by specifying full pathnames with asterisk (*) and question mark (?) wildcards. If a set of files is specified the parser begins with the latest file in the set.
- If the bookmark text is the same in both the old update and the new update, the agent begins parsing text *after the bookmark*.
- If the bookmark text is *not* the same and no Log Archive Path is specified, the agent parses the entire log file from the beginning. If a Log Archive Path is specified, the agent searches for the bookmark in the archive files. If the bookmark cannot be found, the agent bookmarks the end of the log file and starts parsing from there in the next cycle.
- Once parsing is completed a new bookmark is defined based on the last 512 bytes of the newly updated log file and the process repeats itself.

Note: The parsing of a log file is not a procedure event itself. Only a new configuration, or reconfiguration, using [Log Parser](#), [Assign Parser Sets](#) or [Parser Summary](#) generates a procedure you can see in the Procedure History or Pending Procedure tabs of the [Machine Summary](#) page.

Apply

Click [Apply](#) to assign a selected log parser to selected machine IDs.

Clear

Click [Clear](#) to remove a selected log parser from selected machine IDs.

Clear All

Click [Clear All](#) to remove all log parsers from selected machine IDs.

New...

Select [<Select Log Parser>](#) in the [Log File Parser](#) drop-down list and click [New...](#) (page 314) to create a new log parser.

Monitor

Edit...

Select an existing log parser in the **Log File Parser** drop-down list and click **Edit...** (*page 314*) to edit the log parser.

Add Log Parser / Replace Log Parsers

Select **Add Log Parser** to add a log parser to existing machine IDs. Select **Replace Log Parsers** to add a log parser and remove all other log parsers from selected machine IDs.

Log File Parser Definition

Monitor > **Log Monitoring** > **Log Parser** > **Log File Parser Definition**

The **Log File Parser Definition** page defines templates and parameters used to parse log files. Definitions are subsequently assigned to machine IDs using the **Log Parser** (*page 312*) page. Log parsers are initially private, but can be shared with other users.

The Log File Parsing Cycle

The parsing of a log file is triggered whenever the log file is changed. In most cases this involves appending new text to the end of the file. To avoid scanning the entire log file from the beginning each time the file is updated, the agent parses log files as follows:

- After each update the agent stores a "bookmark" of the last 512 bytes of a log file.
- When the log file is updated again, the agent compares the bookmark from the old update with the *same byte position* in the new update.
- Since log files may be archived before the log parser is run, parsing can include archive files if they exist.
- You can specify sets of log files and sets of archive files by specifying full pathnames with asterisk (*) and question mark (?) wildcards. If a set of files is specified the parser begins with the latest file in the set.
- If the bookmark text is the same in both the old update and the new update, the agent begins parsing text *after the bookmark*.
- If the bookmark text is *not* the same and no Log Archive Path is specified, the agent parses the entire log file from the beginning. If a Log Archive Path is specified, the agent searches for the bookmark in the archive files. If the bookmark cannot be found, the agent bookmarks the end of the log file and starts parsing from there in the next cycle.
- Once parsing is completed a new bookmark is defined based on the last 512 bytes of the newly updated log file and the process repeats itself.

Note: The parsing of a log file is not a procedure event itself. Only a new configuration, or reconfiguration, using **Log Parser**, **Assign Parser Sets** or **Parser Summary** generates a procedure you can see in the **Procedure History** or **Pending Procedure** tabs of the **Machine Summary** page.

Save

Select **Save** to save changes to a log file parser definition.

Save As...

Select **Save As...** to save a log file parser definition under a different name.

Delete

Select **Delete** to delete a log file parser definition.

Share...

You can share log file parser definitions you own with other **VSA users** (*page 360*), **user roles** (*page 365*), or make the procedure public to all users.

Parser Name

Enter the name of the parser.

Log File Path

Enter the full UNC pathname or mapped drive pathname on the target machine of the log file you want to parse. You can use asterisk (*) or question mark (?) wildcards to specify a set of log files. If a log file set is specified, the log parser starts with the latest log file first. Example:

`\\morpheus\logs\message.log` or `c:\logs\message.log`. When specifying a UNC path to a share accessed by an agent machine—for example `\\machinename\share`—ensure the share's permissions allow read/write access using the credential specified for that agent machine in Agent > **Set Credential** (page 68).

Log Archive Path

Enter the full UNC pathname or mapped drive pathname on the target machine of the archive files you want to parse. You can use asterisk (*) or question mark (?) wildcards to specify a set of archive files. If an archive set is specified, the log parser starts with the latest log file first. Example: If `message.log` is archived daily to a file in `messageYYYYMMDD.log` format, then you can specify

`c:\logs\message*.log`. When specifying a UNC path to a share accessed by an agent machine—for example `\\machinename\share`—ensure the share's permissions allow read/write access using the credential specified for that agent machine in Agent > **Set Credential** (page 68).

Description

Enter a description for the log parser.

Template

The template is used to compare with the log entry in the log file to extract out the required data into parameters. Parameters are enclosed with \$ character in template.

Enter a pattern of text and log file parameters. This pattern is used to search from the beginning of each line in a log file. If a pattern finds a match in the log file, the log file parameters in the pattern are populated with the values extracted from the log file.

You can use a percent (%) wildcard to specify an alphanumeric string of any length. A log file parameter is bracketed with the dollar (\$) symbol. Enter \$\$ to match a pattern of text containing a \$ symbol. Enter %% to match a pattern of text containing a % symbol.

Note: Template text patterns are case sensitive.

Example

- Log text: `126 Oct 19 2007 12:30:30 127.0.0.1 Device0[123]: return error code -1!`
- Template: `$EventCode$ $Time$ $HostComputer$ Dev[PID]:%error code $ErrorCode$!`
- Parsed result:
 - EventCode=126
 - Time= 2007/10/19 12:30:30 Friday
 - HostComputer=127.0.0.1
 - Dev=Device0
 - PID=123
 - ErrorCode=-1

Guidelines

- To enter a tab character in the template edit box:
 1. Copy and paste a tab character from log data.
 2. Use {tab} if it is enter manually.

Monitor

- To create a template it is easier to copy the original text into the template, then replace the characters that can be ignored with %. Then replace the characters that are saved to a parameter with a parameter name.
- Make sure all parameters in the template are defined in [Log File Parameters](#).
- A date time parameter must have both date and time information from the source data, otherwise just use a string parameter.

Skipping Characters

To skip characters, use `${n}$`, where `n` is the number of characters to skip. Use `$var[n]$` to retrieve a fixed number of characters to be a variable value.

Example

- Log text: 0123456789ABCDEFGHIJ
- Template: `${10}$ABC$str[3]$`
- Result for parameter `str` is DEF.

Multilayer Template

If checked, multiple lines of text and log file parameters are used to parse the log file.

Note: The character string `{tab}` can be used as a tab character and `{n1}` can be used as a new line break. `{n1}` cannot be used in single line template. `%` can be used as wildcard character.

Output Template

Enter a pattern of text and log file parameters to store in [Log Monitoring](#).

Example:

- Output template: Received device error from `Dev` on `$HostComputer$`. Code = `$ErrorCode$`.
- Result output: Received device error from Device0 on 127.0.0.1. Code = -1.

Apply

Click [Apply](#) to add or update a parameter entered in the [Name](#) field.

Clear All

Click [Clear All](#) to remove all parameters from the parameter list.

Log File Parameters

Name

Once the template is created, you need to define the list of parameters used by the template. All the parameters in the template have to be defined, otherwise the parser returns an error. Available parameters are *integer*, *unsigned integer*, *long*, *unsigned long*, *float*, *double*, *datetime*, *string*. The length of parameter name is limited to 32 characters.

Enter the name of a parameter used to store a value. Parameters are subsequently used in the [Template](#) and [Output Template](#) text boxes.

Note: Do *not* bracket the name of the parameter with `$` symbols in the [Name](#) field. This is only required when the parameter is entered in the [Template](#) and [Output Template](#) text boxes.

Type

Enter the data type appropriate for the parameter. If data parsed from a log file cannot be stored using

that data type, the parameter remains empty.

Date Format

If the **Type** selected is **Date Time**, enter a **Date Format**.

- **yy, yyyy, YY, YYYY** - two or four digit year
- **M** - single or two digit month
- **MM** - two digit month
- **MMM** - abbreviation of month name, ex. "Jan"
- **MMMM** - full month name, ex. "January"
- **D, d** - single or two digit day
- **DD, dd** - two digit day
- **DDD, ddd** - abbreviation name of day of week, Ex. "Mon"
- **DDDD, dddd** - full name of day of week, ex. "Monday"
- **H, h** - single or two digit hour
- **HH, hh** - two digit hour
- **m** - single or two digit minute
- **mm** - two digit minute
- **s** - single or two digit second
- **ss** - two digit second
- **f** - one or more digit of fraction of second
- **ff** - ffffffff - two to nine digit
- **t** - one character time mark, ex. "a"
- **tt** - two-character time mark, ex. "am"

Note: *Date and time filtering in views and reports are based on the log entry time. If you include a \$Time\$ parameter using the **Date Time** data type in your template, **Log Monitoring** uses the time stored in the \$Time\$ parameter as the log entry time. If a \$Time\$ parameter is *not* included in your template, then the time the entry was added to **Log Monitoring** serves as the log entry time. Each date time parameter must contain at least the month, day, hour, and second data.*

Example:

- Date time string: `Oct 19 2007 12:30:30`
- DateTime template: `MMM DD YYYY hh:mm:ss`

UTC Date

Log Monitoring stores all date/time values as **universal time, coordinated** (UTC). This enables UTC date and times to be automatically converted to the user's local time when **Log Monitoring** data is displayed or when reports are generated.

If blank, the date and time values stored in the log file parameter are converted from the local time of the machine ID assigned the log parser to UTC. If checked, the date and time values stored in the log file parameter are UTC and no conversion is necessary.

Assign Parser Sets

[Monitor](#) > [Log Monitoring](#) > [Assign Parser Sets](#)

The **Assign Parser Sets** page creates and edits parser sets and assigns parser sets to machine IDs. Optionally triggers an alert based on a parser set assignment. A machine ID only displays in the paging area if:

Monitor

- That machine ID has been previously assigned a **log file parser definition** (page 314) using Monitor > **Log Parser** (page 312).
- That same log file parser definition is selected in the **Select Log File Parser** drop-down list.

Note: Assigning a parser set to a machine ID on this page *activates* the log parser. Parsing occurs whenever the log file being parsed is updated.

Note: You can download a [Configuring Log Parsers Step-by-Step](#)

(http://help.kaseya.com/webhelp/EN/VSA/7000000/EN_logparsers70.pdf#zoom=70&navpanes=0) PDF from the first topic of online user assistance.

Notification

The agent collects log entries and creates an entry in the 'log monitoring' log based on the criteria defined by the parser set, *whether or not any of the notification methods are checked*. You don't have to be notified each time a new log monitoring entry is created. You can simply **review the 'Log Monitoring' log** (page 322) periodically at your convenience.

Parser Definitions and Parser Sets

When configuring **Log Monitoring** (page 555) it's helpful to distinguish between two kinds of configuration records: **parser definitions** and **parser sets**.

A **parser definition** is used to:

- Locate the log file being parsed.
- Select log data based on the log data's *format*, as specified by a template.
- Populate parameters with log data values.
- Optionally format the log entry in **Log Monitoring**.

A **parser set** subsequently *filters* the selected data. Based on the *values* of populated parameters and the criteria you define, a parser set can generate log monitoring entries and optionally trigger alerts.

Without the filtering performed by the parser set, the Kaseya Server database would quickly expand. For example a log file parameter called \$FileServerCapacity\$ might be repeatedly updated with the latest percentage of free space on a file server. Until the free space is less than 20% you may not need to make a record of it in **Log Monitoring**, nor trigger an alert based on this threshold. Each parser set applies only to the parser definition it was created to filter. Multiple parser sets can be created for each parser definition. Each parser set can trigger a separate alert on each machine ID it is assigned to.

Log Monitoring Setup

1. **Log Parser** - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.
2. **Assign Parser Sets** - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. *Activate* parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.
3. **Parser Summary** - Quickly copy *active* parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

To Create a Parser Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
 - Create **Alarm**
 - Create **Ticket**
 - Run **Script**
 - **Email Recipients**

2. Set additional email parameters.
3. Select the parser set to add or replace.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

To Cancel a Parser Set Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.


The alert information listed next to the machine ID is removed.
































Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:

- **1 - Log Monitoring parser alerts.**
- **2 - Multiple log monitoring parser alerts.**
- **3 - Missing log monitoring parser alert.**

Note: Changing this email alarm format changes the format for both **Assign Parser Sets** and **Parser Summary** emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A  in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3
<ad>	#ad#	duration			
<at>	#at#	alert time			
<db-view.column>	not available	Include a view.column (page 423) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>			
<ec>	#ec#	event count			
<ed>	#ed#	event description			
<gr>	#gr#	group ID			
<id>	#id#	machine ID			
<lpm>	#lpm#	Log file set criteria			
<lpn>	#lpn#	Log parser set name			
<lsn>	#lsn#	Log file set name			
	#subject#	subject text of the email message, if an email was sent in response to an alert			
	#body#	body text of the email message, if an email was sent in response to an alert			

Monitor

Create Alarm

If checked and an [alert condition](#) (page 551) is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 219), Monitor > [Alarm Summary](#) (page 227) and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an [agent procedure](#) (page 80) to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged on user displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 353).
- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for [master role users](#) (page 564).
- If the [Add to current list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the [Replace list](#) radio option is selected, when [Apply](#) is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If [Remove](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the [From Address](#) using System > [Outbound Email](#) (page 392).

Select Log File Parser

Select a log parser from the [Select log file parser](#) drop-down list to display all machine IDs previously assigned this log parser using the [Log Parser](#) (page 312) page.

Define log sets to match

After a log parser is selected, click [Edit](#) (page 322) to define a new parser set or select an existing parser set from the [Define log sets to match](#) (page 322) drop-down list.

Alert when...

Specify the *frequency* of the parser set condition required to trigger an alert:

- [Alert when this event occurs once](#)
- [Alert when this event occurs <N> times within <N> <periods>](#)
- [Alert when this event doesn't occur within <N> <periods>](#)
- [Ignore additional alarms for <N> <periods>](#)

Add / Replace

Click the [Add](#) or [Replace](#) radio options, then click [Apply](#) to assign a selected parser set to selected machine IDs.

Remove

Click [Remove](#) to remove all parser sets from selected machine IDs.

Apply

Applies the selected parser set to checked machine IDs.

Clear

Clears the assignment of a selected parser set from selected machine IDs.

Clear All









Clears all parser sets assigned to selected machine IDs.

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (*page 16*) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (*page 556*) displayed is based on the [Machine ID / Group ID filter](#) (*page 23*) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (*page 369*).

Delete

Click the delete icon  next to a parser set to delete its assignment to a machine ID.

Log Set Names

Lists the names of parser sets assigned to this machine ID.

ATSE

The ATSE response code assigned to machine IDs:

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run Procedure
- E = [Email Recipients](#)

Email Address

A comma separated list of email addresses where notifications are sent.

Interval

The interval to wait for the alert event to occur or not occur.

Duration

Applies only if [Alert when this event occurs <N> times within <N> <periods>](#) is selected. Refers to [<N> <periods>](#).

Monitor

Re-Arm

Applies only if **Ignore additional alarms for <N> <periods> is selected**.

Log File Set Definition

Monitor > Log Monitoring > Assign Parser Sets

- Select a log parser from the [Select log file parser](#) drop-down list.
- Then select [<New Parser Set>](#) or an existing parser set from the [Define log set to match](#) drop-down list. The [Log File Set Definition](#) popup window displays.

The [Log File Set Definition](#) page defines parser sets. A parser set is a list of conditions that must be matched to create a [Log Monitoring](#) record. Each condition combines a parameter, operator and value.

Parser Definitions and Parser Sets

When configuring [Log Monitoring](#) ([page 555](#)) it's helpful to distinguish between two kinds of configuration records: [parser definitions](#) and [parser sets](#).

A [parser definition](#) is used to:

- Locate the log file being parsed.
- Select log data based on the log data's *format*, as specified by a template.
- Populate parameters with log data values.
- Optionally format the log entry in [Log Monitoring](#).


A [parser set](#) subsequently *filters* the selected data. Based on the *values* of populated parameters and the criteria you define, a parser set can generate log monitoring entries and optionally trigger alerts.

Without the filtering performed by the parser set, the Kaseya Server database would quickly expand. For example a log file parameter called `$FileServerCapacity$` might be repeatedly updated with the latest percentage of free space on a file server. Until the free space is less than 20% you may not need to make a record of it in [Log Monitoring](#), nor trigger an alert based on this threshold. Each parser set applies only to the parser definition it was created to filter. Multiple parser sets can be created for each parser definition. Each parser set can trigger a separate alert on each machine ID it is assigned to.

To Create a New Parser Set

1. Enter a name for the parser set.
2. Optionally rename the parser set by entering a new name and click [Rename](#) to confirm the change.
3. Select a log file parameter from the [Parser Column](#) drop-down list. Log file parameters are defined using the [Log File Parser Definition](#) ([page 314](#)) this parser set is intended to filter.
4. Select an [Operator](#) from the drop-down list. Different data types provide different lists of possible operators.
5. Enter the value the log file parameter should have in the [Log File Filter](#) field to generate a [Log Monitoring](#) record.

Note: Template text patterns are *case sensitive*.

6. Click [Add](#) to add this parameter/operator/value combination to the list of conditions defined for this parser set.
7. Click [Edit](#) to edit and then [Save](#) an existing parameter/operator/value combination.
8. Click the delete icon  to delete an existing parameter/operator/value combination.

Viewing Log Monitoring Entries

Log Monitoring entries are displayed in [Log Monitoring](#), which can be accessed using:

- Agents > [Agent Logs](#) ([page 31](#)) > Log Monitoring > (parser definition)

- **Live Connect** (*page 344*) > Agent Data > Agent Logs > Log Monitoring > (parser definition). Live Connect is displayed by clicking the check-in status icon of a selected machine ID.
- Audit > **Machine Summary** (*page 131*) > Agent Logs tab > Log Monitoring > (parser definition). The Machine Summary page can also be displayed by *alt-clicking* the check-in status icon of a selected machine ID.
- The Info Center > Reporting > Reports > Monitor - Logs > Log Monitoring report.

Chapter 8

Remote Control

In This Chapter

Remote Control Overview	326
Control Machine	326
Reset Password	330
Preinstall RC.....	331
Uninstall RC.....	332
User Role Policy	333
Machine Policy	334
FTP	336
SSH	338
Task Manager.....	338
Chat	339
Send Message.....	341
Kaseya Remote Control	342
Live Connect.....	344

Remote Control Overview

View and operate managed machines as if they were right in front of you simply by clicking its machine ID. The **Remote Control** module enables you to:

- Automatically connect the user to the remote computer independent of any gateway or firewall configurations, even behind NAT.
- Work independently or with the user to solve problems interactively where both parties can see what is happening in real time.
- Set policies that allow users to block remote control or require users to ask permission before accessing a machine.
- FTP to any managed machine and access files even behind NAT gateways and firewalls.
- Direct chat with any managed machine. Perfect for supporting dial up users with only a single phone line. Remote control and chat at the same time.
- Power up, power down, bootstrap or reboot vPro-enabled machines.

Functions	Description
Control Machine (page 326)	Allows users to view and/or take control of a managed machine's desktop remotely for troubleshooting and/or instructional purposes.
Reset Password (page 330)	Reset the password for a local account on a managed machine.
Preinstall RC (page 331)	Install the remote control service
Uninstall RC (page 332)	Uninstall the remote control service
User Role Policy (page 333)	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by VSA user role.
Machine Policy (page 334)	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by machine ID.
FTP (page 336)	Initiate an FTP session with any remote managed machine.
SSH (page 338)	Runs an SSH command line session on a selected, active Linux or Apple machine.
Task Manager (page 338)	Remotely executes the NT task manager and displays data in the browser.
Chat (page 339)	Start a chat session between a user and any remote machine.
Send Message (page 341)	Allows users to send network messages to selected managed machines.

Control Machine

[Remote Control](#) > [Desktop Control](#) > [Control Machine](#)




The **Control Machine** page establishes a remote control session between the user's local machine and a selected machine ID. Remote control sessions can only be initiated from a Windows-based machine.









Automatic Installation


If K-VNC is not already installed on a machine and a remote control session is initiated using **Control Machine** (page 326), then the package is automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute. To eliminate this delay during first time use, you can pre-install K-VNC on any managed machine using **Preinstall RC** (page 331).

Note: Uninstalling an agent does not remove K-VNC or the KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > **Uninstall RC** (page 332) to uninstall K-VNC on the managed machine. Uninstall all add-on module clients as well.

Initiating Remote Control

Initiate remote control by clicking the name of the target machine. Icons next to the managed machine ID indicate the current connection status for that machine. Only machine IDs with an  or  or  icon can be connected to target machines and have live links; all others will be inactive.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Note: Users can disable remote control and FTP sessions by right-clicking the  icon on their managed machine and selecting **Disable Remote Control**. You can deny users this ability by removing **Disable Remote Control** using Agent > **Agent Menu** (page 59).

Enable verbose relay

Remote control or FTP of machines behind firewalls and NAT gateways may be relayed through the VSA server using a helper application. Checking this box displays a popup window with status information about the normally hidden helper application.

Remote Controlling the KServer

Clicking the **KServer** link starts a remote control session to the Kaseya Server itself. Use this feature to remotely manage your own Kaseya Server. Only master role users can remote control the Kaseya Server.

Remote Control for Machine Users

Machine users can have remote access to their agent machines using Agent > **Portal Access** (page 67).

Remote Control Malfunctions

Some reasons for remote control failure—for target machines with and without an agent—are:

- The remote machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The remote machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- Anti-virus software on the remote machine may block the connection. This problem is eliminated if Endpoint Security protection is installed on the remote machine.
- Wrong primary Kaseya Server address - Remote control can only connect through the primary Kaseya Server address. Machines with an agent can connect through either the primary or

Remote Control









secondary address. Verify the remote machine can see the primary Kaseya Server address using Agent > [Check-in Control](#) (page 61).

Record remote control to a file in the machine working directory




Applies to K-VNC only. If checked, creates a [video recording](#) (page 561) of a remote control session.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369). Only machine IDs with an  or  or  icon can be connected to target machines and have live links; all others will be inactive.

Current User

The user currently logged on to the managed machine.

Active Admin

The VSA user currently conducting a remote control session to this machine ID.

K-VNC Toolbar Options

A [K-VNC](#) remote control session can be started using the Remote Control > [Control Machine](#) (page 326) page. Administrators should use K-VNC for situations not supported by [Kaseya Remote Control](#) (page 342), and when a web-based remote control solution is required. Only K-VNC remote control sessions support [Session recording](#) or [Notify user when session terminates](#) settings, located on the [User Role Policy](#) (page 333) and [Machine Policy](#) (page 334) pages of the [Remote Control](#) module.

A K-VNC session provides a set of toolbar buttons to manage the remote desktop viewer. Hover the mouse over each button to display a tooltip.



- [Set Options](#) - Sets connection options for the current viewer session. See details below.
- [Show Connection Info](#) - Displays connection info about the current desktop viewer session.
- [Refresh Screen](#) - Refreshes the display of the desktop viewer.
- [Zoom Out](#)
- [Zoom In](#)
- [Zoom 100%](#)
- [Zoom to Fit Window](#)
- [Full Screen](#)
- [Send 'Ctrl-Alt-Del'](#) - Selects CTRL+ALT+DEL on the remote machine.
- [Send 'Win' key as 'Ctrl-Esc'](#) - Selects CTRL+ESC on the remote machine.

- **Ctrl-Lock** - If on, holds down the CTRL key on the remote machine.
- **Alt-Lock** - If on, holds down the ALT key on the remote machine.
- **Disconnect** - Disconnects the current viewer session.

Set Options

Format and Encodings

Changes to these settings apply only to the current viewer session.

- **Preferred Encoding**
 - **Tight (default)** - Usually the best choice for low-bandwidth network connections.
 - **HexTile** - Usually the best choice for high-speed network connections.
 - **ZRLE** - Included in applet for compatibility with different VNC servers, but not required in Live Connect.
 - **Raw** - Fastest when the server and viewer are on the same machine.
- **Color format** - Reduce colors for better performance over slower network connections.
- **Custom compression level** - Level 1-9. Default is 6.
 - Level 1 uses minimum CPU time and achieves weak compression ratios.
 - Lower levels are recommended for high bandwidth network environments.
 - Level 9 offers best compression but is slow in terms of CPU time consumption on the remote machine.
 - Higher levels recommended for low bandwidth network environments.
- **Allow JPEG, set quality level** - Level 1-9. Defaults is 6.
 - Refers to JPEG compression level.
 - Level 1 gives bad image quality but high compression ratios, while level 9 offers very good image quality at lower compression ratios.
 - Lower levels recommended for low bandwidth network environments.
 - Higher levels recommended for high bandwidth network environments.
 - Disabling recommended only if perfect image quality is needed.
- **Allow CopyRect encoding** - Enabled by default. Saves bandwidth and drawing time when parts of the remote screen are moving around.

Restrictions

- **View Only** - Disables transfer of mouse and keyboard events from the viewer to remote machine.
- **Disable clipboard transfer** - Disables copy/paste between viewer and remote machine.

Mouse Cursor

- **Track Remote cursor locally** - Remote cursor location is shown in viewer.
- **Let remote server deal with mouse cursor** OR **Don't show remote cursor** - Remote cursor location is not shown in viewer. Conserves bandwidth.

Local cursor shape

- Selects the shape of the local cursor when the mouse is over the viewer window.

(Other)

- **Request shared session** - Always checked.

Reset Password

Remote Control > Desktop Control > Reset Password

The **Reset Password** page creates a new password and, if necessary, a new user account on a managed machine. It can also change domain user accounts on domain name controllers.

If the username does not already exist, checking the **Create new account** checkbox creates a new account with the specified password. **Reset Password** returns an error if you attempt to reset the password for a username that is not already created on the managed machine or if you create a password that is already being used by a user account. Blank passwords are not permitted.

Note: To delete a user account, you can create a procedure to delete the user account or use remote control to manually delete the user account.

Resetting the User Password

Use **Reset Password** to reset the user password on all your managed machines when:

- Your user password is compromised.
- Someone leaves your organization who knew the user password.
- It is time to change the user password as part of a good security policy.

Note: On non-domain controllers, only the local user account on the remote machine is changed. On domain controllers, **Reset Password** changes the domain user accounts.

Apply

Click **Apply** to apply password and user account parameters to selected machine IDs.

Cancel

Click **Cancel** to clear pending password changes and user account creations on selected machine IDs.

Username

Enter the username on the managed machine.

Create new account

Check this box to create a new user account on the managed machine.

as Administrator

Check this box to create the new user account with administrator privileges.

Password / Confirm

Enter a new password.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (*page 16*) window.








Online but waiting for first audit to complete



Agent online



Agent online and user currently logged on.

-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Status

The status of pending password changes and user account creations.

Preinstall RC

Remote Control > Configure > Preinstall RC

The **Preinstall RC** page installs **K-VNC** (page 328) on selected machine IDs without initiating a remote control session. When an install is pending on any machine ID this page automatically refreshes every 5 seconds until the procedure completes.

Automatic Installation

If K-VNC is not already installed on a machine and a remote control session is initiated using **Control Machine** (page 326), then the package is automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute. To eliminate this delay during first time use, you can pre-install K-VNC on any managed machine using **Preinstall RC** (page 331).

Note: Uninstalling an agent does not remove K-VNC or the KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > **Uninstall RC** (page 332) to uninstall K-VNC on the managed machine. Uninstall all add-on module clients as well.

Install

Click **Install** to install K-VNC on selected machine IDs. Linux and Apple OS X agents only use K-VNC.

Cancel








Click **Cancel** to clear pending install procedures for selected machine IDs.

Select All/Unselect All


Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled

Remote Control

 The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Last Status

Pending indicates the install will run the next time that machine checks into the Kaseya Server. Otherwise, this column displays when the remote control package was installed on the machine ID.

Uninstall RC

Remote Control > Configure > Uninstall RC

The **Uninstall RC** page uninstalls **K-VNC** (page 328) from selected machine IDs. When an uninstall is pending on any machine ID this page automatically refreshes every 5 seconds until the procedure completes.

If an existing K-VNC installation has problems then the VSA may not be able to establish a K-VNC session. If remote control using K-VNC fails then running **Uninstall RC** on that machine ID cleans out any existing problem installs. A fresh copy of K-VNC is installed the next time a remote control session is started or using **Preinstall RC** (page 331).

Note: Uninstalling an agent does not remove K-VNC or the KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > Uninstall RC (page 332) to uninstall K-VNC on the managed machine. Uninstall all add-on module clients as well.

Uninstall

Click **Uninstall** to uninstall the remote control package from selected machine IDs.

Cancel









Click **Cancel** to clear pending uninstall procedures for selected machine IDs.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent **Quick View** (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Last Status

Pending indicates the uninstall will run the next time that machine checks into the VSA. Otherwise, this column displays when the remote control package was uninstalled on the machine ID.

User Role Policy

Remote Control > Notification Policy > User Role Policy

The **User Role Policy** page determines how you want to notify users that a remote control session to their machine is about to begin. Policies are applied by **user roles** (page 365).

Note: See **Machine Policy** (page 334) to apply remote control notification policies by machine ID. Machine policy takes precedence over user role policy.

Exceptions

K-VNC (page 328) supports all options on this page. **Kaseya Remote Control** (page 342) supports all options on this page except:

- Notify user when session terminates
- Record remote control to a file in the machine working directory

Apply

Click **Apply** to apply policy parameters to selected machine IDs.

Select User Notification Type

- **Silently take control** - Do not tell the user anything. Take control immediately and silently.
- **If user logged in display alert** - Display notification alert text. The alert text can be edited in the text box below this option.
- **If user logged in ask permission** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed and the VSA removes the dialog box from the target machine. If no user is logged in, proceed with the remote control session.
- **Require Permission. Denied if no one logged in** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed and the VSA removes the dialog box from the target machine. The remote control session is canceled.

Notify user when session terminates

Supported by K-VNC only. Check this box to notify the user when the session terminates.

Session Termination Message

Displays only if the **Notify user when session terminates** box is checked. Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

Notification Alert Text / Ask Permission Text

Displays only if the **Select User Notification Type** is *not Silently take control*. Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

Remove

Click **Remove** to clear policy parameters from selected machine IDs.

Require admin note to start remote control

Click this box to require VSA users to enter a note before starting the remote control session. The note is included in the remote control log and is not displayed to the machine user.

Remote Control


Record remote control to a file in the machine working directory

Supported by K-VNC only. If checked, remote control sessions are automatically **recorded** (page 561) for machines assigned this policy.


Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Delete

Click the delete icon  next to a user role to clear the policy.

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Role Name

The list of **user roles** (page 365).

Policy

The remote control policy applied to a user role.

Message

The text messages applied to a user role.

Machine Policy

Remote Control > Notification Policy > Machine Policy

The **Machine Policy** page determines how you want to notify users a remote control session to their machine is about to begin. This policy is applied to **machine IDs**.

Note: See **User Role Policy** (page 333) to apply remote control notification policies by machine ID. Machine policy takes precedence over user role policy.

Exceptions

K-VNC (page 328) supports all options on this page. **Kaseya Remote Control** (page 342) supports all options on this page except:

- Notify user when session terminates
- Record remote control to a file in the machine working directory

Apply

Click **Apply** to apply policy parameters to selected machine IDs.

Select User Notification Type

- **Silently take control** - Do not tell the user anything. Take control immediately and silently.
- **If user logged in display alert** - Display notification alert text. The alert text can be edited in the text box below this option.
- **If user logged in ask permission** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed

and the VSA removes the dialog box from the target machine. If no user is logged in, proceed with the remote control session.

- **Require Permission. Denied if no one logged in** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed and the VSA removes the dialog box from the target machine. The remote control session is canceled.

Notify user when session terminates.

Supported by WinVNC only. Check this box to notify the user when the session terminates.

Session Termination Message

Displays only if the **Notify user when session terminates** box is checked. Modify the default message if necessary. The <admin> variable is the only variable that can be used in this message.

Notification Alert Text / Ask Permission Text

Displays only if the **Select User Notification Type** is *not Silently take control*. Modify the default message if necessary. The <admin> variable is the only variable that can be used in this message.

Remove

Click **Remove** to clear policy parameters from selected machine IDs.

Require admin note to start remote control

Click this box to require VSA users to enter a note before starting the remote control session. The note is included in the remote control log and is not displayed to the machine user.


Record remote control to a file in the machine working directory

Supported by WinVNC only. If checked, remote control sessions are automatically **recorded** (page 561) for machines assigned this policy.


Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Delete

Click the delete icon  next to a machine ID to clear the policy.

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).

Policy

The remote control policy applied to a machine ID.

Message

The text messages applied to a machine ID.

FTP

Remote Control > Files/Processes > FTP




The **FTP** page establishes an FTP session between the user's local machine and a selected machine ID. FTP sessions can only be initiated from a Windows-based machine. Once the FTP session is initiated, a new browser window pops up displaying the contents of a fixed disk on the managed machine. Just drag and drop files as you normally would.









Note: You can also use **Live Connect** (page 344) to initiate a **File Manager** session with managed machines, depending on the OS type supported.


File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. The **FTP server** is the program on the target machine that listens on the network for connection requests from other computers. The **FTP client** is the program on the VSA user's local machine that initiates a connection to the server. The FTP client machine requires user access rights to the FTP server machine. It is included with the Kaseya Server primarily to provide immediate technical support. Once connected, the client can upload files to the server, download files from the server, rename or delete files on the server and so on. Any software company or individual programmer is able to create FTP server or client software because the protocol is an open standard. Virtually every computer platform supports the FTP protocol. Since Kaseya FTP sessions are relayed through the Kaseya Server, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.

Initiating FTP

Initiate an FTP session by clicking the name of the remote machine. Icons next to the managed machine ID indicate the current connection status for that machine. Only machine IDs with an  or  or  icon can be connected to target machines and have live links; all others will be inactive.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Note: Users can disable remote control and FTP sessions by right-clicking the  icon on their managed machine and selecting **Disable Remote Control**. You can deny users this ability by removing **Disable Remote Control** using **Agent > Agent Menu** (page 59).

Enable verbose relay

Remote control or FTP of machines behind firewalls and NAT gateways may be relayed through the VSA server using a helper application. Checking this box displays a popup window with status information about the normally hidden helper application.

FTP the KServer

Clicking the **FTP the KServer** link starts an FTP session with the Kaseya Server itself. This option only displays for **master role users** (page 564).

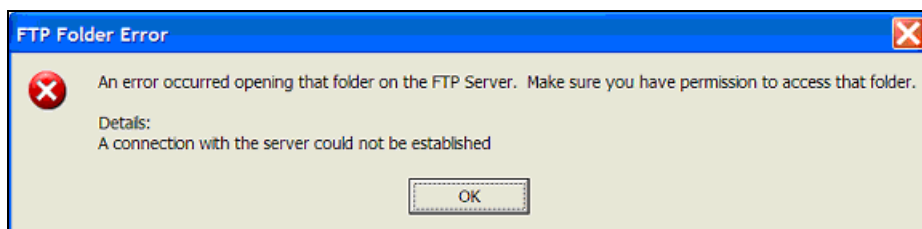
Enable / Disable the Machine User's Ability to Initiate FTP Remotely

Users can enable / disable the machine user's ability to initiate FTP remotely to their own machine from another machine using Agent > [Portal Access](#) (page 67) and System > [Machine Roles](#) (page 367).

FTP Malfunctions

Some reasons for FTP failure with managed machines are:

- The user machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- Anti-virus software on the target machine may block the connection. This problem is eliminated if KES Security protection is installed on the target machine.
- Wrong primary Kaseya Server address - Remote control can only connect through the primary Kaseya Server address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary Kaseya Server address using Agent > [Check-in Control](#) (page 61).
- You accessed the Kaseya Server from a different address. The helper application gets connection information from a cookie on the local machine. To access this information, the helper passes the URL of the Kaseya Server to Windows. Say you downloaded the helper application from `www.yourkserver.net`. Then you open a new browser and access the Kaseya Server by typing in its IP address `192.168.1.34`. The Kaseya Server drops a cookie for `192.168.13.34` while the helper tries to get a cookie corresponding to `www.yourkserver.net`. The helper won't find the cookie. If this happens to you, just download a new helper application and try again.
- FTP requires [Passive FTP](#) be turned **off**. If you get the following error after attempting an FTP session:











Then disable [Passive FTP](#) on your browser as follows:

1. Open [Internet Options...](#) from IE's **Tools** menu.
2. Click on the [Advanced](#) tab.
3. In the [Browsing](#) section, look for [Use Passive FTP](#) and uncheck this setting.
4. Click OK and try FTP again.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of **Machine.Group IDs** (page 556) displayed is based on the **Machine ID / Group ID filter** (page 23) and the machine groups the user is authorized to see using System > User Security > **Scopes** (page 369).




Enter a drive letter to FTP to

Enter the drive letter to FTP to, instead of selecting a remote fixed drive option.

Note: The Kaseya Server determines how many fixed disks a managed machine has via its **Latest Audit** (page 128).

SSH

Remote Control > Files/Processes > SSH

The **SSH** page runs an SSH command line session on a selected, *active* Linux or Apple machine. SSH sessions can only be initiated from a Windows-based machine. Only Linux or Apple machines with an  or  or  icon are active.

ActiveX Control

Remote control, FTP and SSH can only be initiated from Windows OS machines. An ActiveX control automatically configures and runs the package for you. The first time you use any of these packages on a new machine, your browser may ask if it is OK to download and install this ActiveX control. Click yes when asked. If the ActiveX control is blocked by the browser from running, the user is presented with a link to manually download and run the package manually.

Running an SSH Session

1. Click any Linux or Mac machine that displays a hyperlink beneath the machine ID name.
 - A second page states the encrypted SSH session is starting.
 - It attempts to automatically load the ActiveX control. If the ActiveX control fails to load, click the [here](#) hyperlink to download the ActiveX control manually and run it.
 - Once the ActiveX control is downloaded and run, the SSH command line window displays on this same page.
2. The SSH command line session prompts you to enter an administrator username and password.
3. Click the [Back](#) hyperlink to end the SSH command line session.

Task Manager

Remote Control > Files/Processes > Task Manager

The **Task Manager** page performs the same function as Microsoft's Windows NT/2000 task manager. It lists all currently active processes on a managed machine. Clicking the link of a machine ID tasks the agent on the managed machine to collect 10 seconds of process data at the next check-in. **Task Manager** displays the results in tabular form. Task Manager supports all Windows operating systems, Windows 95 and up.

kperfmon.exe

`kperfmon.exe` is a small program run by the agent to collect task data on the target machine. It only runs while collecting task data. On some OS configurations `kperfmon.exe` may take about 4% of the CPU during the 10 seconds required to collect data.

Enable / Disable the Machine User's Ability to Access Task Manager Remotely

VSA users can enable / disable the machine user's access to Task Manager on their own machine remotely from another machine using the System > Machine Roles > [Access Rights](#) (page 368) tab

Name

The name of the process actively running on the managed machine.

CPU

The percent of CPU time consumed by that process over the 10 second data collection interval.

Mem Usage

The amount of main memory used by each active process.

Threads


The number of active threads associated with each active process.

End Process

You can kill any active process on the managed machine by selecting the radio button to the left of the process name and then clicking the [End Process](#) button. In addition to killing the active process, it re-collects the task data again.

Chat

[Remote Control](#) > [Message with Users](#) > [Chat](#)

The [Chat](#) page initiates or continues chat sessions with logged on users  on managed machines. Multiple chat sessions may be active at the same time. Each window title displays the machine ID name for that session. The system automatically removes all messages older than one hour. Press the [Shift-Enter](#) key combination to insert a carriage return into a message.

Note: You can also use [Live Connect](#) (page 344) to chat and video chat with a managed machine. Video chat allows you to video chat with anyone, not just a managed machine user.

To Initiate a Chat Session

Click the machine ID of the machine you wish to start chatting with. A chat session window opens on your machine and a chat window opens in a browser on the remote machine. Enter text in the text pane. Click the [Send](#) button to send the message.

To Respond to a Chat Session

If a chat popup window displays while you are logged on to the Kaseya Server, respond by entering text in the text pane. Click the [Send](#) button to send the message.

Join Session link

Multiple VSA users may participate in the same chat session with a machine user. If a chat session is in progress, the [Join Session](#) link displays next to that machine ID. Click this link to join the session. **If the session was abnormally shut down**, click this link to restart the chat session and recover all messages for the session.

Chatting with Other VSA Users

The names of [logged on](#) VSA users with [scope](#) (page 369) rights to the organizations and group IDs currently displayed by the [machine ID.group ID filter](#) (page 556) display on the [Chat](#) page as well. Click the link of another logged on VSA user to initiate a chat with that VSA user.

Remote Control

Enable / Disable the Machine User's Ability to Initiate Chat with VSA Users

Users can enable / disable the machine user's ability to initiate a chat session with VSA users using the System > Machine Roles > [Access Rights](#) (page 368) tab.

Ensuring Chat Opens a New Window

The default setting for [Internet Explorer](#) reuses open browser windows when any task opens a new URL. This same behavior occurs when you click a link in an email or Word document (the already open browser window is redirected to the new URL). To set Internet Explorer's default behavior to open new URLs in a new window perform the following steps:

1. Select [Internet Option...](#) from the [Tools](#) menu of any Internet Explorer window.
2. Click on the [Advanced](#) tab.
3. Uncheck the box labeled [Reuse windows for launching shortcuts](#) in the Browsing section.
4. Click [OK](#).









My Machine Makes a 'Clicking' Noise Every Time the Chat Window Refreshes

Many Windows themes configure the system to play a sound every time Internet Explorer navigates to a new URL. One of these, `start.wav`, sounds like a click. To turn off the sound perform the following steps:

1. Open the [Control Panel](#) and select [Sounds and Multimedia](#).
2. Click on the [Sounds](#) tab.
3. Scroll down and select [Start Navigation](#) in the [Windows Explorer](#) section.
4. Select [\(None\)](#) from the drop-down control labeled [Name](#).
5. Click [OK](#).

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Play tone with each new message

Check this box to cause a tone to sound every time a new message is sent or received by a chat window.

Automatically close chat window when either party ends chat

Check this box to close the chat window when either party ends the chat. Leave blank, if you want each party to be able to view and copy text from the chat window, even if the other party ends the chat.

Remove your name from chat list seen by other administrators

Check this box to remove your name from the chat list seen by other VSA users.

Remove your name from chat list seen by users

Check this box to remove your name from the chat list seen by machine users.

Send Message

Remote Control > Message with Users > Send Message

The **Send Message** page sends network messages to selected machine IDs. Messages can be sent immediately at the next managed machine check-in, or can be scheduled to be sent at a future date and time.

The message either displays immediately on the managed machine, or the agent icon in the system tray of the managed machine flashes between a white background and its normal background when a message is waiting to be read. When the machine user click's the flashing icon the message displays.

Machine users can also be notified by a conventional Windows dialog box or through a browser window. If a browser window is used, enter a URL instead of a text message. This feature can be handy, for example, to automatically take users to a web page displaying an updated contact sheet or other relevant information.

Enter message/URL sent to remote machines (dialog box or URL)

The text you enter depends on the display window you select.

- Enter a text message if the display window is a dialog box.
- Enter a URL if the display window is a browser.

Select display window

Select the manner in which the user is notified on the managed machine. The default is **Dialog Box**, which displays a standard Windows dialog box with the network message. **Browser** displays a URL in a web browser window.

Send Now

Click **Send Now** to send the message immediately to selected machines. The message displays in the **Messages Not Yet Sent** column until the message is received by the machine. For example, the machine may be offline.

Clear Messages

Click **Clear Messages** to remove messages that have not been delivered to managed machines.

Schedule time to send message

Enter the year, month, day, hour, and minute to send the message.

Schedule

Click **Schedule** to schedule delivery of the message to selected machine IDs using the schedule options previously selected. The message displays in the **Messages Not Yet Sent** column until the message is received by the selected machine.

Display Immediately/Flash Icon

This setting determines how managed machine users are notified once their message has been retrieved from the Kaseya Server.

- **Display Immediately** notifies the user immediately.
- **Flash Icon** flashes the agent icon in the **system tray** (*on page 564*) until the user clicks the icon. The message is then displayed according to the settings in **Select display window**.









Remote Control

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent [Quick View](#) (page 16) window.

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine.Group IDs](#) (page 556) displayed is based on the [Machine ID / Group ID filter](#) (page 23) and the machine groups the user is authorized to see using System > User Security > [Scopes](#) (page 369).

Current User

Displays the currently logged on user.


Messages Not Yet Sent

This column displays messages not yet sent.

Kaseya Remote Control

[Kaseya Remote Control](#) is the primary remote control capability used throughout [Virtual System Administrator™](#). [Kaseya Remote Control](#) connects in seconds to remote machines that already have [Kaseya Remote Control](#) installed. [Kaseya Remote Control](#) maintains a reliable, secure and encrypted connection.

Starting Kaseya Remote Control

Click any agent icon  that supports [Kaseya Remote Control](#) to automatically start or re-start it. You can also hover over the agent icon to display [Quick View](#) (page 16). Click the [Remote Control](#) button to launch [Kaseya Remote Control](#).

Note: You can launch [Live Connect](#) (page 344) by *Ctrl+clicking* the agent icon. You can also click the [Live Connect](#) button in [Quick View](#).

Installing and Updating Kaseya Remote Control

[Kaseya Remote Control](#) is installed as a viewer/server pair of applications: the viewer on the administrator's local machine and the server on the remote agent machine. The [Kaseya Remote Control](#) server is installed as a component of the agent when a new agent is installed, or when the agent is updated using Agent > [Update Agent](#) (page 72).

If the [Kaseya Remote Control](#) application is not already installed on your local administrator machine, when you start your first session a dialog prompts you to download and install it. If already installed and a Kaseya patch release has made a later version available, a dialog prompts you to download and install the updated version. There is no independent launching of the [Kaseya Remote Control](#) application

outside of the VSA.

Main Features

- Supports remote control with or without a machine user being logged in.
- Connects to the console session. If a user is logged on, the administrator shares the console session with the user.
- Allows the administrator to select any additional *monitors* that may be running on the remote system.
- Multiple view sessions can connect to the same agent machine, viewing the same monitor or different monitors.
- Copies and pastes (CTRL+C and CTRL+V) *plain text* between local and remote systems.
- Supports the use of numerous native **Windows and Apple shortcut keys** (<https://helpdesk.kaseya.com/entries/58322696>) on the remote machine.
- Uses the keyboard layout configured on the remote machine. Characters on the administrator's local keyboard might not match the characters shown on the remote user interface. Administrators can temporarily change the keyboard layout on the remote machine to map to their local keyboard. This might apply when entering passwords.
- Connects when a Windows machine is booted into *Safe Mode with Network*.
- A log entry is created in the VSA > System > **System Log** (*page 389*) each time **Kaseya Remote Control** successfully connects to a remote control session.

Note: See **Kaseya Remote Control Requirements**

(<http://help.kaseya.com/webhelp/EN/VSA/7000000/Reqs/index.asp#18007.htm>).

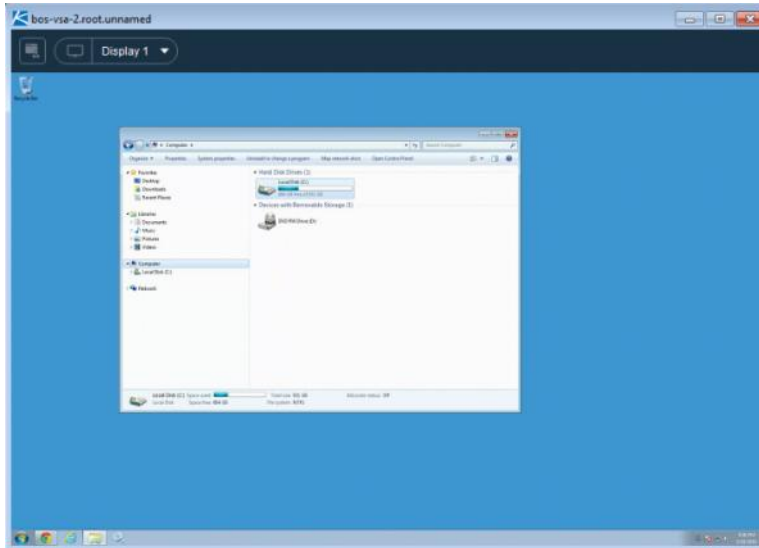
User Interface

The basic layout of the **Kaseya Remote Control** user interface includes the following:

- The machine name displays at the top of the remote control session window.
- A narrow menu bar displays at the top.
- When connecting to Windows machines only, a 'Send CTRL+ALT+DEL' option displays in the menu bar for remote logins.
- When multiple monitors are available on the remote machine, a drop-down list of monitors displays and can be selected to display a specific monitor.
- Closing the window disconnects the session.

Remote Control

- The default screen size for a session window is 1280 X 800. The default position is centered on the screen. New session windows use the size and position last used by the administrator.




Legacy Remote Control Features Removed

With the release of 7.0 all features having to do with RADMIN, PC Anywhere, WINVNC, x11vnc Server and UltraVNC viewer have been removed from the Remote Control module. The Remote Control > [Select Type](#) and [Set Parameters](#) pages have also been removed.

Using K-VNC

A [K-VNC](#) remote control session can be started using the Remote Control > [Control Machine](#) (page 326) page. Administrators should use the K-VNC for situations not supported by [Kaseya Remote Control](#), and when a web-based remote control solution is required. Only K-VNC remote control sessions support [Session recording](#) or [Notify user when session terminates](#) settings, located on the [User Role Policy](#) (page 333) and [Machine Policy](#) (page 334) pages of the [Remote Control](#) module.

Live Connect

[Live Connect](#) is a web-based, single-machine user interface. You can access [Live Connect](#) by Ctrl+clicking the agent icon , or by clicking [Live Connect](#) button in [Quick View](#) (page 16). [Live Connect](#) enables you to perform tasks and functions solely for one managed machine. A menu of tabbed property sheets provide access to various categories of information about the managed machine.



Additional menu items display, depending on the add-on modules installed and the operating system of the target machine.

Note: Both the [Live Connect](#) and [Portal Access](#) plug-in installers can be pre-installed using the [Agent > Update Agent](#) (page 72) page.

Windows

Live Connect for Windows machines supports the following menu items: [Home](#), [Agent Data](#), [Audit](#)

Information, File Manager, Command Shell, Registry Editor, Task Manager, Event Viewer, Ticketing, Chat, Desktop Access and Video Chat.

Windows Cross-Platform OS Support: On Windows XP and later systems, using any of our supported browsers, you can use the File Manager, Command Shell, Registry Editor, Task Manager, Event Viewer, Desktop Access enhanced features with Windows XP and later and File Manager, Command Shell, Desktop Access enhanced features with Mac OS X 10.5 Leopard (Intel) and later systems.

Apple

Live Connect for Macintosh machines supports the following menu items: **Home**, **Agent Data**, **Audit Information**, **File Manager**, **Command Shell**, **Ticketing**, **Chat**, **Desktop Access** and **Video Chat**.

Apple Cross-Platform OS Support: On Mac OS X 10.5 Leopard (Intel) and later systems, using any of our supported browsers, you can use the File Manager, Command Shell, Desktop Access enhanced features with Windows XP and later and Mac OS X 10.5 Leopard (Intel) and later systems.

Linux

Live Connect for Linux machines supports the following menu items: **Home**, **Agent Data**, **Audit Information**, **Ticketing**, **Chat**, and **Video Chat**. Does not include a thumbnail preview image of the desktop in **Live Connect**. Use the **Control Machine** (page 326), **FTP** (page 336) and **SSH** (page 338) pages to remote control Linux agents.

Window Header

Basic information about the managed machine displays at the top of the **Live Connect** window.



- **Thumbnail View** - The desktop of the currently logged on user displays in a thumbnail view, if a user is logged onto the machine.
- **Machine Info** - Lists basic information about the managed machine.
- **Performance Graphs** - Shows CPU % and Memory % performance graphs for the managed machine.
- **Log Off** - Only displays if a machine user using **Portal Access** is logged in remotely from the machine.
- **Help** - Displays online help for **Live Connect**.

Menu Options

A menu of tabbed property sheet provides access to various categories of information about the managed machine.

- **Home** - *The Home tab is the first tab displayed when the Live Connect window opens.*
 - **Home** - Typically the **Home** tab displays a welcome message and the URL page of the agent service provider. The **Run Procedures** section of the **Home** tab enables the **Live Connect** user to run agent procedures on the managed machine immediately. A **Custom Links** section may display on the **Home** tab, if specified by the service provider, offering links to additional resources. Multiple customized **Home** tabs are possible, each with a unique name, if specified by the service provider.
 - **Change Logon** - Changes the *remote* logon user name and password for this managed machine. These logon options enable a user to access the **Live Connect** window to this managed machine from any other machine, including initiating a remote desktop session with the managed machine, if **Desktop Access** is enabled by the service provider. Enter the same URL used to logon to the VSA. Then enter the **Live Connect** user name and password specified in this tab. Accessing **Live Connect** remotely in this manner from another machine is called **Portal Access**. **Portal Access** logon options can also be maintained within the VSA using Agent > **Portal Access** (page 67).

- **Change Profile** - Changes the contact information for this managed machine. This information populates a ticket with contact information when **Live Connect** is used to create a ticket. This information can also be maintained using Agent > **Edit Profile** (page 65).
- **Agent Data** - Displays the following tabs:
 - **Pending Procedures** - Displays and schedules pending agent procedures for a managed machine and the **Procedure History** for that machine. Includes the execution date/time, status and user who scheduled the procedure.
 - ✓ Click the **Schedule Another Procedure** button to schedule a procedure not yet pending. Once selected and scheduled, the procedure displays at the bottom of the **Pending Procedures** section.
 - ✓ Click the **Schedule** button to schedule a selected procedure to run in the future or on recurring basis.
 - ✓ Click the **Run Now** button to run a selected procedure once immediately.
 - ✓ Click the **Cancel** button to cancel any selected pending procedure.
 - **Logs** - Displays the logs available for a machine: Alarm Log, Monitor Action Log, Agent Log, Configuration Changes, Network Statistics, Event Log, Agent Procedure Log, Remote Control Log, Log Monitoring.
 - **Patch Status** - Displays **Missing** and **Pending** Microsoft patches and schedules missing patches. If a machine belongs to a **patch policy** (page 559), missing patches may be further identified as **Denied (Pending Approval)**. The user can manually override the denied patch policy by scheduling the patch.
 - ✓ Click the **Show History** link to display the history of patches installed on the managed machine.
 - ✓ Click the **Schedule** button to schedule the deployment of missing patches.
 - ✓ Click the **Scan Now** button to scan for missing patches immediately.
 - ✓ Click the **Cancel** button to cancel a selected pending patch.
 - ✓ Click the **Set Ignore** button to prevent installing a patch using any of the installation methods. To be installed, the **Set Ignore** checkbox must be cleared.
 - ✓ Check the **Hide patches denied by Patch Approval** - If checked, patches denied by Patch Approval are not displayed.
 - **Agent Settings** - Displays information about the agent on the managed machine:
 - ✓ **Agent version**
 - ✓ **Last check-in**
 - ✓ **Last reboot**
 - ✓ **First time check-in**
 - ✓ **Patch Policy Membership** - Defined using Patch Management > Membership: Patch Policy
 - ✓ **View Definition Collections** - Defined using the **Only show selected machine IDs** option in **View Definitions** (page 24).
 - ✓ **Working Directory** - Can also be defined using Agent > **Working Directory** (page 64).
 - ✓ **Check-In Control** - Can also be defined using Agent > **Check-In Control** (page 61).
 - ✓ **Edit Profile** - Can also be defined using Agent > **Edit Profile** (page 65).
 - **Documents** - Lists documents uploaded to the Kaseya Server for a managed machine. You can upload additional documents. Provides the same functionality as Audit > **Documents** (page 138).
 - **Get File** - Accesses files previously uploaded from a managed machine. Click the link underneath a file to display the file or run it. Provides the same functionality as Agent Procedures > **getFile()** (page 116).

- **Audit Information** - Information tabs include: **Machine Info**, **Installed Apps**, **System Info**, **Disk Volumes**, **PCI & Disk Hardware**, **Printers**, **Software Licenses**, and **Add/Remove Programs**. Provides audit information based on your **Latest Audit** (page 551). You can perform an an immediate audit using the **Machine Info** tab.
 - **File Manager** - Displays two file managers, one for your local machine and one for the managed machine. Using the *upper panes* only you can:
 - Create directories and delete, refresh or rename files or directories using either file manager.
 - *Move* files within the *same* file manager using drag and drop.
 - *Copy* files *between* file managers using drag and drop.
 - **Command Shell** - Opens a command shell on the managed machine. Defaults to the `c:\windows\system32` directory.
 - **Registry Editor** - Displays the registry of the managed machine ID. You can create, rename, refresh or delete keys and values, and set the data for values.
 - **Task Manager** - Lists Windows Task Manager data for the managed machine. You can stop or prioritize **Processes**, stop and start **Services**, check typical **Performance** benchmarks for each process, categorized by CPU, disk, network, and memory, review **Users** session data, **Reboot**, power off the managed machine, or log off sessions on the managed machine, and display **User and Groups** on the managed machine. Launching the **Task Manager** lets you create or modify monitor sets using a wizard, based on processes and services. Hovering the cursor over the monitor icon of a log entry displays a wizard.
 - A monitor wizard  icon displays next to each process and service listed on the **Processes** and **Services** tabs of the **Task Manager**. These two wizards enable you to create a new monitor set criteria based on a selected process or service. The new process or service criteria can be added to any new or existing monitor set. The new or changed monitor set is immediately applied to the machine that served as the source of the process or service criteria. Changing an existing monitor set affects all machines assigned to use that monitor set. See Monitor > Monitor Set > **Process Status** (page 240) and Monitor > Monitor Set > **Services Check** (page 239) a description of each field shown in these two wizards.
 - **Event Viewer** - Displays event data stored on the managed machine by event log type.
 - A monitor wizard  icon displays next to event log entries in the VSA and in **Live Connect**. Hovering the cursor over the monitor wizard icon of a log entry displays a wizard. The wizard enables you to create a new event set criteria based on that log entry. The new event set criteria can be added to any new or existing event set. The new or changed event set is immediately applied to the machine that served as the source of the log entry. Changing an existing event set affects all machines assigned to use that event set. The monitor wizard icon displays in:
 - ✓ Agent > **Agent Logs** (page 31)
 - ✓ Live Connect > Event Viewer
 - ✓ Live Connect > Agent Data > Event Log
 See Monitor > **Event Log Alerts** (page 276) for a description of each field shown in the wizard.
 - **Ticketing** - Displays and creates tickets for the managed machine. Displays and creates tickets for **Ticketing** module tickets or tickets and knowledge base articles for the **Service Desk** module, depending on which module is activated.
- Note:** A service desk must be a member of the Anonymous scope to display **Service Desk** tickets in a machine user **Portal Access** session of **Live Connect**.
- **Chat** - Initiates a chat session with the currently logged on user of the managed machine. You can invite other VSA users to join your chat session. See Remote Control > **Chat** (page 339) for more information.
 - **Remote Control** - Initiates a **Kaseya Remote Control** (page 342) session with the managed machine.

Remote Control

- **Video Chat** - If a machine user is logged on to a managed machine, then a **Live Connect** user can initiate a audio/video chat session with that logged on machine user. The session can be audio only for one or both machines if video is not supported on one or both machines.
 - **Video Chat with the Machine User** - Click the Call button to initiate the video chat session. The machine user will see a browser window or browser tab display on their machine that lets them see your video image and their own video image if their machine has a webcam installed.
 - **Video Chat with Anyone** - Click the Connect URL button. This copies a URL to your clipboard. Copy the URL address into any email or instant message program and send it to anyone. When that URL is entered in a browser the individual will be able to video chat with you. *Video chat does not require the person receiving the chat invitation to be a managed machine.*
 - **Video Chat Confirmation** - The Adobe Flash Player used to transmit the audio/video stream requires each user click an "Allow" button to proceed with their side of the video chat.
 - **Audio/Video Controls** - Hover the mouse over either video image in the chat window to display audio/video controls.
 - **Text Chat** - You can text chat and video chat at the same time using the same window.
- **VPN** - Windows only. Clicking this option creates a VPN connection between your local machine and the **Live Connect** machine. Once connected, the administrator can connect to other machines sharing the same LAN as the **Live Connect** machine, even if those machines do not have an agent installed on them. This includes using applications such as SSH, or telnet or creating another browser instance that targets these other machines on the same LAN. The VPN session ends when the **Live Connect** window closes or the **Stop VPN** button is selected on the **VPN** menu.
- **AntiMalware** - Displays the **AntiMalware** status of the managed machine, if installed.
- **Antivirus** - Displays the **Antivirus** status of the managed machine, if installed.
- **Data Backup** - If **Data Backup** is enabled for the managed machine, you can use this menu to:
 - Run backups immediately.
 - Restore selected backups, directories and files, but only to the same machine.
 - Display the status and history of backups.
- **Discovery** - Displays the **Network Discovery** status of the machine, if installed.

Plugin Manager

Live Connect's enhanced functionality of the browser is managed by a *plug-in manager*.

- **Plug-in Manager Installation** - The user is prompted to install Plug-in Manager after the first logon. Installation of the Plug-in Manager can be deferred until **Live Connect** is started for the first time.
- **Plug-in Updates** - IE and Firefox browsers will detect plug-ins that are out of date and automatically download them in the background. Browser restart is not required for these two browsers. Chrome and Safari browsers also detect out of date plug-ins and automatically download them in the background, with little to no user interaction required.

Additional Notes

- Access to specific **Live Connect** functions depends on access rights in System > User Roles > **Access Rights** (page 366) and Machine Roles > **Access Rights** (page 368).
- All of the **Live Connect** menu options are enabled when the machine is connected to **Live Connect**. Only **Home**, **Audit Information**, **Agent Data** and **Ticketing** are enabled when the machine disconnected from **Live Connect**.
- You can customize the **Live Connect Home** page using System > Customize: **Live Connect** (page 398).
- **Event Viewer** data does not depend on Agent > **Event Log Settings** (page 34).

- If a `externalLink.xml` exists in the `\Webpages\install` directory of the Kaseya Server a **New Ticket** link displays next to the **Help** link in **Live Connect**. Clicking the **New Ticket** link redirects users to the URL specified in `externalLink.xml`. See **Customized New Ticket Link** (page 349) for details.

Customized New Ticket Link

To customize **New Ticket** links on the **Live Connect** page, fill out the `externalLink.xml` file as described in the comments section of the XML below. To activate the new ticket link, place the `externalLink.xml` file in the `\WebPages\install\` directory of your Kaseya Server.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<externalLinks>
  <!--
  URL STRING SUBSTITUTIONS: The URL string displayed is associated
  with a particular machine ID. The string is searched for the following
  case sensitive values and substituted for the values below.
  machineNameVal - the machine name for the active machine is substituted
                   in the URL string.
  groupNameVal - the group name for the active group.
  -->
  <ticketLink displayName="Ext Ticket"
  url="http://192.168.212.52/?mname=machineNameVal&gname=groupNameVal"/>
</externalLinks>
```


Chapter 9

System

In This Chapter

System Overview.....	352
User Settings.....	353
System Preferences.....	356
User Security.....	359
Orgs/Groups/Depts/Staff.....	372
Server Management.....	377
Customize.....	393

System Overview

System

The **System** module enables users to maintain policies for the entire system:

- **Preferences**
- **User Security**
- **Organizations, Groups, Departments and Staff**
- **Server Management**
- **Customization**
- **Database Views**

Functions	Description
Preferences (page 353)	Sets system-wide preferences that apply only to the currently logged in user.
Change Logon (page 355)	Changes the username, password and security question of the currently logged on user.
Check-in Policy (page 356)	Set limits on a variety of agent check-in parameters.
Naming Policy (page 358)	Automatically enforces naming policies based on each machines IP address, network, and computer name
Users (page 360)	Creates, edits and deletes users.
User Roles (page 365)	Creates and deletes user roles. User roles determine the access rights for VSA users. Assign roles types to user roles.
Machine Roles (page 367)	Creates and deletes machine roles. Machine roles determine the access rights for machine users. Assign role types to machine roles.
Scopes (page 369)	Assigns organization, machine groups, machines, departments and service desks to scopes.
Logon Hours (page 372)	Specifies when users can logon to the VSA.
User History (page 372)	Displays the functions visited in the last 30 days for each user.
Manage (page 372)	Defines organizations, groups, departments and staff members of departments.
Set-up Types (page 376)	Defines types of organizations.
Request Support (page 377)	Accesses Kaseya support.
Configure (page 377)	Displays Kaseya Server information, license code and subscription information, obtains latest server updates, and server IP information.
Default Settings (page 384)	Specifies default settings for server management. Applies to all tenant partitions (page 564).
License Manager (page 386)	Allocates available agent and user licenses.
Import Center (page 388)	Imports and exports user-defined automation solutions into and out of the VSA.
System Log (page 389)	Logs events that can not be tracked by machine ID.
Statistics (page 389)	Displays VSA server performance statistics

Logon Policy (page 391)	Sets user logon policies.
Application Logging (page 392)	Enables or disables logging of application-layer transactions. Typically used only by Kaseya support.
Outbound Email (page 392)	Defines the email server for outbound email.
Color Scheme (page 14)	Determines the set of colors displayed by the VSA environment for the current user.
Site Customization (page 394)	Customizes the user interface for all users. <ul style="list-style-type: none"> • Logon Page • Site Header • Report Header • Agent Icons
Local Settings (page 397)	Sets tenant-partition-specific (page 564) settings.
Live Connect (page 398)	Customizes the Live Connect home pages seen by VSA users and machine users.
Database Views (page 419)	Configures database view access.

VSA Logon Policies

Once a VSA user is defined in System > [User Security](#) (page 359), a number of functions manage when and how users can logon and the features that are available to them during logon.

VSA user logon options are specified using:

- System > [Users](#) (page 360) - Optionally reset the user's password, or force the user to change his or her password, or enable/disable the user's logon or log a user off.
- System > [Preferences](#) (page 353) - The [Preferences](#) page sets preference options that typically apply *only to the currently logged in* user.
- System > [Change Logons](#) (page 355) - The [Change Logon](#) page sets your VSA logon username and password. These preference options apply *only to the currently logged on* user.
- System > [Logon Policy](#) (page 391) - The [Logon Policy](#) page sets logon policies that apply to all VSA users.
- System > [Logon Hours](#) (page 372) - The [Logon Hours](#) page determines *when* users can logon to the VSA by specifying the weekdays and hours for each user role. Each day of the week can have different hours of operation set.
- System > Site Customization > [Logon Page](#) (page 394) - Set options that display on the logon page.
- System > Site Customization > [Site Header](#) (page 394) - Set options that display on the logon page.

Note: Additional logon options *for machine users only* are set in Agent > [Portal Access](#) (page 67).

User Settings

[User Settings](#) pages set options that typically apply *only to the currently logged on* user.

Preferences

System > [User Settings](#) > [Preferences](#)

The [Preferences](#) page sets system-wide preferences that apply *only to the currently logged on* user. This includes the email address where you receive alert messages.

Note: Three options on this page apply to *all* users and only display for master role users: setting the **System Default Language Preference** and the **Download** button for installing language packs, and **Show shared and private folder contents from all users**.

Note: See **VSA Logon Policies** (page 353) for a summary of functions affecting user logons.


Set email address to deliver messages for this administrator to

Specifies the email address that alerts, ticket notifications and other email messages will be sent to. After entering the email address, click **Apply** to make it active. Previously set alerts retain the original email recipient addresses specified when the alerts were set.


Set first function after logon

Select the name of the function you want to see when you first log on to the Kaseya Server.

Set delay before displaying detail information when hovering over information icon

A  information icon displays for each ticket row in Ticketing > **View Summary** (page 400) and Service Desk > **Tickets** (<http://help.kaseya.com/webhelp/EN/KSD/7000000/index.asp#3646.htm>). Hovering the cursor over the icon displays a preview of the ticket. Specify the number of milliseconds to wait before the ticket preview window displays, then click the **Apply** button. Click the **Default** button to set this value back to its default.

Set delay before displaying detail information when hovering over agent icon

An agent check-in icon, for example , displays next to each machine ID account in the VSA. Hovering the cursor over the icon displays an **agent quick view window** (page 16). Specify the number of milliseconds to wait before the agent quick view window displays, then click the **Apply** button. Click the **Default** button to set this value back to its default.

Select time zone offset

Select one of the following time zone offset options, then click **Apply**. See **Scheduling and Daylight Savings Time** (page 355).

- **Use time zone of the browser logging into the system**
- **Use time zone of the VSA server** - The time currently shown by your VSA browser displays next to this option.
- **Use fixed offset from the VSA server <N> hours**

Note: Date format is set in **System > Configure** (page 377).

Set up language preferences

- **My language preference is** - Select the language you prefer displayed when you're logged into the VSA. The languages available depend on the language packages installed.
- **System default language preference is** - Select the default language used by the VSA user interface for all users. The languages available depend on the language packages installed. This option only displays for **master role users** (page 564).
- **Download a Language Package** - Display a dialog box that enables you to download and install language packages. A language package enables the VSA user interface to be displayed in that language. This option only displays for **master role users** (page 564).

Show shared and private folder contents from all users - Master Admin Only

If checked, a master role user has visibility of all shared and private folders. For private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

Select display format for long names

The web pages are designed to display well for typical string sizes. Occasionally data fields contain long names that will not display properly on the web pages. You can specify how long names display as follows:

- **Limit names for better page layout** - This setting limits the string size to fit well on the web page. Strings exceeding a maximum length are limited with a ... To view the entire name, hover the mouse over the string and a tool tip pops up showing the entire name.
- **Allow long name wrapping** - Long strings are allowed to wrap within the web page. This may disturb the normal web page layout and names may wrap at any character position.

Clear Snooze

Click **Clear Snooze** to clear all outstanding task notification messages. Task notification messages are generated for tasks that are assigned to you and for tasks that are past due. Tasks are defined using the Info Center > **View Dashboard** (page 210) page.

Defaults

Click **Defaults** to reset all settings to system defaults for this user.

Scheduling and Daylight Savings Time

The VSA does not automatically adjust scheduled events for changes between standard time (ST) and Daylight Savings Time (DST). When a task is scheduled, the time zone used to schedule that task is converted into the time used by the Kaseya Server. Regardless of the time zone preferences set by the user in System > Preferences or whether **agent time scheduling** (page 547) is used or not, once scheduled the task only “knows” the Kaseya Server time it is suppose to run.

The following workarounds are available.

- **Use the System Clock Used by the Kaseya Server – On Premise only** - If the system clock used by system hosting the Kaseya Server is configured to adjust for DST, then scheduled VSA tasks will adjust as well. This option is not available with SaaS because the same instance hosts multiple tenants in different countries and time zones. DST adjustments differ for each country. SaaS instances are set to Greenwich Mean Time (GMT) and never change.
- **Schedule Once – On Premise and SaaS** - The easiest method of managing ST/DST changes is to set the schedules once and plan to run them one hour earlier or later, depending on whether ST or DST was used. For example, in the United States, DST runs for the majority of the year, 238 days out of 365. So for the U.S., scheduling using the DST version of your timezone is recommended.

Change Logon

System > User Settings > Change Logon

The **Change Logon** page sets your VSA logon username and password. These preference options apply *only to the currently logged on user*.

Note: See **VSA Logon Policies** (page 353) for a summary of functions affecting user logons.

Changing Your VSA Logon Name and/or Password

To change your logon name and password:

1. Enter a new name in the **Username** field.

Note: The **Username** field cannot be edited if **Prevent anyone from changing their logon** is checked in **System > Logon Policy**.

System

2. Enter your old password in the **Old Password** field.
3. Enter a new password in the **New Password** field. Passwords are case-sensitive.
Note: If you would like the system to generate a strong password for you, click **Suggest**. A dialog box displays showing the new password; the new password is automatically entered in the **New Password** and **Confirm Password** fields. Be sure to write it down before clicking OK and closing the dialog box.
4. Confirm the password by re-typing it in the **Confirm Password** field.
5. Enter a **Security Question** and **Security Answer**. This enables you to request a new password if you forget your password.
Note: Clicking the **Forgot Password?** link on the logon page—if activated using the System > Site Customization > **Logon Page** (page 394) tab—emails you a link where you can change your password. To change your password, you must have already filled out a **Security Question** and **Security Answer** using System > **Change Logon** (page 355).
6. Click **Change**.

Note: The **Discovery** add-on module can be used to manage VSA user logons and Portal Access logons using domain logons (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#7293.htm>).

System Preferences

Check-in Policy

System > System Preferences > Check-in Policy

The **Check-in Policy** page defines group ID policies controlling the minimum, maximum and fixed values allowed for a variety of options. These policies prevent users from selecting settings that place undue stress on Windows servers running the Kaseya Server.

Changing One Field at a Time

If you need to make a change to only one setting in a group:

1. Enter a new value in the field you want to change.
2. Leave all other fields empty. This indicates that these fields will remain unchanged.
3. Click **Update**.

Min/Max Age for Log Entries

These values determine the minimum and maximum values that can be entered in the **Set Max Age for Log Entries** options in Agent > **Log History** (page 32). To remove a value, enter 0 (zero).

Check-In Period

These values determine the minimum and maximum settings that can be entered in the **Check-In Period** setting of Agent > **Check-In Control** (page 61). To remove a value, enter 0 (zero).

KServer Address (0 for editable) - Primary/Second

Two KServer address fields can be specified. The agent checks into the primary server but not the secondary server unless the primary server goes offline.

If 0 is entered in the **Primary** or **Secondary** fields and **Update** clicked, then the **KServer (1st) (2nd)** column of selected group IDs displays Editable. Users can enter any domain name server (DNS) name or IP address they like in the **Primary KServer** and **Secondary KServer** fields in Agent > **Check-in Control**.

If these checkboxes are checked and *DNS names or IP addresses are entered* in these fields and **Update** clicked, the **KServer** column of selected group IDs display fixed DNS names or IP addresses.

Users are required to use these fixed IP addresses in the **Primary KServer** and **Secondary KServer** fields in Agent > **Check-in Control**.

Best Practices: Although a public IP address may be used, Kaseya recommends using a domain name server (DNS) name for the Kaseya Server. This practice is recommended as a precaution should the IP address need to change. It is easier to modify the DNS entry than redirecting orphaned agents.

Allow automatic account creation for selected Group ID

If enabled, new machine ID accounts are created automatically for selected group IDs as soon as the machine's agent checks into the Kaseya Server the first time using a new machine ID name and selected group ID.

For example, an agent is installed on a new machine. The group ID `acme` already exists, but the machine ID `ksmith` does not. With this option enabled for the `acme` group ID, the `ksmith.acme` machineID.group ID account is created as soon as the agent checks in the first time.

Note: Allow automatic account creation for selected Group ID is enabled by default.

To enable automatic account creation for selected group IDs:

1. Check **Allow automatic account creation for selected Group ID**.
2. Select group IDs in the paging area.
3. Click **Update**.

`Auto Enabled` displays in the **Group IDs/Auto Acct** column of selected group IDs.

Allow automatic account creation for groups without a policy

This option only displays for **master role users** (page 564). If enabled, new machine ID accounts are created automatically for group IDs that do not have any **Check-in Policy** defined, or for agents with a group ID that does not yet exist, as soon as the machine's agent checks into the Kaseya Server the first time using a new machine ID name.

Note: Allow automatic account creation for groups without a policy is enabled by default.

Update

Click **Update** to apply policy parameters to selected group IDs.

Remove

Click **Remove** to remove policy parameters from selected group IDs.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Groups IDs

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

Auto Acct

`Auto Enabled` indicates automatic account creation is enabled for this group ID.

Log Age (Min) / Log Age (Max)

Lists the settings entered in the **Set Max Age For Log Entries** fields in the header, for each group ID.

System

KServer (1st) (2nd)

Lists the IP addresses/host names of the primary (1st) and secondary (2nd) servers allowed for group IDs.

Check-in (Min) / Check-in (Max)

Lists the settings entered in the **Check-In Period** fields in the header, for each group ID.

Naming Policy

System > System Preferences > Naming Policy

The **Naming Policy** page defines the IP address criteria used to automatically re-assign machines to a different machine group. Each machine group can be assigned multiple naming policies.

Naming policies can also force the renaming of a machine ID, if the machine ID name doesn't match the computer name, reducing confusion when administering managed machines.

Assigning machines to machine groups by IP addresses has the following benefits:

- Typically an organization represents a single customer enterprise and group IDs and subgroups represent locations within that enterprise. When an employee transfers to a new location, the managed machine can be automatically re-assigned to the appropriate machine group or sub-group for that location as soon as the managed machine's agent checks in from the new location's network.
- Using **managed variables** (page 107), managed machines can run procedures that access *locally available resources* based on the group ID or subgroup ID. Using **Naming Policy** this benefit can be applied automatically by IP address even to a highly mobile workforce that travels between different enterprise locations.
- Maintaining multiple agent install packages in Agent > **Deploy Agents** (page 35), one for each organization, can be time consuming. Instead some server providers use a single agent package for the unnamed organization and perform all installs using this package. System > **Naming Policy** (page 358) can reassign new agents to the correct organization.group ID automatically—the first time the agents check in—based on each managed machine's IP or connection gateway. Agent > **Copy Settings** (page 55) may be used afterwards, to manually copy specific kinds of agent settings by **machine ID template** (page 557) to the type of machine revealed by the initial audit.

Connection Gateway

Optionally check the **Connection Gateway** checkbox and enter the connection gateway IP address. The connection gateway is typically the WAN address of the managed machine. This rule can be applied independently to a group ID. The managed machine must have this IP address as its connection gateway to be automatically assigned to the group ID.

IP Range

Optionally check the **IP Range** checkbox and enter an IP address range, such as 192.168.1.2 – 192.168.1.254. This rule can be applied independently to a group ID. The IP address of the managed machine must fall within this range to be automatically assigned to the group ID.

Force machine ID to always be computer name

Optionally check the **Force machine ID to always be computer name** checkbox to force each machine ID name to match its corresponding computer name. This rule can be applied independently to a group ID.

Note: Machines are renamed to the new group ID at their next full check-in (page 552). The quick check-in (page 552) cycle does not trigger a rename. To rename a group of machines quickly using Naming Policy, schedule the Force Check-in sample agent procedure located in Agent Procedures > Schedule / Create (page 80).

Update

Click **Update** to apply the naming policy to the selected machine group. The system immediately begins enforcing the group ID's new rule as machines check into the Kaseya Server.

Add

Click **Add** to add a new naming policy to existing naming policies for a selected machine group.

Note: Each machine group can be assigned multiple naming policies. Use this capability to automatically assign machines with different IP address ranges to the same machine group.

Clear

Click **Clear** to remove the naming policy from a machine group. The system immediately stops applying the rule for the machine group.

Machine Group

This column lists the machine groups defined for the system. Select the radio button beside a **Machine Group** before updating, adding or clearing a naming policy.

Connection Gateway

Displays the connection gateway assigned to the machine group.

IP Range

Displays the IP ranges assigned to the the machine groups.

Force Machine ID

Displays a check mark if **Force machine ID to always be computer name** is enabled for a machine group.

User Security

System > User Security

User Security determines the access users have to functions and data objects within the VSA. Understanding **User Security** configuration is easiest if you consider each of the following concepts in the order presented.

1. **Scope Data Objects** (page 372) - A **data object** is an object that you create and name. **Scope data objects** are important enough to warrant being secured system-wide. Scope data objects include organizations, machine groups, machines, departments and service desks. Scope data objects are defined *first*, before being assigned to scopes.
2. **Scopes** (page 369) - Sets of data objects that users have *visibility* of within the VSA.
3. **User Roles** (page 365) - Sets of VSA functions that VSA users can perform. A **function** *acts on data objects*. Examples of functions are opening, adding, editing or deleting records.
4. **User Role Types** (page 367) - Built-in classifications that determine the types of *user-role-based* licenses to apply to users in user roles.
5. **Machine Roles** (page 367) - Sets of **Portal Access** (page 67) functions that machine users can perform when displaying the VSA **Portal Access** page on their machine.
6. **Machine Role Types** (page 368) - Built-in classifications that determines the type of *machine-role-based* licenses to apply to machines in a machine role.
7. **Users** (page 360) - Refers to VSA users. Users of machines with agents on them are always identified as *machine users* to distinguish them from VSA users.

Users

System > User Security > Users

The **Users** page creates and deletes user accounts. This page can also assign users to **User Roles** (page 365) and **Scopes** (page 369) when the user account is created.

Each user must be assigned at least one role and one scope. You can assign multiple roles and scopes to a user, but *only one role and one scope is active at any one time*. The active role and scope are selected using the **Role** and **Scope** drop-down lists in the top-right corner of the page. You can reset the user's password, enable/disable user logons and log off users if you have access to these functions.

Note: Each user can change their own logon name, password and email address using **System > Preferences** (page 353).

Warning: To simplify management and auditing of your VSA, provide each user with their own unique logon name. Avoid using generic logons like **User** or **Admin**. Generic logons make it difficult to audit the administrative actions taken by each user.

Creating a New User

1. Click **New**. The **Add User** dialog box displays.
2. Enter **User Information**:
 - Enter a **Email Address** for the new user.
 - Select an **Initial Role** for new user.
 - Select an **Initial Scope** for the new user.
 - Enter a **First Name** and **Last Name**.
3. Enter **Related Org Staff Member** information:
 - Select a **Staff Org**.
 - Select a **Staff Dept**.
 - Enter or select a **Staff Member** or create a new staff member record.
4. Define **User Credentials**:
 - Enter a **User Name**.
 - Enter a password in the **Password** and **Confirm Password** fields. Passwords are case-sensitive.

Note: If you would like the system to generate a strong password for you, click **Suggest**. The new password is automatically entered in the **Password** and **Confirm Password** fields. Be sure to write it down before clicking **OK** and closing the dialog box.

- Check the **Require password change at next logon** checkbox to force the user to enter a new password when they first logon.
5. Click **Save**. The new user displays in the middle pane.

Changing an Existing User Record

1. Click a **User** displayed in the middle pane.
2. Optional **Edit** the following attributes of the User record:
 - **First Name**
 - **Last Name**
 - **Email Address**
 - **Staff Org**

- [Staff Dept](#)
 - [Staff Member](#)
3. Optionally add or remove roles using the [Roles](#) tab.
 4. Optionally add or remove scopes using the [Scopes](#) tab.
 5. Optionally specify access to machines or other assets using the Personal Scope tab.
 6. Optionally change the password by clicking the [Set Password](#) button.
 7. Optionally force a user to change their password by clicking the [Force Password](#) button.
 8. Optionally enable / disable user logons by clicking the [Enable](#) or [Disable](#) buttons.

Set Password

Select a user in the middle pane and click [Set Password](#) to change the password for the selected user. Passwords are case-sensitive.

Force Password

Forces a selected user in the middle pane to change their logon the next time they logon.

Enable / Disable

Select a user in the middle pane and click [Enable](#) or [Disable](#) to enable or disable a selected user's ability to logon to the VSA. This does not affect users already logged onto the VSA. A [Disabled](#) column in the middle pane indicates whether a user is prevented from logging on to the VSA.

Log Off

A column in the middle pane indicates whether a user is currently logged on. Select a logged on user, other than yourself, in the middle pane and click [Log Off](#) to log off that user. *Users are still logged on if they close their browser without logging off.* The [Minutes of inactivity before a user session expires](#) setting in System > [Logon Policy](#) (page 391) determines when the inactive user sessions are automatically logged off.

Note: See [VSA Logon Policies](#) (page 353) for a summary of functions affecting user logons.

Master User vs. Standard Users

A master user is a VSA [user](#) (page 564) that uses a [Master](#) user role and a [Master](#) scope. The [Master](#) user role provides user access to all functions throughout the VSA. The [Master](#) scope provides access to all scope data objects throughout the VSA. A [Master](#) user role can be used with a non-[Master](#) scope, but a [Master](#) scope cannot be used with a non-[Master](#) role. Kaseya Server management configuration and other [specialized functions](#) (page 365) can only be performed by [Master](#) role users. The term *standard user* is sometimes used to indicate a user that does not use a [Master](#) user role and a [Master](#) scope.

Master Users

- Any user can be assigned a [Master](#) user role and [Master](#) scope, if sufficient roletype licenses exist.
- [Master](#) *role* users can view and operate all navigation and control options provided by the user interface.
- [Master](#) *scope* users can view, add, edit or delete all scope data objects: organizations, machine groups, machines, departments, and service desks.
- Masters can add or delete any user, including other master users. Since even a master user can't delete their own account while logged on, the system requires at least one master user be defined at all times.

System

Standard Users

- A standard role user cannot see roles they have not been granted permission to see.
- A standard scope user cannot see data objects or users they have not been granted permission to see.
- Standard users can create other users, scopes and roles, if given access to these functions.
- A standard user can *not* grant access privileges beyond the ones the standard user has.
- Standard users, if permitted function access, can only create other standard users, not master users.
- By default, a new standard user inherits the scopes and roles of the standard user that created him.
- If a master user creates a new standard user, the standard user inherits *no* scopes or roles. Using this method the master user has to manually assign the scopes and roles of the new standard user.

Machine Users

- Machine users use machines with VSA agents installed on them. They should not be confused with VSA users who can logon to the VSA.
- Machine users can click the agent icon on the machine's system tray to see a VSA **Portal Access** (page 67) window of functions and data related to that single machine. **Portal Access** is called **Live Connect** (page 344) when accessed from the VSA.
- Access to **Portal Access** functions are determined by the machine role the machine is assigned to. Managed machines are assigned to the Default machine role by default and have access to all machine user **Portal Access** functions, unless limited by a VSA user.
- Data object access from the machine is determined by the Anonymous **scope** (page 369). Currently, the only data objects enabled by the Anonymous scope are **Service Desk** tickets. All other data seen in **Portal Access** is generated by the machine itself.

Create a New Master User

Forgotten User Password

If you have forgotten your master user account password, the system provides a way for you to create a new master user account or reset just the password of an existing master user account. This enables you to log back in to the system and retrieve the forgotten account information. A master user is a VSA **user** (page 564) that uses a **Master** user role and a **Master** scope.

Note: You must have administrator privileges on the Kaseya Server. Due to security reasons, you cannot perform the following procedure remotely.

Creating a New Master User Account

1. Log in to the machine running the Kaseya Server.
2. Access the following web page:
`http://localhost/LocalAuth/setAccount.asp`
3. Enter a new account name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Enter an email address in the **Email Address**.
6. Click **Create**.

You can now log on to the system using the new master user account.

Reset the Password of an Existing Master User Account

Note: The master user account cannot be disabled.

1. Log in to the machine running the Kaseya Server.
2. Access the following web page:
`http://localhost/LocalAuth/setAccount.asp`
3. Enter an existing, enabled master account user name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Skip the **Email Address**. You cannot reset the email address of an existing user using this web page.
6. Click **Create**.

You can now log on to the system using the existing master user account.

If Your Account Is Disabled

If your VSA account is disabled because you entered the wrong password too many times, then you can choose to wait for a set period of time for the account to be automatically re-enabled. By default this time period is 1 hour, but the waiting period may have been adjusted by your VSA system administrator.

If your account has been disabled for another reason, you will have to contact your VSA system administrator to re-enable your account. A disabled user account cannot be re-enabled by resetting the password.

To create a new master account on the Kaseya Server see: [Create a New Master User](#) (page 362).

Changing Passwords Used by External Applications

External Applications and Authentication Using the Web Service API

External applications can be integrated to the VSA via the [Web Service API](#) (page 470). These external applications can be provided by independent software vendors (ISVs) such as Autotask, ConnectWise, or Tigerpaw. External applications can also be developed by consulting firms, or any organization with technical expertise. To use the Web Service API, external applications must be programmed to authenticate using a valid VSA user name and password.

V6.2 Password Changes that Impact External Applications

VSA v6.1 and prior versions used a SHA-1 algorithm to hash passwords. Therefore, external applications that were compatible with v6.1 used an authentication method based on SHA-1. Beginning with v6.2, a SHA-256 algorithm is used to hash any password that is created under v6.2. Passwords created in prior versions of the VSA remain hashed with SHA-1 until such time as the password is changed or the user is renamed at which point the password is hashed using SHA-256. External applications that were used with v6.1 must be updated, via a programming change, to support SHA-256 passwords in v6.2.

Updating External Applications and Passwords

If you used v6.1 or a prior version of the VSA with an external application, ensure the compatibility of the credential being using. Kaseya recommends arranging to get an updated version of the external application that is compatible with VSA v6.2. Until then, following the procedure for [Creating a New SHA-1 Credential for a Legacy External Application](#) described below can be used to maintain compatibility with third party applications.

Warning: Changing a password used by a legacy external application will **disable the integration** until either the external application is updated to use the required SHA-256 hashing algorithm or a new SHA-1 credential is created and implemented. Ensure passwords used by external applications are not changed before the update is implemented.

If you used v6.1 or a prior version of the VSA with an external application provided by an ISV or other party:

1. Contact the ISV or party who developed the external application.
2. Request an updated version of the external application.
3. Implement the updated version of the external application.
4. At this point, you can change the password or rename the account used by the external application.

For ISVs or parties responsible for the development of external applications

1. Refer to the **Hashing Algorithm** section of the **Authenticate** (page 485) topic in online help. This section provides instructions on how to update the external application to be compatible with VSA v6.2, while also retaining compatibility with prior versions of the VSA.
2. Implement the required programming change to the external application.

Creating a New SHA-1 Credential for a Legacy External Application

If you are running VSA v6.2 or later, and need to create an SHA-1 username and password that is compatible with a legacy external application, and that has not yet been updated to be compatible with v6.2 passwords, use one of the following procedures. You can either create a new master user and password, or reset just the password of an existing master user.

Note: You must have administrator privileges on the Kaseya Server. For security reasons, you cannot perform the following procedure remotely.

Creating a New Master User Account

1. Log in to the machine running the Kaseya Server.
2. Access the following web page:
`http://localhost/localAuth/setAccountV61.asp`
3. Enter a new account name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Enter an email address in the **Email Address**.
6. Click **Create**.

The external application can now be updated to use the new user account and SHA-1 password to connect to the VSA.

Reset the Password of an Existing Master User Account

Note: The master user account cannot be disabled.

1. Log in to the machine running the Kaseya Server.
2. Access the following web page:
`http://localhost/localAuth/setAccountV61.asp`
3. Enter an existing, enabled master account user name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.

5. Skip the **Email Address**. You cannot reset the email address of an existing user using this web page.
6. Click **Create**.

The external application can now be updated to use the new SHA-1 password to connect to the VSA.

User Roles

System > User Security > User Roles

The **User Roles** (page 365) page creates and deletes user roles. Within an user role you can select:

- **Members** (page 365) - Assign or remove members for a user role.
- **Access Rights** (page 366) - Select the access rights for a user role. Access rights determine the functions a *user* can access.
- **Role Types** (page 367) - Assign or remove role types for a user role. Access rights are restricted by the set of licensed role types assigned that user role.

VSA users can belong to one or more VSA user roles. Each user role must be assigned to at least one user role type.

Note: A VSA user logs on with both a user role (functions they can perform) and a scope (scope data objects they can see). Membership in a user role and a scope is independent of each other.

Note: VSA users can also be assigned to user roles using the System > Users (page 360) > Roles tab.

Note: See System > Users (page 360) for a discussion of the Master user role.

Warning: Restrict access to **User Roles** and **Roles** for all roles except roles responsible for administrating function access.

Middle Pane

You can perform the following actions in the middle pane of **Roles**:

- **New** - Create a new role.
- **Copy Permissions** - Copy the access rights to the selected role from any other role.
- **Rename** - Rename the role. Role names can only be all lower case.
- **Delete** - Delete the selected role. All VSA users must be removed from a role before you can delete it.

Related Pages

The following policies are assigned by user role:

- Access to the entire VSA by weekday and hour using System > **Logon Hours** (page 372)
- Remote control user notification using Remote Control > **User Role Policy** (page 333)
- Field permissions for editing tickets in Ticketing > **Edit Fields** (page 412) and Service Desk > Role Preferences
- **Sharable objects** (page 370)—such as procedures, reports, monitor sets and agent installation packages—can be shared by user role.

Members tab

The **Members** tab displays which VSA users are assigned to the role selected in the middle pane.

- Click the **Assign** and **Remove** buttons to change the role VSA users are assigned to.
- Sort and filter the VSA users listed in the **Members** page.

Access Rights tab


The **Access Rights** tab in the System > **User Roles** page determines what functions VSA users belonging to a selected role can perform. For example, access rights can include whether or not a user can open, add, edit or delete a particular record.

Note: **Scopes** determine whether a user can *see* certain user-created data structures displayed in the VSA. **Roles** determine access rights to the functions that act on those data structures.

A navigation tree provides access to each module, folder, item, and control in the VSA.

- Click the or icons next to any item in the tree to display or hide child branches of that item.
 - A checked item means a role provides access to that item.
 - A unchecked item means a role does *not* have access to that item.
 - Click **Expand All** to expand the entire tree.
 - Click **Collapse All** to collapse the entire tree.
- Click **Set Role Access Rights** to change access rights for a role.
 - Checking or clearing any checkbox sets the same state for any child items.
 - Click **Enable All** to enable all items.
 - Click **Disable All** to disable all items.

Specialized Access Rights

- Info Center > Dashboard > **Admin Notes**
- Info Center > Dashboard > **Status**
- Info Center > Dashboard > **Online Help**
- Quick View - Hovering the cursor over a check-in icon displays an agent **Quick View** window immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent **Quick View** window. You can use **agent badges** (page 16) to display **Special Instructions** text in the bottom of the the **Quick View** window.
 - **Quick Launch Functions** - Shows or hides the action buttons that display along the top of the Quick View popup window.
 - **Run Procedure Now**
 - ✓ **Execute Procedures** - Shows or hides all agent procedure in the Quick View **Run Procedure Now** list.
 - ✓ **Edit Procedure List** - Shows or hides the add and delete buttons in the Quick View **Run Procedure Now** list.
 - ✓ **Change Settings** - Shows or hides the configuration gear icon  in the Quick View title bar. The configuration settings let the user show, hide or re-order the list of options displayed in the Quick View popup window, according to user's own preferences.
 - **Quick View Data** - Shows or hides agent data options in the Quick View popup window.
- System > System Preferences > **Functional Access** - (*Deprecated*)
- System > System Preferences > **Enable Scheduling** - Applies to the **Schedule** button for the following functions only. For more information see the **Kaseya knowledge base** (<https://helpdesk.kaseya.com/entries/33901207>).
 - Patch Management > Manage Machines > Scan Machine
 - Patch Management > Manage Machines > Initial Update
 - Patch Management > Manage Machines > Automatic Update
 - info center > Reporting > Reports
 - Info Center > Reporting > Report Sets

- System > System Preferences > Enable Wake on LAN - Applies to Patch Management > Scan Machine > Schedule button only

Role Types tab

Click the **Assign** and **Remove** buttons to change the role types a user role is assigned to.

Roles Types

Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions listed in the User Roles > **Access Rights** (page 366) tab and Machine Roles > **Access Rights** (page 368) tab. The number of role type licenses purchased displays in the System > **License Manager** (page 386) > Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

User Roles Types

Every user role must be assigned to at least one user role type. If a user role is assigned to more than one role type, access to a function is enabled if any one of the role types enables access to that function. Function access can be optionally limited further by user role or machine role. Examples of user role types include, but are not limited to:

- **VSA Admin** - Includes both master users and standard users.
- **End Users** - Provides limited access to selected functions in the VSA. Primarily intended for customers of service providers. Customers can logon to the VSA and print reports or look at tickets about their own organizations.
- **Service Desk Technician** - Can edit **Service Desk** tickets and run reports, but not configure service desks, support tables or service desk procedures.
- **Service Desk Admin** - Can do anything in **Service Desk**.
- Additional **SaaS** (page 564) user role types are defined and depend on the bundle purchased.

Machine Roles

System > User Security > Machine Roles

The **Machine Roles** (page 365) page creates and deletes machine roles. Machine roles determine what *machine users* see when they use **Portal Access** (page 67)—a version of **Live Connect** (page 344)—from a machine with an agent. The **Portal Access** window displays when a *machine user double-clicks the agent icon in the system tray of their managed machine*.

Note: The **User Roles** page determines what *VSA users* see when they use **Live Connect** from within the VSA.

Within the **Machine Roles** page you can select:

- **Members** (page 368) - Assign or remove machines for a machine role.
- **Access Rights** (page 368) - Select the access rights for a machine role. Access rights determine the functions a *machine user* can access.
- **Role Types** (page 368) - Assign or remove role types for a machine role. Currently there is only one machine role type provided and no access rights are restricted.

Note: The **Home** page seen by machine users when they first display the **Portal Access** window can be customized using **System > Customize > Live Connect** (page 398).

Note: See **Enabling Ticketing for Portal Access Users on Unsupported Browsers** (page 68).

Note: See the PDF quick start guide, **Live Connect**

(http://help.kaseya.com/webhelp/EN/VSA/7000000/EN_RCtools70.pdf#zoom=70&navpanes=0).

The Default Machine Role

A predefined **Default** machine role is provided when the VSA is installed. Newly created machine ID accounts are automatically assigned to the **Default** machine role when the account is created. If you create other machine roles, you can re-assign machine ID accounts to these other machine roles. You might want to do this if you want to limit machine user access to functions on the **Portal Access** page for different populations of machine users. Each machine ID account can only belong to a single machine role.

Middle Pane

You can perform the following actions in the middle pane of **Machines Roles**:

- **New** - Create a new machine role.
- **Copy Permissions** - Copy the access rights to the selected machine role from any other machine role.
- **Rename** - Rename the machine role.
- **Delete** - Delete the selected machine role. All machines must be removed from a machine role before you can delete it.

Members tab

The **Members** tab displays which machines belong to the machine role selected in the middle pane.

- Click the **Change Machine Role** button to change the machine role a machine is assigned to.
- Sort and filter the machines listed in the **Members** page.

Access Rights tab

The **Access Rights** tab in the System > **Machine Roles** page determines what functions *machine users* can perform on machines belonging to a selected machine role. For example, access rights can include whether or not a machine user has access to their own machine remotely from another machine.

A navigation tree provides access to each item and control on the **Live Connect** page.

- Click the or icons next to any item in the tree to display or hide child branches of that item.
 - A checked item means a machine role provides access to that item.
 - An unchecked item means a machine role does *not* have access to that item.
 - Click **Expand All** to expand the entire tree.
 - Click **Collapse All** to collapse the entire tree.
- Click **Set Role Access Rights** to change access rights for a machine role.
 - Checking or clearing any checkbox sets the same state for any child items.
 - Click **Enable All** to enable all items.
 - Click **Disable All** to disable all items.

Role Type tab

Note: In this release of Kaseya 2 there is only one role type, so all machines must use the **Basic Machine** role type.

- **Basic Machine** - Provides access to all **Portal Access** functions available to machine users.

Role Types

Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions

listed in the User Roles > [Access Rights](#) (page 366) tab and Machine Roles > [Access Rights](#) (page 368) tab. The number of role type licenses purchased displays in the System > [License Manager](#) (page 386) > Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

Machine Role Types

Every machine role must be assigned to a machine role type. *For the initial release of Kaseya 2, there is only one machine role type.* The machine role type determines the type of *machine-based-license* to apply to machines included in a machine role. For example, if you create a machine role called `StdMach` and assign `StdMach` to the machine role type called `Basic Machine`—and there are 150 machines in the `StdMach` machine role—then the System > [License Manager](#) (page 386) shows 150 of the total number of `Basic Machine` licenses used.

Scopes

System > User Security > Scopes

The [Scopes](#) (page 369) page defines *visibility* of certain types of user-defined data objects throughout the VSA. For example, a user could see some machine groups, but not be able to see other machine groups. Once a scope has made a data object visible to a user, the functions the user can perform on that data object are determined by user role. Scopes enables VSA users responsible for user security to create different scopes of data objects and assign them to different populations of users.

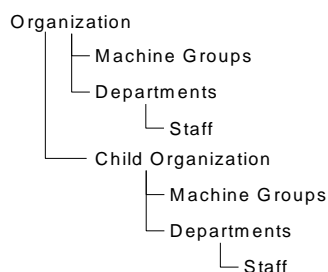
Note: A user logs on with both an assigned role (the functions they can perform) and an assigned scope (the data they can see). Membership in a role and membership in a scope are independent of each other.

Users can also be assigned to scopes using the System > [Users](#) (page 360) > Scopes tab.

Scope Data Objects

There are five types of data objects that can be assigned to scopes. Each are defined outside of scopes before being assigned to scopes.

- **Organizations** - An organization is typically a customer but not necessarily only customers. An organization record contains certain general information, such as its name and address, number of employees and website. An organization also defines a hierarchy of additional information, as illustrated below, representing all the machine groups and personnel within that organization. Organizations are defined using System > Orgs/Groups/Depts/Staff > [Manage](#) (page 372).



- **Machine Groups** - Machine groups are groups of managed machines within an organization. Machine Groups are defined using System > Orgs/Groups/Depts/Staff > Manage > Machine Groups.
- **Machines** - A managed machine is a computer with an agent installed on it. Each machine has to belong to a machine group. Machines are typically created using the Agents > [Deploy Agents](#) page.
- **Departments** - A department is a group of staff members within an organization. A staff member is not necessarily the same as a machine user. Departments and staff members are defined using System > Orgs/Groups/Depts/Staff > Manage > Departments.
- **Service Desk** - A service desk processes tickets using the [Service Desk](#) module. Service desks are defined using Service Desk > Desk Configuration > Desk Definition.

System

Scope Assignment

The parent-child relationships between data structures affect how scopes are maintained.

Implicit Assignment

Assigning any parent record to a scope *implicitly* assigns all child records to that same scope. For example, assigning an organization to a scope includes the following in that same scope:

- Child organizations.
- Machine groups of the organization and any child organizations.
- Machines of the machine groups in that organization and any child organizations.
- Departments in the organization and any child organizations.

Explicit Assignment

The only way to include a top level organization in a scope is to manually add it to that scope, because no parent record exists to include it. This is called explicit assignment. You can also explicitly assign a lower level object in scope, *but only if the lower level object is not already assigned implicitly to the scope through its parent*. For example, you could include a machine group explicitly, without adding the machine group's parent organization. You can also explicitly include individual machines and departments in a scope without including their parent records.

All in Scope

The **Scopes** function provides an **All in Scope** button, when appropriate. The button displays a window that lists all records in a particular Scope tab, regardless of whether records are assigned implicitly or explicitly.

Master Scope

See System > **Users** (page 360) for a discussion of the **Master** scope.

Middle Panel

You can perform the following actions in the middle pane of **Roles**:

- **New** - Create a new scope.
- **Rename** - Rename the scope.
- **Delete** - Delete the selected scope. All VSA users must be removed from a scope before you can delete it.

Scope Details

Each tab provides the following actions:

- **Assign** - Assigns access for a data structure to a scope.
- **Remove** - Removes access for a data structure from a scope.
- **All in Scope** - Displays only on the **Organizations**, **Machine Groups**, **Machines** and **Departments** tabs. Clicking the **All in Scope** button on a tab displays a new window listing all data structures of that tab type in the scope, whether defined explicitly or implicitly.

Sharing User-Owned Objects

Each user has the ability to create user-owned objects—such as filtered views, reports, procedures, or monitor sets. Typically these objects start out as private objects. As a private object no other user can see them or use them. These user-owned objects can be shared with other *user roles* or with individual *users*. In some cases, a **Master** role user can make a user-defined object public for all users. Share options can include the right to use an object, edit, export, delete, or share an object with additional users. Share rights are set by each individual object separately. You can elect to share a user-owned object with:

- Any user roles you are a member of, whether you are currently using that user role or not.
- Any individual users that are members of your current scope.

If share rights for an object are granted by both user role and individual user, share rights are added to one another.

Typically a **Share** button displays on any page or dialog that edits a user-owned object. Individual **Share** buttons sometimes display next to each user-owned object in a list.

Examples of user-owned objects in the VSA are:

- View Definitions
- Deploy Agent install packages
- Monitoring Dashlets
- Agent Procedures folders
- Service Desk Procedures folders
- Monitor Sets folders
- SNMP Sets folders
- Reports folders
- Report Sets folders
- **Service Desk** ticket named filters

Note: Folder trees have specialized rules about how folders are shared. See [Agent Procedures > Schedule/Create > Folder Rights](#) (page 108) in online user assistance for details.

Sharing Options

Kaseya 2 Share Options

- Adding a user or user role to the **Shared Pane** allows that user to use that object. No additional rights have to be assigned to the user or user role to use that object.
- Checking any *additional rights*—such as **Edit**, **Create**, **Delete**, **Rename**, or **Share**—when you *add* the user or user role, provides that user or user role with those additional rights. You have to remove the user or user role and re-add them to make changes to their additional rights.
- **Share** means the users or user roles can assign share rights.

Legacy Share Options

Certain functions in Kaseya 2 still set sharing rights using a legacy dialog as follows:

- Share rights are assigned *by object*. There are three sharing checkbox options. The first two checkboxes are *mutually exclusive* and determine what share rights are assigned. If neither of the first two checkboxes are checked, the shared object can only be seen by the users given share access, but the object cannot be used nor edited. The **Shared** and **Not Shared** list boxes and the third checkbox determine who can see the object.
 - **Allow other administrators to modify** - If checked, share rights to the object includes being able to use it, view its details and edit it.
 - **Other administrators may use but may not view or edit** - If checked, share rights to the object only allows using it.
 - **Make public (seen by all administrators)** - If checked, ensures that *all* current and future VSA users can see the object. If blank, only selected user roles and users can see the shared object. If blank, and new users or user roles are added later, you have to return to this dialog to enable them to see the specific object.

Logon Hours

[System](#) > [User Security](#) > [Logon Hours](#)

The **Logon Hours** page determines *when* users can logon to the VSA by specifying the weekdays and hours for each user role. Each day of the week can have different hours of operation set.

Note: See [VSA Logon Policies \(page 353\)](#) for a summary of functions affecting user logons.

Select user role

Select a **user role** ([page 333](#)) to display and maintain its logon hour settings.

No Hours Restrictions

If checked, users can logon to the VSA at any time and day of the week. Uncheck to enable all other settings.

Deny

Denies logon access for the entire weekday.

or allow between <12:00 am> and <12:00 am>

Specify the range of time logons are allowed. All times are in the Kaseya Server's time zone. For all day access, set start and end time to the same time.

User History

[System](#) > [User Security](#) > [User History](#)

The **User History** page displays a history, in date order, of every function used by a user. The history also displays any actions captured by the **System Log** ([page 389](#)) performed by the selected user. The system saves history data for each user for the number of days specified for the **System Log**.

Click [a user name](#) to display the log for that user.

Note: This log data does not appear in any reports.

Orgs/Groups/Depts/Staff

- **Manage** ([page 372](#)) - Create organizations, machine groups, departments and staff.
- **Set-up Types** ([page 376](#)) - Create organization types used to classify organizations.

Manage

[System](#) > [Orgs/Groups/Depts/Staff](#) > [Manage](#)

The **Manage** page defines the organizations you do business with. Typically an organization is a customer, but an organization could also be a business partner. Organizations are associated with **Scopes** ([page 369](#)), tickets and with desk definitions. Every managed machine, managed device and VSA user belongs to an organization.

Within an organization you can define:

- **General** ([page 373](#)) - General settings for the organization.
- **Machine Groups** ([page 374](#)) - Machine groups associated with this organization.
- **Departments** ([page 374](#)) - A unit of administrative responsibility within an organization.
- **Staff** ([page 375](#)) - Personnel assigned to a department.

- **Custom Fields** (page 376) - Assigns values to custom fields used to classify organizations.
- **Systems Management** (page 376) - Configures **Policy Management** policies for an organization using a setup wizard.

Manage - General tab

System > Orgs/Groups/Depts/Staff > Manage > General tab

Click **New** to display the **Add Organization** window, or click a row in the middle panel, then click **Edit** to display the **Change Organization** window. Enter the following attributes:

- **New/Convert** - Select **New Organization** if no other data source exists to convert from. If **Service Billing** is installed you can create a organization by **converting** (page 559) an existing customer record or vendor record.
- **ID** - The record identifier. Can only be changed using the **Rename** button.
- **Org Name** - The display name for the identifier.
- **Org Type** - The type of organization. See **Organization Types** (page 376).
- **Default Dept. Name** - The default department for the organization.
- **Default MachGroup Name** - The default machine group for the organization.
- **Org Web Site** - The organization's web site.
- **Number of Employees** - The number of employees in the organization.
- **Annual Revenue** - The annual revenue of the organization.
- **Preferred Method of Contact** - The organization's preferred method of contact: Phone, Email, Mail, Fax.
- **Parent Organization** - The parent organization of this organization. The parent organization must be previously defined to display in this drop-down list.
- **Primary Phone** - The primary phone of the organization.
- **Primary Email** - The primary email of the organization.
- **Primary Contact** - The primary contact for the organization. A contact is a **staff** (page 375) member of a department.
- The address of the organization:
 - **Country**
 - **Street**
 - **City**
 - **US State**
 - **Zip Code**
- **Map** - Clicking this hyperlink displays the location of the address in Google maps.

Three pre-defined organizations are provided:

- **myOrg** is the **organization** (page 559) of the service provider using the VSA. All other organizations in the VSA are second party organizations doing business with myOrg. The default name of myOrg, called My Organization, should be renamed to match the service provider's company or organization name. *This name displays at the top of various reports to brand the report.* Agents installed to internally managed machines can be assigned to this organization. *VSA user logons are typically associated with staff records in the myOrg organization.* myOrg cannot be assigned a parent organization.
- **Kserver** is the org assigned to agents installed on your Kaseya Server. This makes it easy to apply specialized settings to the Kaseya Server, which is typically maintained differently from other agent managed machines.
- **Unnamed** is the default organization to assign an agent. Maintaining multiple agent install packages in Agent > **Deploy Agents** (page 35), one for each organization, can be time consuming. Instead some server providers use a single agent package for the unnamed organization and perform all installs using this package. System > **Naming Policy** (page 358) can reassign new agents

System

to the correct organization.group ID automatically—the first time the agents check in—based on each managed machine’s IP or connection gateway. Agent > **Copy Settings** (page 55) may be used afterwards, to manually copy specific kinds of agent settings by **machine ID template** (page 557) to the type of machine revealed by the initial audit.

Manage - Machine Groups tab

System > Orgs/Groups/Depts/Staff > Manage > Machine Groups tab

Define the machine groups associated with this organization. Machines are always defined by machine group and machine groups are always defined by organization. You can define multi-level hierarchies of machine groups by identifying a parent machine group for a machine group.

Actions

- **New** - Adds a new machine group.
 - **Name** - The name of the machine group.
 - **Parent Group** - Parent machine group. Optional.
- **Change Machine Group ID** - Renames a selected machine group ID.
- **Move** - Moves all machines and sub-machine groups from a source machine group to a target machine group. The move can be to a target machine group in the same organization or a different organization. *The source machine group is deleted after the move.* Cannot be used on the last machine group in a source organization.

Note: If you want to re-create the same machine group with the same contents at the target location, create the machine group at the new location *before* the move, then select it when you perform the move.

- **Delete** - Deletes a selected machine group. A machine group must be empty of member machines to delete it. Machines can be moved to a different machine group using Agent > **Change Group** (page 55).
- **Agents** - Lists the member machines of a selected machine group.
- **Set Default** - Sets a selected machine group as the default machine group for an organization.

Manage - Departments tab

System > Orgs/Groups/Depts/Staff > Manage > Departments tab

Departments can be defined within an organization, customer record or vendor record. Example: IT, Sales or Accounting. All staff members are defined by the department they belong to. You can define multi-level hierarchies of departments by identifying a parent department for a department. You can reassign a staff member to any other department within the same organization, customer record, or vendor record.

Actions

- **New / Edit** - Adds a new department.
 - **Department Name** - The name of the department.
 - **Parent Department** - Parent department. Optional.
 - **Manager** - The manager of the department. Optional. The staff member record must be previously defined.
- **Move** - Moves all staff and sub-departments from a source department to a target department. The move can be to a target department in the same organization or a different organization. *The source department is deleted after the move.* Cannot be used on the last department in a source organization.

Note: If you want to re-create the same department with the same contents at the target location, create the new department at the new location *before* the move, then select it when you perform the move.

- **Change Department ID** - Renames the department ID of a selected department.
- **Delete** - Deletes a selected department. A department must be empty of staff members to delete it. Staff members can be moved using the **Staff** (page 375) tab.
- **Set Default** - Sets a selected department as the default department for an organization.
- **Delete** - Deletes a selected department. A department must be empty of staff members to delete it. Staff members can be moved using the **Staff** (page 375) tab.

Manage - Staff tab

System > Orgs/Groups/Depts/Staff > Manage > Staff tab

Create staff members within departments and maintain contact information for each staff member. Contacts and their phone numbers can be associated with tickets and with desk definitions. Staff member information can also be updated by Active Directory domain using Discovery > Domains > **Domain Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#10750.htm>).

Adding / Editing a Staff Record

- **Full Name** - The full name of a person within the organization.
- **Department** - The department the person is associated with. The department must be previously defined to display in this drop-down list.
- **Supervisor** - The person this staff member reports to. The Supervisor must be previously defined as a staff member in the same department.
- **Title** - The person's title in the organization.
- **Function** - The function the person performs in the organization.
- **Phone Number** - The person's direct phone number.
- **Email Address** - The person's email address.
- **User Name** - VSA user ID associated with this staff member. Required to **View All Tickets** and for Time Tracking.
- **View All Tickets** - If checked, the VSA user associated with this staff member can view all **Service Desk** tickets in his or her scope as well as tickets associated with this specific staff member record. If blank, this VSA user can only view **Service Desk** tickets associated with this specific staff member record.

Time Approval

A staff member record must be associated with a VSA user to approve timesheets and have visibility of timers.

- **Approve All Timesheets** - If checked, this staff member can approve any timesheet. This ensures all timesheets can be approved in a timely manner, if other approvers are temporarily unavailable.
- **Approval Pattern** - Specifies the approval pattern required to approve this staff member's timesheets. Approval patterns determine whether the staff member's supervisor, or the supervisor's supervisor, or both, are required to approve the staff member's timesheet.

Note: See Time Tracking configuration options.

Visibility of Service Desk Tickets by a Staff Member

If a VSA user name is associated with the staff member record of an organization, then that VSA user has visibility of tickets associated with that staff member record *even if the VSA user's scope does not allow it*. Any tickets created by that VSA user are automatically associated with their staff member

System

record and organization. This method primarily supports machine users using **Portal Access** (page 67) to create and manage their own tickets. Machine users expect to have access to all the tickets they create and to any tickets created on their behalf, but may have no scope privileges defined for them. If a scope does exist for a VSA user associated with a staff member, checking the checkbox called **View all tickets** in the **staff member** (page 375) record provides visibility of those additional tickets by scope.

Example: Dale is the main customer contact for the XYZ organization. He is provided a scope that allows him to see all tickets related to his organization, even tickets not created by him, so the **View all tickets** checkbox is enabled. Brandon from the XYZ organization contacts the service desk to submit a ticket as well. Initially it's unclear whether Brandon should have access to any other tickets beyond the tickets he himself creates, so the **View all tickets** is left unchecked. Later, if Dale okays greater access for Brandon, the service desk provider can assign a scope to Brandon and check the **View all tickets** checkbox.

Manage - Custom Fields tab

System > Orgs/Groups/Depts/Staff > Manage > Custom Fields tab

Assign values to the custom fields displayed on this tab. The values you assign are used to classify organizations. The titles of the custom fields displayed on this tab can be customized using Site Customization > **Org Custom Field Title** (page 396).

Manage - Systems Management tab

System > Orgs/Groups/Depts/Staff > Manage > Systems Management tab

The **Systems Management** tab provides a setup wizard. The setup wizard enables you to quickly *configure and apply machine management policies for a specific organization*. Once configured, these policies are assigned to each machine you manage on behalf of that organization. Policies govern many different aspects of machine management:

- Audit scheduling
- Monitoring
- Alerts
- Patch Management
- Routine machine maintenance using agent procedures

With policies you no longer have to manage each machine individually. You only have to assign or change the policy. A policy assignment or a change within an assigned policy is propagated within 30 minutes to all member machines without you having to schedule anything. Once applied, you can quickly determine whether managed machines are in compliance or out of compliance with their assigned policies. Compliance tracking by individual policy provides you with the information you need to deliver IT services consistently throughout the organizations you manage.

Note: See the **Standard Solution Package** for a detailed explanation of each option in the setup wizard (<http://help.kaseya.com/webhelp/EN/SSP/7000000/index.asp#11220.htm>).

Set-up Types

System > Orgs/Groups/Depts/Staff > Set-up Types

The **Set-up Types** page defines records that classify your organizations. For example, you might define an organization as a **division** within your enterprise, or classify organizations regionally or by revenue. Alternatively, you might classify organizations as a **prospect**, **preferred customer**, or **business partner**. It depends on your business requirements.

Service Desk

Set-up Types can be optionally used to automatically **associate a ticket with a policy** (<http://help.kaseya.com/webhelp/EN/KSD/7000000/index.asp#6210.htm>) in the **Service Desk** module.

General tab

Click **New** to display the **Add Organization Types** window, or click a row in the *middle* panel, then click **Edit** to display the **Change Organization Types** window. Enter the following attributes:

- **ID** - The record identifier. Can't be changed once you save it.
- **Description** - A brief description of this ID.

Server Management

Request Support

System > Server Management > Request Support

The **Request Support** page provides multiple ways of contacting Kaseya support.

- **Support Web Site** - Find answers to common questions using the Kaseya Support website at <http://www.kaseya.com/support.aspx> (<http://www.kaseya.com/support.aspx>). This website provides links to the **Kaseya Forum** and to the **Kaseya Knowledge Base**. The Kaseya Forum hosts an interactive community of Kaseya users that discuss a wide variety of issues and solutions on a daily basis. Subscribe to the forum to get new posts of interest directly emailed to you as new information appears. The Kaseya Knowledge Base provides technical information about installation and usage of the Kaseya IT Automation Framework.
- **Allow Kaseya support to access your system** - Kaseya support engineers can solve problems with your system quickly and efficiently when they can directly access your Kaseya Server. Click **Create** to create a kaseyasupport master user account on your system. The Kaseya Support engineer can use our system to log into your system and help solve any problems.

Note: We realize the security implications of providing access to your Kaseya Server. To protect this logon, your system creates a secure logon. No one has access to the password, not even the Kaseya support engineer. The password gets changed every time you click this button.

- **Click here to manage support request** - The **Kaseya Help Desk** (<https://helpdesk.kaseya.com/home>) provides a single point of contact for managing your Kaseya support tickets, accessing the knowledge base, and participating in the user forum.

Your Information

Typically Kaseya support needs some basic information about your system to begin providing support. Your user name, email address, Customer ID, and system URL are provided for your convenience.

Configure

System > Server Management > Configure

The **Configure** page manages the configuration of your Kaseya Server and related services. Related topics include:

- **Change Reporting Configuration** ([page 382](#))
- **Indexing the Audit Results Table** ([page 384](#))
- **Default Settings** ([page 384](#))
- **Kaseya Server Setup** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/Install>)

System

Version, Patch Level, and Licensing

- **Version Number** - Shows the version number of the system.
- **Installed Patch Level** – Shows the installed patch level of the system.
- **Available Patch Level** – Shows the highest patch level available to install.
- **Check for Latest Patches** – Click this link to see the **latest patch release notes** (<http://help.kaseya.com/webhelp/EN/RN/index.asp#PatchReleaseNotes.htm>) and instructions on how to update your system with the latest patches.
- **Warn if the server cannot get data from <http://vsaupdate.kaseya.net>** - Check this box to display a warning if your VSA cannot connect to <http://vsaupdate.kaseya.net> to fetch the latest PCI ID list used by audit. Your VSA attempts to automatically fetch this information from <http://vsaupdate.kaseya.net>. Verify that the server can connect outbound to port 80 on <http://vsaupdate.kaseya.net> and that its responses are not blocked by your firewall.
- **Warn when the license reaches the maximum number of seats** - Check this box to display a warning when the number of machine ID accounts reaches the maximum for your VSA.

Reapply Schema / Defrag Database

Warning: Do not use the Microsoft SQL tuning advisor against the schema. It adds keys that conflict with the smooth operation of the system.

- Click **Reapply Schema** to re-install and validate the last database schema that was downloaded using **Check for Update**. Reapply schema is a safe operation that users can run in an attempt to resolve a variety of problems. Reapply schema:
 - Sets default values and runs basic consistency checks on the database.
 - Rebuilds all pre-defined Kaseya procedures.
 - Rebuilds all pre-defined Kaseya procedure samples.
 - Reschedules default backend processing procedures for the Kaseya Server.
 - Only runs automatically when the Kaseya Server is updated or an add-on is installed. This is all completed without the risk of losing any agent data. This is a good self healing routine to run if you observe:
 - Procedures failing in the **IF** condition or in specific steps.
 - Pending alerts not being processed within a two minute interval. You can monitor this using the System > **Statistics** (*page 389*) page. This might indicate a problem with backend processing procedures.
- Click **Defrag Database** to defragment the physical files on your disk arrays. Fragmented SQL Server data files can slow I/O access.

Sample Data

- **Reload sample scripts with every update and database maintenance cycle** - Check to reload sample agent procedures.
- **Reload sample event sets with every update and database maintenance cycle** - Check to reload sample event sets.
- **Reload sample monitor sets with every update and database maintenance cycle** - Check to reload sample monitor sets.

HTTPS

- **Automatically redirect to https at logon page (except when accessing via localhost)** - If checked, ensures all users logging into the VSA remotely use the secure HTTPS protocol.

API

- **Enable VSA API Web Service** - Check to enable the **VSA API Web Service** (*page 470*).

Patch Management

- **Enable Invalid Patch Location Notifications** - Microsoft sometimes prepares patches that do not allow the File Source function to download patches successfully. If checked, this option notifies Kaseya that an "invalid patch location" exists for a patch required by any of the managed machines on your system. Notification alerts Kaseya to prepare a valid patch location manually and send it out as an updated patch location override for all customers to use. If blank, no notification is sent to Kaseya. You will still receive updated patch location overrides prepared in response to notifications reported by *other* customers, regardless of this setting.

Note: Notification sends no customer-specific or machine-specific information to Kaseya.

Ticketing

- **Allow non-authenticated users to download attachments from ticket notifications** - If checked, links to attachments embedded in the notes of tickets can be opened in outbound emails without requiring the user to authentic themselves to the VSA. For security reasons, enabling this option is not recommended.

Database Backups

- **Run database backup / maintenance every <N> Days @ <Time>** - The Kaseya Server automatically backs up and maintains the MS-SQL database and transaction log for you. Click **Set Period** to set the frequency and time selected. If your Kaseya Server is shut down at the scheduled backup time, the backup will occur the next time the Kaseya Server goes online. You can enter zero to disable recurring backups.
- **Backup folder on KServer** - Set the directory path to store database backups in. The default directory path is typically C:\Kaseya\UserProfiles\@dbBackup. Click **Change** to confirm changes to the directory path. Click **Default** to reset the directory path to its default.

Note: Database backups older than three times the backup and maintenance period are discarded automatically to prevent your disk drive from filling up. For example, if the backup occurs every 7 days, any backup older than 21 days is deleted.

- **Change DB** - Connect your Kaseya Server to a database on a different machine.
 1. Backup your existing `ksubscribers` database by clicking **Backup Now** in the System > Configure page.
 2. Copy the database backup file to the database server you wish to connect to.
 3. Use SQL Server Management Studio (SSMS) on the new database server to restore the `ksubscribers` database. Right click Databases > Restore Databases...
 4. Verify the restored `ksubscribers` database is set to **mixed mode authentication**.
 - ✓ In SQL Server Management Studio (SSMS) right click the restored `ksubscribers` database and select **Properties**.
 - ✓ Click the **Security** tab.
 - ✓ Under authentication, select **SQL Server and Windows**.
 - ✓ Click **OK**.
 5. **Verify CLR is enabled in the new database server** (<https://helpdesk.kaseya.com/entries/33743166>).
 6. Verify your Kaseya Server is on the same LAN as your new database server and **port 1433** is open on the database server.
 7. Click the **Change DB** button.
 8. Enter the database location using one of the following formats:
 - ✓ computer name
 - ✓ computer name\instance name

System

✓ IP address

9. Enter a database logon name. The default logon name is **sa**.

Note: This logon is only used to configure the database. The system creates its own database logon to use going forward.

10. Enter the password associated with this logon name.

11. Click **Apply**. The system then connects to the remote database and configures it.

- **Backup Now** - Initiate a full database backup now. Use this function *before* you shut down or move your Kaseya Server, to ensure you have the latest Kaseya Server data saved to a backup. The backup will be scheduled to run within the next 2 minutes.
- **Restore** - Click to restore the Kaseya Server's database from a backup file. A file browser displays a list of Kaseya Server database backup files you can restore from.

Note: After a restore of a 5.1 database, the SSRS URL will be invalid and need to be reset. After a restore of a 6.x database the SSRS URL may be invalid and need to be reset.

Archive

Archiving of agent logs are enabled, by log and machine ID, using Agent > **Log History** (page 32).

- **Archive and purge logs every day at <time>** - Specifies the time of day log files are archived and purged.
- **Set Period** - Click to confirm changing the time log files are purged and archived.
- **Log file archive path** - The file location where the archive files are stored.

Note: Monitoring data log archives—identified on the Agent > **Log History** (page 32) page—are stored in the <KaseyaRoot>\UserProfiles\@dbBackup directory. This is to improve performance on systems where the database is on a different server. All other agent log archives are stored in the directory specified by the System > **Configure** (page 377) > **Log file archive path** field.

- **Change** - Click to confirm changing the archive file location. A procedure runs to move any existing archive files in the old file location to the new file location.
- **Default** - Resets the log file archive path to the default location on the Kaseya Server. A procedure runs to move any existing archive files in the old file location to the new file location.

Server Status

- **KServer Log** - Displays the last 300 kbytes of the Kaseya Server's log file. The entire log file is up to 5 Mbytes in size and is located at xx\KServer\KServer.log where xx is the parent directory of the VSA web directory.
- **Live Connect KServer** - An agent is automatically installed on the Kaseya Server. You can click the check-in icon for this agent to initiate a **Live Connect** (page 344) session with the Kaseya Server.
- **Stop KServer** - Shows the current status of the Kaseya Server: **running** or **stopped**. The Kaseya Server can be stopped by clicking **Stop Service**.
- **Enable alarm generation** - Uncheck to prevent generating unnecessary alarms. This can occur if you stop the Kaseya Server, disconnect from the internet, or maintain the system. Otherwise leave this box checked.
- **Restart MsgSys** - Restarts the MessageSys service. This service is the application server that manages requests from VSA application users.
- **Enable logging of procedure errors marked "Continue procedure if step fail"** - If checked, failed steps in procedures are logged. If blank, failed steps in procedures are *not* logged.
- **Enable logging of successful child script execution in agent procedure log** - If unchecked, child script success entries are not included in the **agent procedure log** (page 31). This can reduce the size of

the agent procedure log tremendously. It takes up to 5 minutes for the KServer to read this setting change.

- **Enable auto close of alarms and tickets** - If checked, open alarms and tickets for monitor sets and offline alerts are automatically close when the alert condition no longer exists. Offline alerts are configured using Agent Status alerts. Checking this checkbox requires the **Enable alarm generation** checkbox be checked to auto close alarms and tickets.

Server Settings

- **Select time format** - Click the appropriate radio button to select how time data is displayed. The default is AM/PM format. Both these display formats are compatible with Microsoft Excel.
 - AM/PM format - 9:55:50 pm 9-Apr-07
 - 24-hour format - 21:55:50 9-Apr-07

Note: Time offset is set in System > Preferences (page 353). The date format is set in System > Local Settings (page 397).

- **Change external name / IP address of Server** - Shows the current external name or IP address of the Kaseya Server. This is the address the agents of managed machines access for check-in purposes. The address can be changed by entering a new address or host name in the field and pressing **Change Name/IP**.

Note: Do *not* use a computer name for your Kaseya Server. The agent uses standard WinSock calls to resolve a IP address from a fully qualified host name. Resolving an IP address from a computer name requires NETBIOS, which may or may not be enabled on each computer. NETBIOS is an optional last choice that the Windows will attempt to use to resolve a name. Therefore, only fully qualified names or IP addresses are supported.

- **Set URL to MS-SQL Reporting Services Engine** - Click the **Change Reporting Config...** (page 382) button to specify the URL used by the VSA to connect to Reporting Services. You can also specify the credential used to access Reporting Services and customize the URL displayed in the header of all VSA reports.
- **Specify port Agents check into Server with** - Entering a different port and clicking **Change Port** switches the port the Kaseya Server uses *immediately*.

Warning: Before you change the Kaseya Server port ensure that all agents are set to use the new port with their primary or secondary Kaseya Server. Agent check-ins are configured using Agent > Check-in Control (page 61).

- **KServer ID** - ID used to bind agents to the Kaseya Server - The unique identifier for this Kaseya Server. Bound agents cannot check-in successfully unless the unique Kaseya Server ID they are bound to using the Agent > **Check-in Control** (page 61) page matches the unique ID assigned to the Kaseya Server using the System > **Configure** (page 377) > **Change ID** option. Prevents IP address spoofing from redirecting agent check-ins. Only change the Kaseya Server ID if you are installing a fresh VSA and wish to duplicate the ID of an existing Kaseya Server with agents already bound to it.

Version Information

Displays the following information about your VSA configuration.

- OS Version
- IIS Version
- Kaseya Server Version
- SQL Version

System

- Database Location
- Agent On Kaseya Server

References

- **Release Notes** - Click **Release Notes** to display a list of all changes and enhancements made to the VSA, for all versions of the software.
- **Show License** - Click **Show License** to display the current license agreement to use the VSA.

Change Reporting Configuration

System > Server Management > Configure (page 377) > Change Reporting Config...

The **Change Reporting Configuration** dialog selects the type of reporting server used to run reports.

- A built-in, proprietary report server is provided that requires no additional configuration.
- If instead, a SQL Server Reporting Services (SSRS) is preferred, you can configure the VSA connection to the SSRS instance used to generate VSA reports. The SSRS may be installed locally or remotely from the Kaseya Server and locally or remotely from the SQL Server instance hosting the `ksubscribers` database.

Actions

- **Edit** - Edits the reporting server configuration.
- **Test** - Tests that reporting server configuration is working.
- **Run Registration** - This button is used by developers to register newly created **data sets** (page 166) for customizable reports, instead of running **Reapply Schema** for the entire VSA.

Options

- **Use Kaseya Reporting** - If checked, a built-in, proprietary report server is used to run reports. Intended for smaller implementations of the VSA. This report server is used by default for new installs of the VSA. If blank, an SSRS report service is used to run reports. SSRS is intended for larger implementations. If blank, you must provide a **Host Name** URL to a SQL Server Reporting Services instance to run reports.
- **Reporting Timeout (Min)** - Sets the time to wait for a report to complete publishing.
- **Host Name** - The URL used by the VSA to connect to a SQL Server Reporting Services instance. Mandatory to run reports. The VSA typically uses one of the following URL patterns to connect to a SQL Server Reporting Services instance. Specifying the appropriate URL is mandatory to run reports.

Note: - See the **Kaseya Server Setup**

(<http://help.kaseya.com/webhelp/EN/VSA/7000000/install/index.asp#home.htm>) for a visual walkthrough of the steps required to configure an SSRS reporting server.

SQL on the same box as VSA

```
http://localhost/ReportServer (most common)
http://localhost/ReportServer$SQLEXPRESS
http://localhost/ReportServer$<SQLINSTANCENAME> (2005)
http://localhost/ReportServer_<SQLINSTANCENAME> (2008)
http://localhost:<PORTNUMBER>/ReportServer$<SQLINSTANCENAME> (2005)
http://localhost:<PORTNUMBER>/ReportServer_<SQLINSTANCENAME> (2008)
```

SQL box separate from VSA

```
http(s)://<SQLSERVERNAME>/ReportServer (most common)
http(s)://<SQLSERVERNAME>/ReportServer$SQLEXPRESS
http(s)://<SQLSERVERNAME>/ReportServer$<SQLINSTANCENAME> (2005)
http(s)://<SQLSERVERNAME>/ReportServer_<SQLINSTANCENAME> (2008)
```

http(s)://<SQLSERVERNAME>:<PORTNUMBER>/ReportServer\$<SQLINSTANCENAME> (2005)
 http(s)://<SQLSERVERNAME>:<PORTNUMBER>/ReportServer_<SQLINSTANCENAME> (2008)

- **User Name** - The user name used to access the Reporting Services instance when running reports. Applies to some configurations. See the **User Name** section below for more details.
- **Logo** - The URL of the image displayed in the header of reports. Applies to some configurations. By default, VSA report headers display the image specified by the System > Site Customization > **Site Header** (page 394). Changing the value in the System > Configure > **Change Reporting Config...** (page 382) > **Logo** field overrides this default, changing the URL *for report headers only*. Changing the URL in the Change Reporting Config... > **Logo** field does not affect the display of the **Site Header** image. If a logo does not display in SSRS reports it may be due to either of the following conditions:
 - The SSRS is installed on the same machine as the Kaseya Server. SSRS is unable to retrieve the logo because of firewall issues. Change the URL to `localhost` from the externally available URL/IP address.
 - The VSA has been configured using a self-signed SSL certificate. Change the protocol from `https` to `http`.
- **Report URL Base** - Overrides the URL used for CURL reports. For most reports the *external* VSA URL is used to generate reports but, an issue called "router loopback" can occur with CURL reports. Enter a different URL from the external VSA URL to avoid this issue. Defaults to `http://localhost:80/`
- **Concurrent Reports** - Sets the number of reports that can be published simultaneously. Concurrent reports greater than this number are queued.
- **Keep All Reports** - If No, **Number of Days** determines how long reports are kept. If Yes, all reports are kept and **Number of Days** setting is not applicable.
- **Keep Number of Days** - Sets the number of days to keep a report after its creation date. Must be at least 30 days.

Note: Only deletes reports *created after the Number of Days value is enabled*. Reports can be manually deleted from the `<Kaseya_Installation_Directory>\WebPages\DataReports` directory.

User Name

You can provide all VSA users with a credential that lets them run SSRS reports. This eliminates the need to maintain access rights for each VSA user requiring access to the SSRS. This applies in particular to VSA users in a workgroup instead of a domain, who don't have a centralized method of authentication such as Active Directory to manage access rights to the SSRS.

Credentials are specified in three locations:

- User Accounts in the system hosting the SSRS.
- SSRS Report Manager.
- VSA > System > Configure > Change URL... > User Name

This procedure creates a dedicated user—in this example, `KaseyaReport`—in the system hosting the SSRS. The SSRS **Report Manager** is used to give the `KaseyaReport` user access to running reports in the SSRS. Finally, the `KaseyaReport` credential is registered in the System > Configure > Change URL... > User Name fields. From that point forward the VSA uses that credential to access the SSRS every time a VSA user runs a report.

1. On the system hosting the SSRS, add a `KaseyaReport` user using the **Microsoft Management Console**. Using the console enables you to set the checkboxes below for the new user.
 - Give the user a strong password.
 - Uncheck the **User must change password at next logon** field.
 - Check the **User cannot change password** and **Password never expires** fields.

System

2. Apply appropriate permissions to the new user for your environment.
3. On the system hosting the SSRS, open a browser and type in the URL for **Report Manager**, for example, `http://localhost/Reports`, using the **Administrator** account.
4. Click **Site Settings** at the top right hand corner.
5. Click **Security** in the left hand sidebar.
6. Click **New Role Assignment** along the menu bar.
7. Enter the username that was created in step 1 in the **Group or user name** field, for example, `KaseyaReport`.
8. Select **System User** checkbox.
9. Click **Add**.
10. In the VSA, display the System > Server Management > **Configure** page. Click on the **Change URL** button to open the dialog.
11. Click on the **Edit** button at the top of the page.
12. Enter the credential you defined in step 1 and make sure the **Specify Account** checkbox is checked. This means SSRS will use the credential you entered. If the user, for example `KaseyaReport`, is not a domain user you can leave the **Domain** field blank.
13. Click **Save** and then click on the **Test** button to test the changes.

Indexing the Audit Results Table

Note: The following "one time" configuration task applies only if a dialog recommends indexing of the Audit Results table. The dialog only displays, if applicable, when a master user logs on to the VSA.

The response time of the Kaseya Server database can be improved by indexing the audit results table. **Depending on the number of records in this table, this process could take 1 to 4 hours to complete. The Kaseya Server should be shut down during this process to prevent the possibility of losing audit data.**

1. Click the **Stop Kserver** button on the System > **Configure** (page 377) page.
2. In SQL Server Management Studio:
 - a. Open a new query window and ensure `ksubscribers` is the selected database.
 - b. Run the following stored procedure: `Exec spCreateAuditRsItAppsPK`
This procedure might run 1 to 4 hours or longer, depending on the number of records in the table and the speed of the SQL Server.
3. Click the **Start Kserver** button on the System > **Configure** (page 377) page.

Note: Creating indexes manually or through the SQL tuning advisor on the `ksubscribers` database can cause errors during Reapply-Schema and when upgrading to new versions of Kaseya and is strongly discouraged.

Default Settings

System > Server Management > Default Settings

The **Default Settings** page specifies default settings for server management and a file upload whitelist.

Default Settings tab

- **Default value for Time on Schedule** - Sets the default time to use for scheduling, using either **agent time scheduling** (page 547) or server time scheduling. Applies only to schedulers that support agent time scheduling.

- **Discovery - Domain Watch policies "Include new Computers/Contacts" include moved objects** - If a policy is applied to an OU/Container that has "Include New Computers" or Include new Contacts" checked, and:
 - This option is Y, then the policy is applied to computers or contacts moved into the OU/Container.
 - This option is N, then the policy is not applied to computers or contacts moved into the OU/Container.
 - **Discovery - Staff record "View All Tickets" enabled** - If checked, the **View All Tickets** (page 375) checkbox is checked when the staff member record is created.
 - **Discovery - Staff record Department name assignment scheme**
 - **Assign based on Active Directory OU Name** - A department is created for the new staff record based on the OU/Container name.
 - **Assign based on Active Directory Department property** - A department is created for the new staff record based on the department name specified for the user in Active Directory.
 - **Discovery - Staff record Staff name assignment scheme**
 - **Assign based on Active Directory Display name. If empty, use First name plus Last name**
 - **Assign based on Active Directory User logon name**
 - **Assign based on Active Directory First name plus Last name**
 - **LAN Cache - Use auto-generated administrator credentials** - If yes, then credentials are automatically created for you when you create a LAN Cache using the Agent > Configure Agent > **LAN Cache** (page 69) > Add LAN Cache dialog. If no, this same dialog provides the option of manually specifying existing credentials for the LAN Cache you create.
 - **Require email address at logon** - If yes and a user does not already have an email address specified, requires the user to enter an email address as soon as the user logs on. If no, an email address is optional.
 - **Require email address for user name** - If yes, a user name record must have an email address. If no, an email address is optional.
 - **Show organizations in views with one machine group** - Controls the display of the **Machine Group** dropdown filter list at the top of every agent page. If Y, the **Machine Group** drop-down displays every organization and every machine group as separate items. If N, organizations are not shown as separate items in the list *for organizations with one machine group only*.
- Note:** If you are using the Ticketing module and associating tickets by organization, then this option should be set to N.
- **Use domain short name in the construction of user passwords** - If legacy AD logons were created using the **View AD Users** page in VSA 6.2 or earlier and these legacy AD logons continue to be used, then set to Yes. This enables user passwords for existing legacy AD logons to continue to be recognized. Whenever a password for an existing AD logon is reset, a newer hashing algorithm is used, based on fully qualified domain names. If legacy AD logons using the **View AD Users** page were never implemented prior to 6.3, then set this option to No.

Attachment Upload Whitelist tab

The **Attachment Upload Whitelist** tab controls the types of attachments that can be uploaded to the various **rich text editors** (page 140) used throughout the VSA framework. A default set of file types is specified. Default file types can be deleted but not modified. Users can set the list back to only the default list of file types. Only master role users have access to this new tab.

Service Desk and **Ticketing** tickets created by inbound email only accept attachments with extensions allowed by this tab. If an attachment is not accepted during inbound email processing, a message is inserted into the description of the ticket to notify the user that the attachment was excluded and lists

System

the supported file extensions.

License Manager

[System](#) > [Server Management](#) > [License Manager](#)

The [License Manager](#) page allocates machine licenses by org ID or group ID. This page also displays the number of user licenses purchased for each role type. If necessary, you can kill user sessions from the page to enable other users to logon.

Types of licenses managed include:

- Agent licenses - applies to machines by organization, group or group ID
- Role type licenses - applies to VSA users or machines by role type

Add-on module licenses only display if you have purchased and installed those add-on modules.

Agent License Counts

The following events affect agent license counts:

- An "unused" agent license is changed to "used" if a machine ID account is created and the agent installed.
- If the agent is deleted but not the account, the agent license is still considered "used".
- If the account is deleted, regardless of what happens to the agent, the agent license goes back to "unused".
- If an account is created, but the agent is not yet installed the first time, the account is called a [machine ID template](#) (page 557). Machine ID template accounts are not counted as "used" until you install the agent.

General tab

The [General](#) tab displays the products you have purchased.

Update Code...

Click the [Update Code...](#) to enter a new license code or reapply your existing license code.

Show License

Click [Show License](#) to display the current license agreement to use the VSA.

(Header Information)

Displays the following information about your VSA configuration.

- [Kaseya Managed Services Edition](#) - The version number of the Kaseya Server.
- [License Code](#) - The current license code for this Kaseya Server.
- [Expiration Date](#) - The current expiration date for running the system "as is" with the current license code.
- [Maintenance Expiration Date](#) - The current expiration date of maintenance services, including upgrades and access to tech support.

Product Name Table

Displays the following information about your add-on modules.

- [Product Name](#) - The version number of the Kaseya Server.
- [Version](#) - The version number of the product.
- [Status](#) - The status of the product: `Installed`.
- [Latest Hotfix Level](#) - The latest hotfix level for the add-on module.
- [Usage Type](#) - The level of functionality enabled for the product. Applies across all role types. See Service Desk Licensing.

Licenses tab

The **Licenses** tab displays the number of agent-based licenses for each product you have purchased. You can allocate portions of the total number of agent licenses you have purchased for a product to specific organization and machine groups.

(License Type Table)

The license type table displays the following:

- **License Type** - Lists each product you have purchased that requires an agent-based license. This can include:
 - Agents - VSA agents
 - KBU - Workstation clients
 - KBU - Servers clients
 - KES - Endpoint Security clients.
 - KDPM - Desktop Management clients.
- **Used** - The current number of managed machines that have this product installed.
- **Max** - The maximum number of managed machines that can install this product

Change License Allocations

The total number of licenses available can be allocated to a specific organization, group or sub-group ID. Select any organization, group or sub-group in the allocation table, then click the **Change License Allocations** button.

(Allocation Table)

The allocation table displays the following:

- **Organization/Machine Group** - Lists both organizations and groups within organization in a single column. You select any row to allocate agent licenses to that row.
- **Type** - Org or Group. Machine groups can include machine sub-groups.
- **Agents Used** - The current number of managed machines that have this product installed in this organization or machine group.
- **Agents Max** - The maximum number of managed machines that can install this product in this organization or machine group.

Role Types tab

The **Role Types** tab displays the license counts you've purchased for each role type in your VSA. Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions listed in the User Roles > **Access Rights** (page 366) tab and Machine Roles > **Access Rights** (page 368) tab. The number of role type licenses purchased displays in the System > **License Manager** (page 386) > Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

- **RoleType** - The name of the roletype.
- **Description** - The description of the roletype.
- **Max Named Licenses** - The maximum number of users licensed for this roletype.
- **Max Concurrent Licenses** - The maximum number of current users licensed for this roletype.

View Sessions

Click a role type, then click **View Sessions** to display a list of current VSA user sessions using that role type. You can select one or more sessions and click **Log Off Selected Sessions** to end those sessions. Use this feature to log off unnecessary sessions if a user is unable to logon because a roletype maximum of *concurrent* sessions has been reached.

Import Center

System > Server Management > Import Center

The **Import Center** page imports and exports automation solutions—user-defined data structures that can be applied to multiple agents—into and out of the VSA. This enables you to migrate automation solutions between VSAs, or import automation solutions from other solution providers. Import/export types of automation solutions include:

- Packages
- Agent Procedures - Includes the option of exporting and importing folders of agent procedures. Check the **Show Only Folders** checkbox at the top of the **New Export** dialog to select a *folder* of agent procedures to export.
- Agent Templates
- Event Sets
- Service Desk Holiday
- Monitor Sets
- Monitor SNMP Sets
- Patch Policies
- Policy
- Reports
- Report Data Part
- Report Template
- Service Desk Tickets
- Service Desk Definitions
- Service Desk Message Templates
- Views

You can import or export multiple items of multiple types using a single XML. For example, you may want to import a set of agent procedures and monitor sets that are both used together for form a single automation solution.

Imports tab

Use this tab to import an automation solution XML into your VSA.

- **New Import** - Select an XML file to import, then click the **Process** button.
- **View Import Details** - Displays a history of the import.

The paging displays a log of the files you have imported.

Exports tab

Use this tab to export an automation solution XML into your VSA.

- **New Export**
 1. Select the type of automation solution to export.
 2. Select one or more items of that type to export.
 3. **Click the Continue button to add another type of automation solution.**
 4. Click the **Export** button to export. A single XML file is created that is still stored on the Kaseya Server.
 5. Click the hyperlink for the newly exported file that displays in the table grid of the Exports page.
 6. Confirm saving the file to your local machine.
- **View Export Details** - Displays a history of the export.

System Log

[System](#) > [Server Management](#) > [System Log](#)



The **System Log** page logs events that cannot be tracked by machine ID, for a specified time period. *This log captures events not contained in any of the agent logs.* Examples include:

- Deleting machine IDs
- Failed and successful logon attempts
- Successful Kaseya Remote Control sessions
- Starting/stopping of the Kaseya Server
- Deleting trouble tickets assigned to a group (not a machine)
- Scheduling reports

Save History to N Days

Click **Apply** to save system log events for the specified number of days.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Search

The search function acts as a filter on the **Description** field. Enter a set of words to search for and click the **Search** button. Only rows matching the search criteria are listed. Use % or * as a wild card. Use the underscore character (_) as a single character placeholder. Text is case insensitive.

Note: This log data does not appear in any reports.

Statistics

[System](#) > [Server Management](#) > [Statistics](#)

- Related information is provided using [Reports](#) > [Network Statistics](#) (page 181).

The **Statistics** page displays various statistics to provide an indication that the Kaseya Server is running optimally. The statistics shown are not affected by the **machine ID/group ID filter** (page 556) setting.

Agents currently online

Number of agents currently checking into the system.

Total Licenses Used

Number of agent licenses used.

Total Template Accounts

Number of **machine ID templates** (page 557) defined.

Total Machine IDs

Number of machine IDs defined on the Kaseya Server, whether their agents have ever checked in or not. *Total Licenses Used + Total Template Accounts = Total Machine IDs.*

KServer CPU usage

the last 5 minutes: x%
long term average: x%

System

Total System CPU usage

the last 5 minutes: x%
long term average: x%

Remote Control Sessions

The number of remote control sessions relayed through the Kaseya Server that are currently active.

Pending Alerts

Alerts are processed by the background task every two minutes. This number shows how many alerts are backed up waiting to be processed by your system. If more than 0 alerts are pending, a button appears labeled **Clear Alerts** appears. Click this button to clear out all pending alerts.

Pending Patch Scan Results

The number of machines that currently have patch scan results that have been completed but not yet processed. If a Kaseya Server has a lot of patch scans that happen in a short period of time, the actual results of those scans might not appear for some time. The count is a measure of that backlog of processing.

Database Location

Displays the location of the database.

Database Size

Total size of your database. Typical systems consume about 1 to 2 MB of database size per machine ID.

Database File Path

Full path to the database on the database server machine.

Kaseya File Path

Full path on the Kaseya Server to the location of its system files.

Statistics Collected

- **Active connections** - Number of managed machines that currently have active connections to the Kaseya Server.
- **New connections in last 10 seconds** - Number of new TCP/IP connections accepted by the Kaseya Server. Agents using a connection established during a prior check-in do not contribute to this count.
- **Checkin message queue length** - Number of check-in messages waiting for processing by the Kaseya Server.
- **Command message queue length** - Number of messages, other than check-in, waiting for processing by the Kaseya Server.
- **Bandwidth - received bytes/sec** - Bytes per second input into the Kaseya Server agent port.
- **Bandwidth - sent bytes/sec** - Bytes per second output from the Kaseya Server agent port.
- **Database CPU utilization** - This number indicates the percentage of CPU utilization by the database server at the time specified. Excessively high values for prolonged periods may be an indication that this server is underpowered or could benefit from additional RAM.
- **Total connections processed since KServer start** - This number indicates the total agent connections processed by the Kaseya Server since the service last started.
- **Event log entries received in last minute** - The number of event log entries received in the last minute for the entire system.
- **Event log entries received in last five minutes** - The number of event log entries received in the last five minutes for the entire system.

- **Event log entries received in last hour** - The number of event log entries received in the last hour for the entire system.

Top procedures run in the last hour

This table lists the procedures that have run and completed execution on all online machines in the last hour, with the greatest frequency listed first.

Top procedures pending (online machines only)

This table lists the procedures waiting to execute on all online machines, with the greatest frequency listed first.

Logon Policy

System > Server Management > Logon Policy

The **Logon Policy** page sets logon policies that apply to all VSA users. Logon policies prevent a brute force break-in to the system. By limiting the successive number of bad logon attempts and disabling rogue accounts for a set amount of time, you can prevent unauthorized access achieved by repeatedly entering random passwords.

Note: See [VSA Logon Policies \(page 353\)](#) for a summary of functions affecting user logons.

Specify the bad logon attempt policy

- **Number of consecutive failed logon attempts allowed before disabling** - Specify the number of consecutive bad logons a VSA user or [Portal Access \(page 67\)](#) user is allowed before their account is disabled in the account field. The count is reset to zero after a successful logon.
- **Length of time to disable account after max logon failures exceeded** - Specify the amount of time, in hours or days, that the account is disabled in the field.

Note: To activate the account manually before the lockout time elapses, another user must enable the account using the [System > Users \(page 360\)](#) page.

- **Minutes of inactivity before a user session expires** - Specify the time period of user inactivity before the user is automatically logged out. Set the number of minutes of inactivity in the field.
- **Prevent anyone from changing their logon name** - Prevent anyone from changing their logon *name*.
- **Do not show domain on logon page** - Hide the **Domain** field on the logon page.

Note: If left blank, the domain checkbox still does not show on the logon page until at least one domain logon exists. Domain logons can be imported using [Agent > View AD Users](#) or added manually using [System > Change Logon \(page 355\)](#).

- **Do not show remember me checkbox on logon** - Hide the **Remember my username on this computer** checkbox on the logon page.

Specify password strength policy

Specify a password strength policy by checking the boxes beside the following:

- **Require password change every N days**
- **Enforce minimum password length**
- **Prohibit password reuse for N passwords**
- **Require upper and lower case alpha characters**
- **Require both alpha and numeric characters**
- **Require non-alphanumeric characters**

System

Update

Press **Update** to apply the settings.

Application Logging

System > Server Management > Application Logging

The **Application Logging** page controls the logging of application activity on the application server. *This function is only visible to master role users and is used primarily by Kaseya support.*

- It is possible to set the level of logging in the log files, from **None** to **Maximum**. The amount of information in these logs depends on how much logging is in each application and the level of detail specified by the **Application Logging** configuration.
- There are also checkboxes to record the request and response. An XML file is created in `\Kaseya>XML>Log` for each request and each response. In addition, there is an option to log transactions. When this is checked, another XML file is created in this same directory for each database update.
- There are options to filter by queue. This is to help narrow down the amount of information that goes into the log.
- The **Log** tab displays log records. This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 17).

Outbound Email

System > Server Management > Outbound Email

The **Outbound Email** page maintains settings for routing outbound email generated by the Kaseya Server to a host email server. The host email server accepts outbound email and delivers it to recipients on your behalf. If the email server host requires authentication you can include a username and password.

Note: These settings are typically set during the install process. You can modify them after the install using this page.

Enable/Disable Automatic Delivery

Automatic delivery of outbound email is disabled by default. You must enable automatic delivery of outbound email to send emails automatically throughout the VSA as soon as they are created.

Manual Delivery

If you disable automatic delivery, you can still send outbound email manually:

1. Click the **System > Outbound Email > Log** tab
2. Select one or more outbound emails with a status set to **Queued**.
3. Click the **Send Now** button.

Configuration

Click **Edit**. Complete the fields in the **Edit** dialog box.

- **Host Name** - The name of the host email server. Example: `smtp.mycompany.com`. If no authentication or special port number is required, then only specify values for the **Default Days to Keep Logs** and **Default Sender Email** fields.

Note: Entering localhost in the Host Name field means you are using the Kaseya Server's IIS Default SMTP Virtual Server to route outbound email. The Default SMTP Virtual Server service must be installed and running in order to send email. The service must also be able to resolve DNS addresses to route email to other SMTP servers.

- **Port** - Typically 25, but the host email server may require a different port number. Ports 465 and 587 are typically used for connecting to an SMTP email server over SSL/TLS.
- **User Name** - If required for authentication, enter the username of an account authorized to use the host email server.
- **Password** - If required for authentication, enter the password of the account.
- **Default Days to Keep Logs** - Enter the number of days to keep log outbound email entries.
- **Default Sender Email** - Enter the default From address displayed by outbound email. The From address displayed by outbound email uses the following order of precedence:
 1. If there is a From address in the **sendEmail()** step of a procedure, then that address is used.
 2. Else the sendEmail() step uses the From address provided by a linked Service Desk > **Message Template**, if the link exists and a From address is specified.
 3. Else the sendEmail() step uses the **Reply Email Address** of the Service Desk > **Incoming Email and Alarm Settings** > email reader linked to the service desk. This link between the email reader and the service desk is set using the Service Desk > Desk Definition > Properties > General > Standard Field Defaults > Email field.
 4. Else the **Default Sender Email** address set in System > **Outbound Email** is used.

Testing

If you suspect that you are not receiving emails from the Kaseya Server, click the **Test** button on this page to send test emails to various recipient addresses.

Note: If localhost is entered in the Host Name field, the Log tab could show a sent email as successful, but still not be relayed successfully because of configuration problems with the Default SMTP Virtual Server.

Click **Test**. Complete the fields in the **Test** dialog box.

- **To** - The email address to send the test email.
- **Subject** - The subject line of the test email.

Logging

The **Log** tab displays a log of all outbound emails sent by the Kaseya Server. This table supports **selectable columns, column sorting, column filtering and flexible columns widths** (page 17).

- **Send Now** - Send or resend selected emails
- **Forward** - Forward a selected email to a different address than originally specified.
- **View** - View a selected email.
- **Delete** - Delete selected emails.

Customize

Color Scheme

System > Customize > Color Scheme

The **Color Scheme** page determines the set of colors displayed by the VSA environment. **Color Scheme** selection applies to all users within the same **partition** (page 564).

To change color schemes:

System

1. Select a color scheme in the middle pane.
2. Click the **Set Scheme** button.

Site Customization

System > Customize > Site Customization

The **Site Customization** page provides the following tabs for customizing the user interface *for all users*.

- **Logon Page** (page 394)
- **Site Header** (page 394)
- **Agent Icons** (page 395)
- **Deploy Header** (page 395)
- **Org Custom Field Title** (page 396)

Each tab is edited separately.

Logon Page

System > Customize > Site Customization > Logon Page

The **Logon Page** tab of the **Site Customization** page sets the options displayed when a user logs on.

Note: See **VSA Logon Policies** (page 353) for a summary of functions affecting user logons.

1. Click the **Edit** button on the **Logon Page** tab. The **Edit Logon Page** dialog displays.
2. The following settings are all optional:
 - **Logo for Logon Page** - Browse to select a custom logon on your local machine or network.

Note: Your logo should be no larger than the recommended size.

- **Title** - Enter title text for this environment. The title displays just beneath the logo on the logon page.
- **Right Frame URL** - Enter the path to a custom webpage. The path must be relative to the `Webpages` directory, or relative to the `Webpages\Access` directory, or a fully-formed URL.
- **Display System Version on logon page** - If checked, the system version displays.
- **Display Forgot Password on logon page** - If checked, a **Forgot Password?** hyperlink displays on the logon page. Clicking the **Forgot Password?** link on the logon page—if activated using the **System > Site Customization > Logon Page** (page 394) tab—emails you a link where you can change your password. To change your password, you must have already filled out a **Security Question** and **Security Answer** using **System > Change Logon** (page 355).
- **Display System Status on logon page** - If checked, the system status displays on the logon page.
- **Display Customer ID on logon page** - If checked, the customer ID displays on the logon page.

Site Header

System > Customize > Site Customization > Site Header

1. Click the **Edit** button on the **Site Header** tab. The **Edit Site Header** dialog displays.
2. The following settings can be customized:
 - **Logo** - Browse to select a custom logo on your local machine or network. Click the **Default** button to reset back to the default.

Note: By default, VSA report headers display the image specified by the System > Site Customization > Site Header (page 394). Changing the value in the System > Configure > Change Reporting Config... (page 382) > Logo field overrides this default, changing the URL for report headers only. Changing the URL in the Change Reporting Config... > Logo field does not affect the display of the Site Header image.

- **Title** - Enter a custom title that displays next to the logo. Click the **Default** button to reset back to the default.
- **Header Height** - The header height in pixels. Defaults to 50.
- **Favorites Icon** - When your VSA website is bookmarked in a browser, this "favicon" image displays next to the text of the bookmark. Customize this image using a 16x16 pixel ico file.

Note: The Favorites Icon is not supported in a SaaS (page 564)-based VSA.

Agent Icons

System > Customize > Site Customization > Agent Icons

1. Click the **Edit** button on the **Agent Icons** tab. The **Edit Agent Icons** dialog displays.
2. Upload customized Windows icons to the Kaseya Server. Windows icons must be in .ico format, the color depth must not exceed 256 colors. The maximum size of 32x32 pixels is recommended.
 - **Agent online** - The agent is checking in successfully.
 - **Agent offline** - The agent is not checking in.
 - **Agent blinking** - A message is waiting to be read by the machine user.
 - **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.
3. Upload customized Mac icons to the Kaseya Server. Mac icons must be in .tif format, the color depth must not exceed 32 bit color. The maximum size of 48x48 pixels is recommended.
 - **Agent online** - The agent is checking in successfully.
 - **Agent offline** - The agent is not checking in.
 - **Agent blinking** - A message is waiting to be read by the machine user.
 - **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.

Note: Custom Mac icon images do not display in the Site Customization page, but display correctly when an agent install package is subsequently created and installed on a Mac machine.

4. Upload customized Linux icons to the Kaseya Server. Linux icons must be in .png format, the color depth must not exceed 256 colors. A size of 24x24 pixels is recommended.
 - **Agent online** - The agent is checking in successfully.
 - **Agent offline** - The agent is not checking in.
 - **Agent blinking** - A message is waiting to be read by the machine user.
 - **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.

Note: See *Creating Custom Agent Icons* (page 396) for more information.

Deploy Header

System > Customize > Site Customization > Deploy Header














Customize the logo and text displayed when Agent > **Deploy Agent** (page 35) displays a web page to the

System

user, instructing them to install the agent.

Use the edit toolbar to add images and special formatting to the text. *Images must be uploaded rather than copied and pasted in.*



-  - Hyperlink selected text. You may need to reset links copied and pasted from another source.
-  - Insert a table.
-  - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
-  - Indent text.
-  - Outdent text.
-  - Remove formatting.
-  - Insert a symbol.
-  - Insert an emoticon.
-  - Preview the display of text and images.
-  - Upload a file or image.
-  - Set selected text to subscript.
-  - Set selected text to superscript.
-  - Toggle full screen mode for editing and viewing.

Org Custom Field Title

System > Customize > Site Customization > Org Custom Field Titles


Customize the titles of custom fields that are used to classify organizations. Assign values to custom fields using System > Manage > Org/Groups/Depts/Staff > [Custom Fields](#) (page 376).

Creating Custom Agent Icons


Four Agent Icons

To incorporate custom agent icons in the system tray (Windows) or menu bar (Mac OS X) of each managed machine, create *four icons*. These icons must be named:

For Windows Agents


- `online.ico` – By default, this is the blue K icon  displayed when agent is connected to the Kaseya Server.
- `offline.ico` – By default, this is the gray K icon displayed when agent is not connected to the Kaseya Server.
- `blink.ico` – By default, this is the white K icon displayed when agent requires the user to click the icon to see a message.
- `noremote.ico` – By default, this is the red K icon displayed when the user has selected the [Disable remote control](#) menu item from the agent popup menu.

For Mac Agents

- `macOnline.tif` - By default, this is the blue K icon  displayed when agent is connected to the Kaseya Server.
- `macOffline.tif` - By default, this is the gray K icon displayed when agent is not connected to the Kaseya Server.
- `macNoremote.tif` - By default, this is the white K icon displayed when agent requires the user to click the icon to display a message.

- `macBlink.tif` - By default, this is the red K icon displayed when the user has selected the **Disable remote control** menu item from the agent popup menu.

For Linux Agents

- `linuxOnline.png` - By default, this is the blue K icon  displayed when agent is connected to the Kaseya Server.
- `linuxOffline.png` - By default, this is the gray K icon displayed when agent is not connected to the Kaseya Server.
- `linuxNoremove.png` - By default, this is the white K icon displayed when agent requires the user to click the icon to display a message.
- `linuxBlink.png` - By default, this is the red K icon displayed when the user has selected the **Disable remote control** menu item from the agent popup menu.

Formatting Custom Agent Icons

For **Windows** custom agent icons:

- The format must use the Windows icon format. A simple bitmap file cannot simply be renamed using the .ico extension.
- The maximum size of 32x32 pixels is recommended.
- The color depth cannot exceed 8 bit color (256 colors).

For **Apple** custom agent icons:

- The format must be .tif.
- The maximum size of 48x48 pixels is recommended.
- The color depth should be RGB 32 bit color.

For **Linux** custom agent icons:

- The format must be .png.
- A size of 24x24 pixels is recommended.
- The color depth cannot exceed 8 bit color (256 colors).

Installing Custom Icons

1. Navigate to the System > Site Customization > **Agent Icons** (*page 395*) tab.
2. Click the **Agent Icons** tab.
3. Click the **Edit** button. The **Edit Agent Icons** dialog displays.
4. Click the browse button for any agent icon to select a custom agent icon on your local machine.
5. Optionally click the **Use Default** buttons to reset agent icons to their default images.

Updating Existing Agents with Custom Agent Icons

The customized agent icons are automatically deployed when updating Agents using the Agent tab -> **Update Agent** (*page 72*). You will need to check the **Force update** check box to update agents that are already at the current version.

Creating Agent Install Packages with Custom Agent Icons

Updated agent icons are included in any newly downloaded `KcsSetup` files created by **Deploy Agent** (*page 35*). If you have placed an agent installer `KcsSetup` file in a domain logon script, then you must re-download the `KcsSetup` file to include the updated icons and replace the file on the domain server.

Local Settings

System > Customize > Local Settings

The following settings will be applied system wide going forward from this release. These settings currently affect the **Time Tracking** and **Service Billing** modules.

System

Date Format

- **Format** - Selects the date format used by dates the VSA.
 - mm/dd/yyyy
 - dd/mm/yyyy
 - yy/mm/dd
- **Delimiter used** - Selects the date format delimiter used by dates in the VSA.
 - / (slash)
 - - (dash)
 - . (dot)

Note: The time format is set in [System > Configure](#) (page 377).

Number Format

- **Decimal Places** - Selects the number of decimal places used to display currency in the VSA. Accepts up to 3 decimal places.
- **Decimal Format** - Selects the decimal format used to display currency in the VSA.
 - xx,xxx.xx
 - xx.xxx,xx

Customize: Live Connect

System > Customize > Live Connect

The **Customize: Live Connect** page customizes **Home** tabs that display in the **Live Connect** (page 344) and **Portal Access** (page 67) windows. You can create multiple, customized **Home** tabs and save them by name.

These **Home** tabs are enabled for a particular role by checking the checkbox underneath Live Connect > Home in:

- System > User Roles > **Access Rights** (page 366)
- System > Machine Roles > **Access Rights** (page 368)

Note: You can download a Live Connect PDF from the first topic of online help.

You can customize three sections on the default **Home** page.

- **Portal Header** - Customize the text and image displayed at the top of the **Home** tab.
- **Agent Procedures** - Provide a customized list of agent procedures that the user can run immediately from this tab.
- **Custom Links** - Provide a customized list of URLs that the user can click using this tab. For example, you could provide a URL to a website page providing technical information used to troubleshoot problems on managed machines.

Make available to All Tenants

If checked, this Home page can be added to user roles and machines roles on all tenant partitions. This option only displays for **master role users** (page 564).

Chapter 10

Ticketing

In This Chapter

Ticketing Overview	400
View Summary	400
Create/View	403
Delete/Archive	405
Migrate Tickets	408
Notify Policy	408
Access Policy	410
Assignee Policy	411
Due Date Policy	411
Edit Fields	412
Email Reader	414
Email Mapping	416

Ticketing Overview

The **Ticketing** module manages service requests. These service requests, and your response to them, are documented using **tickets**.

The ticketing system automatically notifies designated VSA users and ticket submitters by email for such system events as ticket creation, changes, or resolutions. The system organizes tickets by machine ID, group ID, organization ID, department ID or staff ID. You may wish to create a "generic" organization in System > **Manage** (page 372) to hold tickets of a global nature, such as general network problems.

Visibility of Tickets in Other Modules

Tickets can also be viewed using **Live Connect** (page 344) and in Info Center > **View Dashboard** (page 210).

Functions	Description
View Summary (page 400)	Lists all tickets. Each row displays summary data for a single ticket.
Create/View (page 403)	Create new tickets, or add or modify notes in existing tickets.
Delete/Archive (page 405)	Permanently delete tickets or move tickets into archival storage.
Migrate Tickets (page 408)	Migrate Ticketing tickets to and from Service Desk tickets.
Notify Policy (page 408)	Determine when email notifications are sent out by the Ticketing module.
Access Policy (page 410)	Determine who can edit and/or display fields in tickets.
Assignee Policy (page 411)	Create policies to automatically assign users to a new or existing ticket.
Due Date Policy (page 411)	Define default due dates for new tickets based on field values and email subject lines.
Edit Fields (page 412)	Define, modify, or create ticket fields used to classify tickets.
Email Reader (page 414)	Setup automatic polling of a POP3 email server to generate new ticket entries.
Email Mapping (page 416)	Define default field values for new tickets received using the Email Reader.

View Summary



Ticketing > Manage Tickets > View Summary

- Similar information is provided using Info Center > Reporting > Reports > **Ticketing** (page 208).

The **View Summary** page lists all tickets. Each row displays summary data for a single ticket.

New Tickets or New Notes

New tickets, or new notes in existing tickets, are clearly highlighted in one of two ways.

- **By Date** - Tickets with new notes entered in the last 1 day are **highlighted in red**. New notes entered in the last 7 days are **highlighted in yellow**. You can adjust these times and colors by clicking the **Change Highlight** link.
- **Read Flag** - Each ticket is flagged to indicate if the user has viewed all the notes in the ticket. Once viewed, the ticket is marked as read using the  icon. If another user or user adds or modifies a note, the flag is switched back to unread for you, showing the  icon.

Filtering

The list of tickets displayed depends on several factors:

- The list of machines displayed depends on the **machine ID / group ID filter** (page 23) and the user's **scope** (page 369).
- You can further *sort* and *filter* listed tickets by selecting values in the field drop-down lists.
- **Search** does not display any tickets if notes contain none of the words being searched for.
- Machine users only have access to tickets for their own machine ID using **Portal Access** (page 67).

Assignees

The assignee list displayed in **View Summary** (page 400) and **Create/View** (page 403) is based on the scope of the currently logged on user. Ticketing assignment in the **Ticketing** module always allows you to see master users, regardless of your role or scope.

Open Tickets, Past Due, Closed Tickets, Total Tickets

Shows the number of tickets open, past due, closed, and total for all tickets matching the filtering criteria described above.

Search

Search restricts the list of tickets to only tickets containing **any** of the words or phrases in the search string. Enclose a phrase in double-quotes (""). Search examines the ticket **Summary** line, submitter **Name**, submitter **Email**, submitter **Phone**, or any of the **Notes**.

Note: Using an asterisk (*) in the search field only finds tickets that include an asterisk.

Clicking any of the ticket **Summary** links in the paging area displays the details of that ticket using the **View Ticket** (page 403) page. Words in the ticket notes matching any **Search** word are *highlighted with a green background*.

<last 10 searches>

The drop-down list below the **Search** edit box lists the **<last 10 searches>** you have made. Selecting any item from the list automatically re-searches for those words.

Sort

Click either **ascending** or **descending** to order tickets by the selected column.

Fields...

Allows each user to organize the columns displayed in the table. Clicking **Fields...** opens a dialog in a new browser window. There, you can select which columns to show or hide and also the order in which columns are displayed. You can show/hide any of the following columns:

- **ID** - Unique ID number automatically assigned to each ticket.
- **Machine ID** - The ticket applied to this machine.
- **Assignee** - Name of the user responsible for solving this problem.
- **Category** - Type of problem this ticket discusses.

Ticketing

- **Status** - Open, Hold, Closed
- **Priority** - High, Normal, Low
- **SLA Type** - Service Level Agreement type
- **Dispatch Tech** - Yes, No
- **Approval** - Required, Not Required
- **Hours Worked** - Hours worked, in decimal format.
- **Last Modified Date** - Last time any note was added to this ticket.
- **Creation Date** - Time when the ticket was first entered.
- **Due Date** - Ticket due date.
- **Resolution Date** - Date the ticket was closed.
- **Submitter Name** - Person who submitted this ticket: user, user name, or machine ID.
- **Submitter Email** - The submitter email address.
- **Submitter Phone** - The submitter phone number.

You can also select additional custom fields you have previously created using Ticketing > [Edit Fields](#) (page 412).



Automatically submit on field changes / Submit

If **Automatically submit on field changes** is checked, then the **View Summary** page redisplay as soon as a single field in the **List Fields Filter** is changed. If blank, then you can change several of the **List Fields Filter** at one time. The **View Summary** page won't redisplay until you click **Submit**.

(List Fields Filter)

Each field of type **List**—such as **Category**, **Status**, or **Priority**—are shown as selectable drop-down lists. Selecting values from one or more of these drop-down lists filters the paging area to display only those tickets matching the selected values. Custom **List** fields are created using Ticketing > [Edit Fields](#) (page 412).



Mark All Read

Click to mark all tickets as read. Read tickets display a  icon. Any changes or note additions inserted by other users reset the ticket to unread. Unread tickets display a  icon.

Set Field...

Use **Set Field...** to change multiple field values on multiple tickets at once. Check the box for all the tickets you wish to change a field value for. Then click **Set Field...** A dialog box displays that enables you to set a new value for any of the fields.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Merge...

To merge tickets, *check the box for any two tickets* listed, then click the **Merge...** button. The resulting merged ticket contains all the notes and attachments from both tickets. You are asked which field values you wish to use in the ticket for all field values that are different between the two tickets.

Change Highlight

Click **Change Highlight** to set and/or modify row highlighting based on date. Highlight tickets in two ways. Tickets with a date within 1 day of the current time are **highlighted in red**. Tickets with a date within 7 days are **highlighted in yellow**. You can independently *adjust both the number of days and the highlight color*. To disable highlighting by date, set each number of days to zero. The highlight date may be **last modified date**, **due date**, or **creation date**.

Select All/Unselect All





Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Column Headings

Clicking any column heading re-orders the table using that column as the sort criteria.

Data Table

Each row of the table lists summary data for a single ticket.





- To display the details of the ticket in a *new window* click the new window  icon. Hovering the mouse cursor over the  icon of a ticket displays a preview window of the latest notes for that ticket. Use this to quickly review tickets in your queue. The number of milliseconds the cursor has to hover can be specified using System > [Preferences](#) (page 353).
- To display the details of the ticket in the *same window* click the [summary](#) line link.
- To toggle the state to *read* click .
- To toggle the state to *unread* click .

Create/View

[Ticketing](#) > [Manage Tickets](#) > [Create/View](#)

The [Create/View](#) page creates new tickets, or adds or modify notes in existing tickets.

Adding a New Ticket

1. Bypass the [Ticket ID](#) field. It will be populated with a new unique number when the ticket is created.
2. Click [Select association](#) to associate the ticket with one of six types of VSA records: asset, machine ID, machine group, organization, department, or staff. This is mandatory.
3. Enter a short description of the problem in the [Summary](#) field.
4. The [Submitter](#) fields are populated as follows:
 - If a machine ID was selected in step 2, the submitter [User Name](#), [User Email](#) and [User Phone](#) fields are populated with contact data maintained for this machine ID using Agent > [Edit Profile](#) (page 65). This information can be updated if need be.
 - If anything other than machine ID was selected in step 2, these submitter fields can be filled in manually, if applicable.
 - If a ticket was created by an incoming email using Ticketing > [Email Reader](#) (page 414), the [Submitter Email](#) field is populated with the sender's email address.
5. The [Date Created](#) is automatically assigned.
6. The [Age / Closed](#) date is automatically assigned. [Age](#) lists the number of hours/days since the creation date for non-closed tickets. If the ticket has been closed then [Age](#) is replaced with [Closed](#) and displays the date and time this ticket was closed.
7. The default due date for a ticket is determined by the Ticketing > [Due Date Policy](#) (page 411). The due date is based on the ticket attributes you enter when a *new* ticket is entered. If a due date policy is in force for a ticket, then a policy icon  displays next to the due date. You can override the existing due date by clicking the edit icon  next to the due date. The policy icon  is replaced by a manual override icon  next to the due date. Click the [Apply](#) button to reset the due date to the policy enforced due date. If the due date does not match any of the defined [due date policies](#) (page 411), then the [Due Date](#) label is highlighted. If no due date policies are defined then the system default due date is used, which is one week from the creation date of the ticket. When a ticket is overdue, the due date displays in bolded **dark red text**, both in the [View Summary](#) (page 400) page and in [Ticketing](#) (page 208) reports. It also displays in **red text** in the header of the [Create/View](#) (page

Ticketing

403) page. You can optionally send an email for overdue tickets using Ticketing > **Notify Policy** (page 408). A ticket is resolved when its status is set to closed and the resolution date is recorded.

8. Classify the ticket using the built-in **List** type fields, such as **Assignee**, **Category**, **Status**, and **Priority**. You can also classify the ticket using additional **List** type fields that have been created for tickets using Ticketing > **Edit Fields** (page 412).
9. Enter details of the problem in the **Notes** edit box. Click the **Note Size** link to change the number of rows available for your note text.
10. To attach a file, such as a screen shot, to the ticket, click **Browse...** below the note entry area. Locate the file you wish to attach on your local computer. Click **Open** in the browse window to upload the file to the VSA server. Once the file has been successfully uploaded, tag text is automatically entered into the note in this format: `<attached file:filename.ext>`. This tag appears as a hyperlink in a note for the ticket. Display/download the file at any time by clicking that link.

Note: The following list of filename extensions display as images or text in the note, instead of displaying as a hyperlinked filename: gif, jpg, png, bmp, txt, sql.




Note: Ticket note attachments are typically located in the C:\Kaseya\WebPages\ManagedFiles directory.

11. Check the **Suppress email notification** checkbox if you don't want email recipients, either VSA users or machine users, to be notified about the ticket. In most cases you'll want to leave this blank.
12. Check the **Suppress automatic note creation checkbox** if you don't want a note to be added automatically. This option is hidden by default. Use **Access Policy** (page 410) to display it.
13. Complete the creation of the ticket in one of two ways:
 - Click **Submit** to complete the creation of the ticket and to notify *both* VSA users and machine users by email.
 - Click **New Hidden** to complete the creation of the ticket to notify *only* VSA users by email. Use hidden notes to record data or analysis that may be too detailed or confusing to machine users but useful to other VSA users.

Note: Hidden notes are *never* included in email notifications.

Editing an Existing Ticket

To display an existing ticket, enter a ticket number in the **Ticket ID** field.




- If you don't know the number of the ticket, use **View Summary** (page 400) or **Delete/Archive** (page 405) to locate and select the ticket. The ticket will be displayed using this page.
- When an existing ticket first displays on this page, the header fields show the most recent settings for the ticket.
- Making changes to any of the **List** type fields immediately creates a new note for the ticket, identifying the change.
- Making changes to any of the non-**List** type fields—such as the **Summary** field, **Submitter** information, or fields that accept freeform text entries or numbers—requires you to click **Update** afterwards to create a new note.
- Edit any *previous* note for a ticket by clicking the edit icon  next to the note you wish to edit. This populates the header fields with the settings for this note. It also highlights the row of the note being edited in light yellow. You can change the contents of the note, including the timestamp for the note. Click **Change** to confirm the changes you have made.
- Delete notes by clicking the delete  icon next to the note.
- Split a ticket into two tickets by clicking the split  icon next to the note. The new ticket contains the note and all more recent notes. The original ticket can either be closed or left unchanged.



Note: View, edit and delete privileges for tickets and fields are controlled using [Ticketing > Access Policy](#) (page 410). VSA users and machine users are notified about ticket changes based on [Ticketing > Notify Policy](#) (page 408). Change the number automatically assigned to the next new ticket using [Edit Fields](#) (page 412).

Assignees

The assignee list displayed in [View Summary](#) (page 400) and [Create/View](#) (page 403) is based on the scope of the currently logged on user. Ticketing assignment in the [Ticketing](#) module always allows you to see master users, regardless of your role or scope.

Assignee Policy Icon

By default a always enforce assignee policy icon  displays next to the assignee field. This indicates that assignee names are automatically selected using [Assignee Policy](#) (page 411). Click the  icon once to display the override the assignee policy icon . This overrides the assignee policy and allows you to select an assignee manually.

Note: If no assignee policy is defined for the combination of List type fields values selected, then toggling between the  and  icons has no effect.

Displaying the "Create/View" Page Using a URL

The following URL displays the [Create/View](#) (page 403) web page for a specific ticket ID

`http://...?ticaid=<TicketID>`

For example:

`http://demo.kaseya.com?ticaid=1234`

Time/Admin

Lists the time a change was made to a ticket and the user or user who made the change.

Note

Lists all notes relating to this ticket in ascending or descending time order. Each note is time stamped and labeled with the logon name of the person entering the note.

Note: User entered notes are labeled with the machine ID they logged in with. See [Portal Access](#) (page 67) for details.

Hide

If checked, the note is hidden from VSA users but not machine users. The default setting is determined by the [as hidden note](#) checkbox in [Ticketing > Access Policy](#) (page 410). Access policies are applied by user role. If you belong to more than one user role, the most restrictive policy has precedence.

Delete/Archive

[Ticketing](#) > [Manage Tickets](#) > [Delete/Archive](#)

The [Delete/Archive](#) page deletes old tickets, or deletes tickets in a particular category or status. You may reach the point where your system has so many old tickets that they are cluttering up searches with obsolete data.

Ticketing

Note: View, edit and delete privileges for tickets and fields are controlled using [Ticketing > Access Policy](#) (page 410).

Archiving Tickets

In addition to delete, you can also **archive** tickets. Archived tickets stay in the database but are moved to separate tables. Use archive to move obsolete or old tickets out of the active database **without** deleting them from the system. You can always move tickets back and forth between the active database table and the archive database table.

Filtering

The list of tickets displayed depends on several factors:

- The list of machines displayed depends on the **machine ID / group ID filter** (page 23) and the user's **scope** (page 369).
- You can further *sort* and *filter* listed tickets by selecting values in the field drop-down lists.
- **Search** does not display any tickets if notes contain none of the words being searched for.
- Machine users only have access to tickets for their own machine ID using **Portal Access** (page 67).
- Use the **Hide tickets last modified after** control to only display tickets *earlier* than a certain date.

Archiving Closed Tickets

If, for example, you want to archive **Closed** tickets older than 6 months perform the following steps:

1. Select **Closed** from the **Status** control.
2. Set the **Hide tickets last modified after** control to list only tickets last modified 6 months ago or earlier.
3. Click the **Set** button.
4. Click the **Select All** link.
5. Click the **Archive...** button.
6. Check the **Display archived tickets instead of active tickets** checkbox to search and examine the archived tickets. You can move tickets back to the active table here using the **Restore...** button.

Open Tickets, Past Due, Closed Tickets, Total Tickets

Shows the number of tickets open, past due, closed, and total for all tickets matching the filtering criteria described above.

Search

Search restricts the list of tickets to only tickets containing **any** of the words or phrases in the search string. Enclose a phrase in double-quotes ("). Search examines the ticket **Summary** line, submitter **Name**, submitter **Email**, submitter **Phone**, or any of the **Notes**.

Note: Using an asterisk (*) in the search field only finds tickets that include an asterisk.

Clicking any of the ticket **Summary** links in the paging area displays the details of that ticket using the **View Ticket** (page 403) page. Words in the ticket notes matching any **Search** word are *highlighted with a green background*.

<last 10 searches>

The drop-down list below the **Search** edit box lists the **<last 10 searches>** you have made. Selecting any item from the list automatically re-searches for those words.

Sort

Click either **ascending** or **descending** to order tickets by the selected column.

Fields...

Allows each user to organize the columns displayed in the table. Clicking [Fields...](#) opens a dialog in a new browser window. There, you can select which columns to show or hide and also the order in which columns are displayed. You can show/hide any of the following columns:

- **ID** - Unique ID number automatically assigned to each ticket.
- **Machine ID** - The ticket applied to this machine.
- **Assignee** - Name of the user responsible for solving this problem.
- **Category** - Type of problem this ticket discusses.
- **Status** - Open, Hold, Closed
- **Priority** - High, Normal, Low
- **SLA Type** - Service Level Agreement type
- **Dispatch Tech** - Yes, No
- **Approval** - Required, Not Required
- **Hours Worked** - Hours worked, in decimal format.
- **Last Modified Date** - Last time any note was added to this ticket.
- **Creation Date** - Time when the ticket was first entered.
- **Due Date** - Ticket due date.
- **Resolution Date** - Date the ticket was closed.
- **Submitter Name** - Person who submitted this ticket: user, user name, or machine ID.
- **Submitter Email** - The submitter email address.
- **Submitter Phone** - The submitter phone number.

You can also select additional custom fields you have previously created using Ticketing > [Edit Fields](#) (page 412).

Automatically submit on field changes / Submit

If [Automatically submit on field changes](#) is checked, then the [View Summary](#) page redisplay as soon as a single field in the [List Fields Filter](#) is changed. If blank, then you can change several of the [List Fields Filter](#) at one time. The [View Summary](#) page won't redisplay until you click [Submit](#).

(List Fields Filter)

Each field of type [List](#)—such as [Category](#), [Status](#), or [Priority](#)—are shown as selectable drop-down lists. Selecting values from one or more of these drop-down lists filters the paging area to display only those tickets matching the selected values. Custom [List](#) fields are created using Ticketing > [Edit Fields](#) (page 412).



Hide tickets last modified after / Set

[Set](#) the date and time of this control to only display tickets *earlier* than a certain date.

Select All/Unselect All

Click the [Select All](#) link to check all rows on the page. Click the [Unselect All](#) link to uncheck all rows on the page.

Select Page

When more rows of data are selected than can be displayed on a single page, click the  and  buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Delete...

Select one or more tickets and click the [Delete...](#) button to permanently delete the tickets from the system. Deleted tickets cannot be restored.

Ticketing

Archive...

Select one or more tickets and click the **Archive...** button. Archived tickets stay in the database but are moved to separate tables. Use archive to move obsolete or old tickets out of the active database *without* deleting them from the system. You can always move tickets back and forth between the active database table and the archive database table.

Display archived tickets instead of active tickets / Restore

Check the **Display archived tickets instead of active tickets** checkbox to search and examine the archived tickets. You can move tickets back to the active table here using the **Restore...** button.

Migrate Tickets

[Ticketing](#) > [Manage Tickets](#) > [Migrate Tickets](#)

The **Migrate Tickets** page performs two tasks:

- Migrates selected **Ticketing** tickets into **Service Desk** tickets.
- Imports **Service Desk** ticket XMLs into **Ticketing** tickets.

Migrating Tickets from Ticketing into Service Desk

The paging area of **Migrate Tickets** displays all the tickets visible to you in the [Ticketing > View Summary](#) (page 400) page.

1. Select the tickets you want to migrate in the paging area. Click **Select All** to select all tickets.
2. Click **Migrate** to migrate all the selected tickets into **Service Desk**.

Importing Service Desk Tickets into Ticketing

1. Export selected tickets in **Service Desk** to an XML file on your local machine or network, using the **Export** button in [Service Desk > Tickets](#).
2. Click **Import** in [Ticketing > Migrate Tickets](#) and select the XML file you created in step 1 above.

Notify Policy

[Ticketing](#) > [Configure Ticketing](#) > [Notify Policy](#)

The **Notify Policy** page determines when email notifications are sent out by the **Ticketing** module. *Multiple policies can be defined for each machine group, by clicking the **Add** button instead of the **Update** button.* This lets you specify different email lists for different ticketing events. For example, you may wish to send email alerts to a group of users for ticket creations and note additions, but send email to a different list of users for overdue tickets.

To be sent email notification for a ticketing event:

1. Check the box to the left of each ticketing event you need to be notified about.
2. Enter a comma separated list of email address in the **Email List** edit box.
3. Check the box to the left of all group IDs you wish to apply this notification policy to.
4. Click the **Update** or **Add** button.

Note: You can *not* send notifications to the email address used to receive tickets, defined using [Ticketing > Email Reader](#) (page 414).

From Address

The **From** address used by ticket notifications is based on the **Email Reader** (page 414) address, if one is

defined. If an **Email Reader** has not yet been defined then the **From** address in System > **Outbound Email** (page 392) is used.

Notification Type Checkbox

The list below describes when the ticketing system sends an email notification *to all email recipients in the email list*.

- **Ticket Creation** - If checked, an email is sent at the time of ticket creation.
- **Modify/Add Note** - If checked, an email is sent when a ticket is changed, including adding a note to ticket.
- **Overdue Ticket** - If checked, an email is sent when a ticket passes its due date without being closed.
- **Edit Summary** - If checked, an email is sent when anyone changes the summary line for a ticket. Click **Format** to edit the format for this email notification.
- **Send auto response to emails creating new tickets** - If checked, an automated reply message is sent out to the person that sent in an email that generated a new ticket. Automated response emails give your users an acknowledgement that their request has been received and processed by the system. Creating tickets based on inbound emails are configured using **Email Reader** (page 414) and **Email Mapping** (page 416). Click **Format** to edit the format for this email notification.
- **Assignee Change** - If checked, an email is sent when a ticket is assigned to a different user. Click **Format** to edit the format for this email notification.
- **Field Change** - If checked, an email is sent when anyone changes any custom field in a ticket. Click **Format** to edit the format for this email notification.
- **Due Date Change** - If checked, an email is sent when anyone changes the due date of a ticket. Click **Format** to edit the format for this email notification.
- **Notify Ticket Submitter when note added** - If checked, an email is sent to the email address entered for the ticket submitter, in addition to the email list for all email notification messages.
- **Include all public notes in Modify/Add notification** - If checked, *all* notes for a ticket are included when a **Modify/Add Note** message is sent out.
- **Received email alerts always sent to assignee** - If checked, an email is sent to the ticket assignee, whenever a reply email is received and added to the ticket, even if the assignee is not on the notification email list for this group ID.
- **Send auto response to emails creating new tickets** - If checked, an automated reply message is sent out to the person that sent in an email that generated a new ticket. Automated response emails give your users an acknowledgement that their request has been received and processed by the system. Creating tickets based on inbound emails are configured using **Email Reader** (page 414) and **Email Mapping** (page 416). Click **Format** to edit the format for this email notification.

Note: Format Email... buttons only display for master role users.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Machine Group

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

Enable Events TMOAFEDNIRS

Identifies the ticketing events that trigger email notification of email recipients listed in the **Email List** column.

Email List

The list of email recipients notified by selected ticketing events for this group ID.

Access Policy

Ticketing > Configure Ticketing > Access Policy

The **Access Policy** page determines who can edit and/or display fields in tickets. Independent policies can be set for each user role and for all machine users. Machine users only see tickets assigned to their machine ID. Non-master role users only see tickets for scopes they are authorized to access.

Select user or role

Before setting any other policy options, select `<Users>`, meaning all machine users, or a user role from the drop-down list.

Access Rights

The following access rights apply to *all machine users* or to a selected *user role*, as specified using **Select user or user group**.

- **Enable ticket delete** - If checked, the selected user role can delete entire tickets using the **Delete/Archive** (page 405) page.
- **Enable ticket edit to modify or remove notes or modify summary line (Adding new notes is always enabled)** - If checked, the selected user role can edit existing notes or modify the summary line.

Note: Adding new notes is always enabled for all user groups.

- **Enable associate ticket with editing** - If checked, enables the selected user role to edit the machine ID or group associated with a ticket.
- **Enable submitter information editing** - If checked, enables submitter information to be edited.
- **Enable due date edit when editing trouble tickets** - If checked, the selected user role can modify the ticket due date.
- **Enable suppress email notifications when editing trouble tickets** - If checked, the selected user role can suppress email notifications when modifying an existing ticket.
- **View hidden notes** - If checked, the selected user role can view hidden notes.

Note: Hidden notes can never be viewed by users.



- **Change hidden notes status checkbox** - If checked for the selected user role, notes display a **Hide** checkbox at the far right edge of each ticket note. Toggling the **Hide** checkbox makes a note hidden or not hidden.
- **Automatically insert new note with every field change** - If checked for the selected user role, notes are automatically inserted whenever any ticket field changes.
 - **As hidden note** - If checked for the selected user role, automatic notes are added as hidden notes. This policy only applies if **Automatically insert new note with every field change** is checked.
 - **Allow admin to suppress auto note add** - Suppresses the adding of an automatic note when ticket properties are changed and no manual note is added.
- **Define access to each ticket field** - Defines access to each field for the selected user role. Fields are created using **Edit Fields** (page 412). Three levels of access are possible:
 - **Full Access** - Can view and modify this field in every ticket.
 - **View Only** - Can see but not change the value of this field.
 - **Hidden** - Hidden fields are not shown.

Assignee Policy


Ticketing > Configure Ticketing > Assignee Policy

The **Assignee Policy** page automatically assigns a VSA user to a new or existing ticket. Assignment is based on the combination of List type field values entered for a ticket. List type fields and their possible values are defined using Ticketing > **Edit Fields** (page 412). The policy is enforced every time the ticket is saved.

Overriding Assignee Policy

Assignee Policy can be overridden for a specific ticket using the **Create/View** (page 403) page, by the toggling the  icon next to the **Assignee** field to display a  icon, then assigning a user manually.

Order of Precedence

The order of precedence for policy *selection* is based on the alphabetical sort order of the policy *name*, which also determines how the policies are listed in the paging area. For example, a policy named of AAA will always be selected before BBB, so long as all of the fields in AAA match the settings of the ticket. You can *force* policy selection to use the sort order you prefer by naming the policies accordingly. For example, you can add a numerical prefix to each policy name, such as 01, 02, 03, ... and adjust the sort order in this fashion. To rename existing policies, select the edit icon  next to a policy name, then enter a new name and click **Apply**.

Policy Name

Enter the name for the assignee policy.

Assignee

Select the user who will be assigned tickets that match the selected combination of List type field values.

Create

Click **Create** to create the assignee policy.

List Fields

Each field of type List—such as **Category**, **Status**, or **Priority**—are shown as selectable drop-down lists. Select values for one or more of the fields. The combination of List type field values associated with an assignee determines which assignee is automatically assigned to a new or existing ticket.

Due Date Policy

Ticketing > Configure Ticketing > Due Date Policy

The **Due Date Policy** page sets the due date for each **new ticket** based on field values. Any combination of List type fields may be defined to set a due date. This allows you to set a new ticket due date based on the urgency of the ticket and a guaranteed level of service. For example, define a new List type field named **Service Level** with the following values: Premium, Standard, Economy. Create different due date policies for each combination such as:

- Set resolution time to 1 Hrs when **Priority** = High and **Service Level** = Premium
- Set resolution time to 7 Days when **Priority** = Normal and **Service Level** = Economy

When a new ticket gets created, the due date is set by adding the number of hours in the policy to the current time.


Note: You can change the due date of an existing ticket manually using **Create/View** (page 403).

Ticketing

Overdue Tickets

When a ticket is overdue, the due date displays in bolded **dark red text**, both in the [View Summary](#) (page 400) page and in [Ticketing](#) (page 208) reports. It also displays in **red text** in the header of the [Create/View](#) (page 403) page. You can optionally send an email for overdue tickets using Ticketing > [Notify Policy](#) (page 408). A ticket is resolved when its status is set to closed and the resolution date is recorded.

Order of Precedence

The order of precedence for policy *selection* is based on the alphabetical sort order of the policy *name*, which also determines how the policies are listed in the paging area. For example, a policy named of AAA will always be selected before BBB, so long as all of the fields in AAA match the settings of the ticket. You can *force* policy selection to use the sort order you prefer by naming the policies accordingly. For example, you can add a numerical prefix to each policy name, such as 01, 02, 03, ... and adjust the sort order in this fashion. To rename existing policies, select the edit icon  next to a policy name, then enter a new name and click [Apply](#).

Default time to resolve tickets with no policy

Enter the number of hours or days to resolve tickets when new tickets are created that do not match any policy.

Policy Name

Enter a name for a new or selected due date policy.

Resolve Time

When new tickets are created that match the field values in this policy, then the due date is set to this number of hours or days plus the current time.

Fields

Select values for one or more [List](#) type fields that a new ticket must match to automatically set the due date for the new ticket.

Delete Icon

Click the delete icon  to delete a row in the paging area.

Edit Icon

Click a row's edit icon  to populate header parameters with values from that row. You can edit these values in the header and re-apply them. The selected row is highlighted in yellow.

Name

The name of the due date policy.

Time

The time added to the current date and time to set the due date policy for a new ticket.

All Other Columns

The values of list fields that must be matched to set a due date for a new ticket using this policy. User defined [List](#) fields are maintained using [Edit Fields](#) (page 412).

Edit Fields

[Ticketing](#) > [Configure Ticketing](#) > [Edit Fields](#)

The [Edit Fields](#) page creates fields used to classify tickets and sets the default values for those fields. Fields are associated with the entire ticket, as opposed to each note of the ticket. You can *customize*

the field label and corresponding values of each field, including the mandatory fields. The fields you define here display in the following pages: [View Summary](#) (page 400), [View Ticket](#) (page 403), [Delete/Archive](#) (page 405), [Access Policy](#) (page 410), [Due Date Policy](#) (page 411) and [Email Mapping](#) (page 416).

Mandatory Fields


Three mandatory **List** type fields exist that may not be removed from the system. The values for these list fields can be customized. The mandatory fields are:

- **Category** - Classifies tickets by IT category.
- **Status** - State of the current ticket: **Open**, **Hold**, **Closed**
- **Priority** - **High**, **Normal**, **Low**

Set the next ticket ID to N / Apply

Specify the ticket number for the next ticket. Displays the current "next" ticket number. Click **Apply** to confirm any changes.

Field Position

Click the up/down arrows  to the left of the field label to change the display position for this field in [Create/View Tickets](#) (page 403).

Field Label

You can modify the label for any field here. Click the **Update** button to apply the change.

Type

Specify the data type for each field.

- **String** - Can contain any text up to 500 characters in length. Best used to hold things like problem location or other variables that do not belong in the summary line.
- **Integer** - Can contain any positive or negative integer value
- **List** - Lets you create a drop-down list of choices. The choices for **List** type fields are edited by clicking the **<Edit List>** value in the **Default Value** drop-down list.

Note: Only **List** type fields display as a selectable drop-down list that can filter the display of tickets in the [View Summary](#) (page 400) and [Delete/Archive](#) (page 405) pages.

- **Number (nn.d)** - A number that always shows one digit to the right of the decimal point.
- **Number (nn.dd)** - A number that always shows two digits to the right of the decimal point.
- **Number (nn.ddd)** - A number that always shows three digits to the right of the decimal point.
- **Number (nn.dddd)** - A number that always shows four digits to the right of the decimal point.

Default Value

Creating a new ticket automatically sets each field to its default value. You can specify that default value here.

Note: Default values are system wide and may not be different for different machine group IDs or user roles.

Note: [Email Mapping](#) (page 416) can override the default values selected here for tickets created using [Email Reader](#) (page 414).

<Edit List>

This value displays in the drop-down list for a **List** type field in the **Default Value** column. Click **<Edit List>** to edit the list of values for that field.

Ticketing

Update

Click **Update** to confirm changes to field labels, default values, or **List** type values.

New

Click **New** to create a new field.

Email Reader

Ticketing > Configure Ticketing > Email Reader

The **Email Reader** page specifies a POP3 email account to periodically poll. Email messages retrieved from the POP3 server are classified by **Email Mapping** (page 416) and converted into tickets.

Alarm to Ticket Integration

When a VSA user clicks a **New Ticket...** link—typically for an alarm—anywhere in the system, the **Ticketing** module converts it into a ticket. The **Ticketing** email reader does not have to be enabled.

Note: If the **Service Desk** module is installed, see **Service Desk > Activating Service Desk Integration** (<http://help.kaseya.com/webhelp/EN/KSD/7000000/index.asp#5478.htm>).

Contents of Email

The **Email Reader** can receive any email, with or without attachments, and add the contents to the ticketing system. Additional information can be added to the email to enhance the mapping of the email to the ticketing system. The following tags can be included in *either the subject or the body* of the email.

- `~ticrefid='xxx'` - Appends the body of the email to an existing ticket rather than cause a new ticket to be created.
- `~username='xxx'` - Automatically inserts the value given as `xxx` into the **Submitter Name** field.

Note: If `~username='xxx'` is *not* included in the either the subject or the body of the email, then the email sender's From address is used to populate the **Submitter Name** field.

- `~useremail='xxx'` - Automatically inserts the value given as `xxx` into the **Submitter Email** field.
- `~userphone='xxx'` - Automatically inserts the value given as `xxx` into the **Submitter Phone** field.
- `~category='xxx'` - Assigns the ticket created to a specific category. The category must exist.
- `~priority='xxx'` - Assigns the ticket created to a specific priority. The priority must exist.
- `~status='xxx'` - Assigns the ticket created to a specific status. The status must exist.
- `~assignee='xxx'` - Assigns the ticket created to a specific user. The user must exist.
- `~machineid='xxx.xxx'` - Assigns the ticket created to a machine ID. The machine ID must exist. If this information is not included, and tickets are not assigned to a machine ID or group ID using **Email Mapping** (page 416), tickets are assigned to the **unnamed** group by default.
- `~fieldName='xxx'` - Assigns the value `xxx` for any defined field. If the field is a **List** type, then the value must exist in the list.

Suppressed Notes

Notes are suppressed if an email is sent with no body and no attachments or if no response text is sent with a reply email.

Email Reader Alerts

You can be alerted by email if the Ticketing > Email Reader fails using Monitor > **Alerts - System** (page 275) alerts.

Email Address

Enter the email address you wish to retrieve email messages from periodically. Replies to this email address are in turn processed by the ticketing system and added as notes to the relevant ticket.

Disable email reader

Check this box to prevent the email reader component from polling a server.

View Log

Click [View Log](#) to review the polling log for this email reader.

Turn off independent ticket sequence numbering (use identity value)

For "on premises" single [partition](#) (page 564) environments only, if checked, ticket numbers match the ticket numbers displayed in outbound emails. If unchecked, these two numbers can be different. These number always match in additional partitions.

Host Name

The name of the POP3 host service is needed. POP3 is the only email protocol supported. An example is `pop.gmail.com`.

Port

Provide the port number used by the POP3 service. Typically non-SSL POP3 ports are 110 and SSL POP3 ports are 995.

Use SSL

Check this box to enable SSL communications with your POP server. Your POP server must support SSL to use this feature. Typically, SSL enabled POP3 servers use port 995.

Logon

Enter the email account name. Do not include the @ domain name with the account name. For example, if the [Email Address](#) is `jsmith@acme.com`, then enter `jsmith` as the account name.

Password

Enter the email account password.

Check for new emails every <N> minutes

The number of minutes the [Email Reader](#) should wait before polling the POP3 server for new emails.

Reject inbound emails containing the following in the subject line

This option only displays for [master role users](#) (page 564). Enter text to ignore inbound emails containing this text *in the subject line*. Matching is case insensitive. *Quotes and wildcard characters such as * and ? are interpreted literally as part of the string content.* Create multiple filters using multiple lines. Multiple filters act as an OR statement. Surround whole words with spaces on both sides of each word. Example:

```
Undeliverable
Do not reply
```

This same ignore list can be maintained in the Ticketing > [Email Reader](#) (<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#434.htm>) page and the Service Desk > Incoming Email and Alarm Settings > General tab. This list can also be maintained manually by editing the `<Kaseya_Installation_Directory>\Kaseya\KServer\ignoreSubject.txt` file.

Apply

Click [Apply](#) to begin using the email reader.

Connect Now

Click [Connect Now](#) to connect to the POP3 server immediately instead of waiting for the next polling time. This can be used to test your configuration of the email reader.

Email Mapping

[Ticketing](#) > [Configure Ticketing](#) > [Email Mapping](#)

The [Email Mapping](#) page assigns default values for [new tickets](#) created using the [Email Reader](#) (page 414). The default values assigned are based on the email address or email domain of the email *sender*. Matching can be optionally filtered by the text entered in the email subject line. This information overrides the standard defaults defined using [Edit Fields](#) (page 412).

Email Address or Domain

The email address or domain *of the sender*. For example: `jsmith@acme.com` or `acme.com`.

Set map for unassigned emails

If checked, assigns default field values for inbound emails not covered by any other email map.

Subject Line Filter

Assigns ticket defaults when the *email subject line matches the filter string*. Matching is case insensitive. No wildcard processing is provided. A single *, without any other characters in the filter, means let anything through. Booleans statements are not accepted.

Associate map with

Click the [Select association](#) link to associate new tickets created using this map with a machine ID, machine group, organization, department or staff record.

Assignee

Enter the name of the VSA user assigned to new tickets created using this email map.

Fields

Specify the default field values assigned to new tickets created when an email is received by the ticketing system using this map.


Create

Click [Create](#) to create a new email map using the header values you have previously selected.

Delete Icon

Click the delete icon  to delete this record.

Edit icon

Click the edit icon  for a row to automatically set header parameters to those matching the selected machine ID.

Chapter 11

Database Views

In This Chapter

Database Views and Functions	419
Excel Usage	419
Crystal Reporting Usage	420
Views and Functions Provided	423
fnMissingPatchCounts_UsePolicy / fnMissingPatchCounts_NoPolicy	425
fnOSCounts	426
vAddRemoveList	427
vAdminNotesLog	427
vAgentConfiguration	427
vAgentLabel.....	428
vAlertLog	429
vBackupLog.....	430
vBaseApplicationInfo / vCurrApplicationInfo	431
vBaseCpuInfo / vCurrCpuInfo	432
vBaseDiskInfo / vCurrDiskInfo.....	432
vBaseDriveManufacturer / vCurrDriveManufacturer	433
vBasePciInfo / vCurrPciInfo.....	433
vBasePrinterInfo / vCurrPrinterInfo	434
vCollectionMember.....	434
vConfigLog	435
vEventDetail	435
vEventInstanceDetail.....	436
vEventInstanceHistoryDetail	438
vLicenseInfo	439
vMachine	440
vMonitorAlarmAlert.....	442
vMonitorAlarmCounter.....	443
vMonitorAlarmProcess	444
vMonitorAlarmService	445
vMonitorAlarmSNMP	446
vMonitorAlarmSystemCheck	447

Database Views

vNetStatsLog	448
vNtEventLog	448
vOnBoardDeviceInfo	449
vPatchApprovalPolicyStatus	449
vPatchApprovalStatus	450
vPatchConfiguration	451
vPatchPieChartCountsNoPolicy	453
vPatchPieChartCountsUsePolicy	454
vPatchPolicy	454
vPatchPolicyMember	456
vPatchStatus	456
vPatchStatusByAgent	458
vPortInfo	461
vScriptLog	461
vScriptStatus	462
vSystemInfo	462
vSystemInfoManual	463
vTicketField	464
vTicketNote	464
vTicketSummary	465
vUptimeHistory	465
vvProAssetDetails	466

Database Views and Functions

System > Database Access > Database Views

The system exposes a set of **database views and database functions** (page 423) allowing clients to directly access data within the Kaseya repository. The database functions can be thought of as parameterized views. These views can be used to bring data into a spreadsheet for analysis or to prepare reports. This document describes the views and functions and gives two example applications, **Crystal Reporting** (page 420) and **Microsoft Excel** (page 419). Kaseya does not present itself as an expert in how to use Excel or Crystal. These examples are to assist in the basics of getting started. For third party product training or other questions please contact the third party tool vendor. Finally, an appendix is provided with a field-by-field description of the contents of the views and functions.

The views provided can be broken into **four groups of database views** (page 423).

- The first group provides information on all the **machines** being monitored.
- The second group provides information about the **activity and current status** of key parts of the system.
- The third group provides information on the **ticketing** system.
- The fourth group provides information on the **monitoring** alarms.

Accessing the Database Views

The database views are installed or updated whenever the **Reapply Schema** action is taken. A single database user ID, `KaseyaViews` is provided to access these views.

1. For security purposes, you must first create or change the password for the `KaseyaViews` user ID by entering the password in the System > **Database Views** page.
2. From that point forward, you can use external applications, such as Crystal Reports or Excel, to access the database views directly, using the `KaseyaViews` user ID and the password you have entered.

Excel Usage

Creating a Data Source in Windows

Microsoft Excel can access the views by setting up a data source. A data source is a core definition within Microsoft. Most Microsoft products have facilities to access data through a data source definition. Selecting the Settings option from the Start button allows the creation a data source. From the Settings option select the Control Panel. From the Control Panel next select Administrative Tools. From this menu a data source can be created.

The data source should be set up as a System DSN. From this dialog, create a source using the SQL Server driver. The set-up will require the name of the database server (usually the ComputerName), the user id (`KaseyaViews`) and password, and the database schema name (`ksubscribers`).

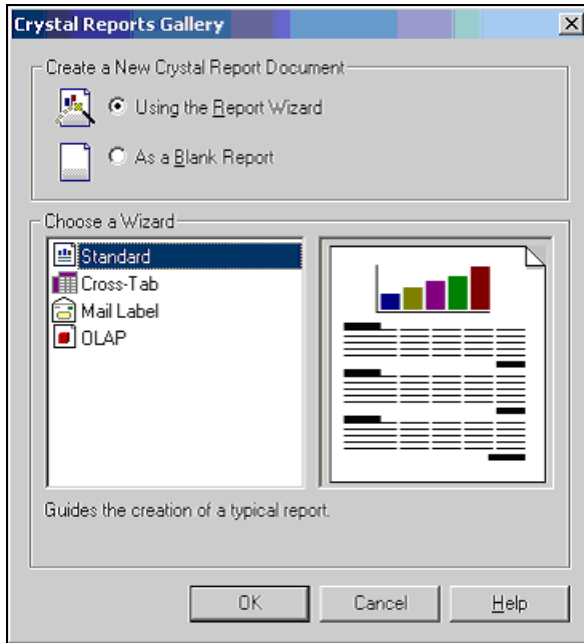
Selecting the Data Source in Excel

Once a data source is created it can be referenced by Excel. Open a blank spreadsheet and select the **Data > Get External Data > New Database Query...** option. The user is prompted for the credentials to the database. Once this completes a view can be selected. A SQL query can be constructed to bring information directly into Excel at this point.

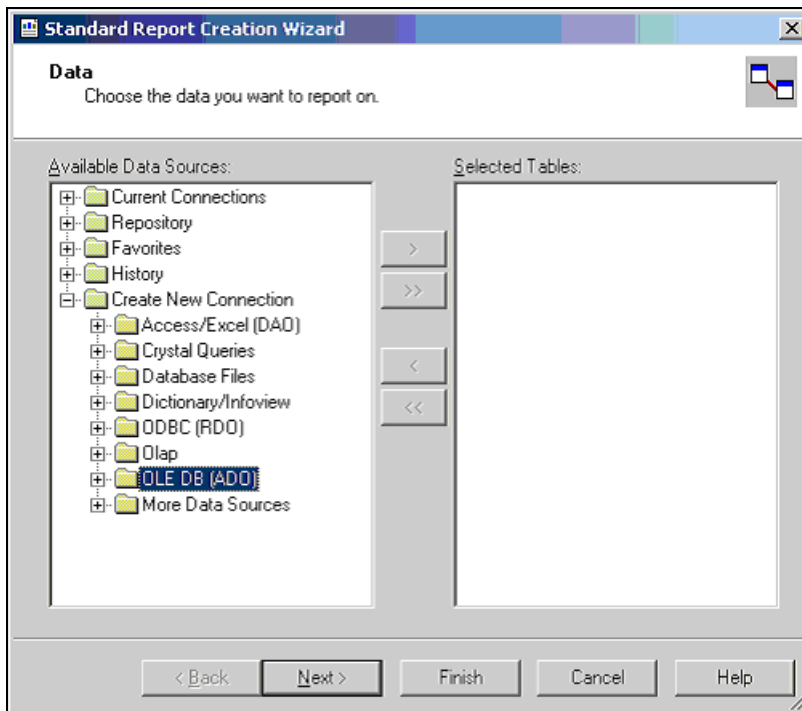
Crystal Reporting Usage

Crystal Reporting can be used to create client specified reports. Crystal 9 and 10 can be used to produce various output formats include PDF, Word and Excel. To set up a report the Crystal Report Wizard can be used. This process begins with the following dialog.

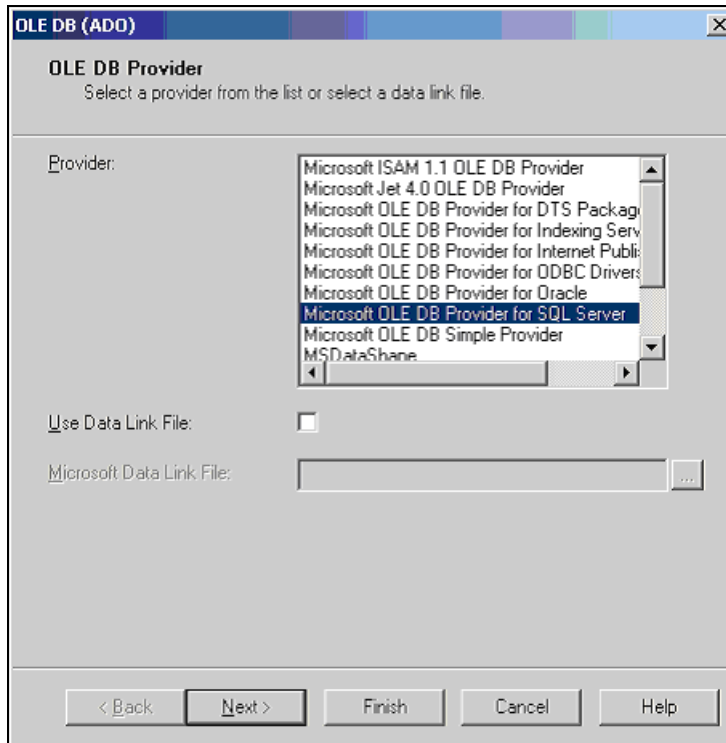
1. The client picks a report format. For this example standard will be used.



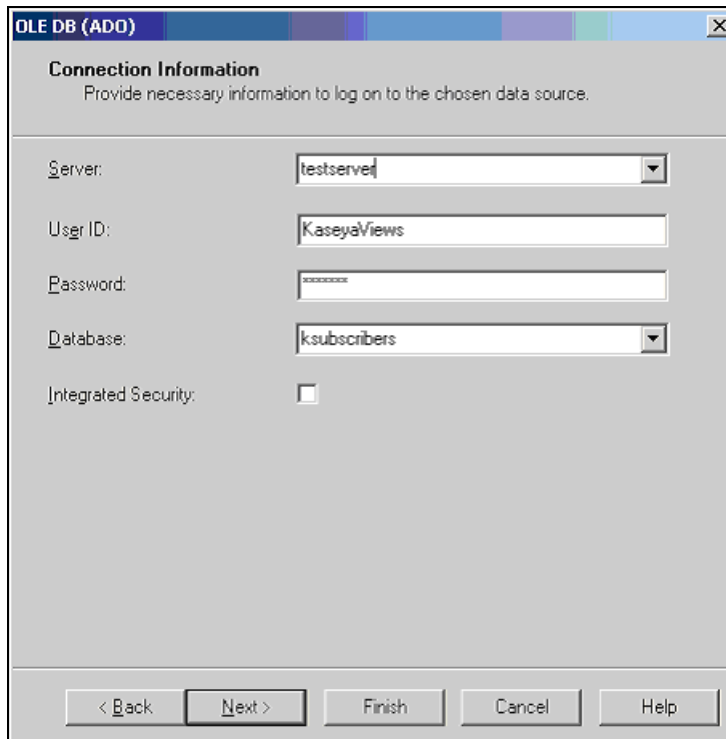
2. Next the data source is selected. This begins by picking an access method. ADO should be selected.



- Once ADO is selected the SQL Server driver can be selected. This is the correct selection to access the Kaseya database.

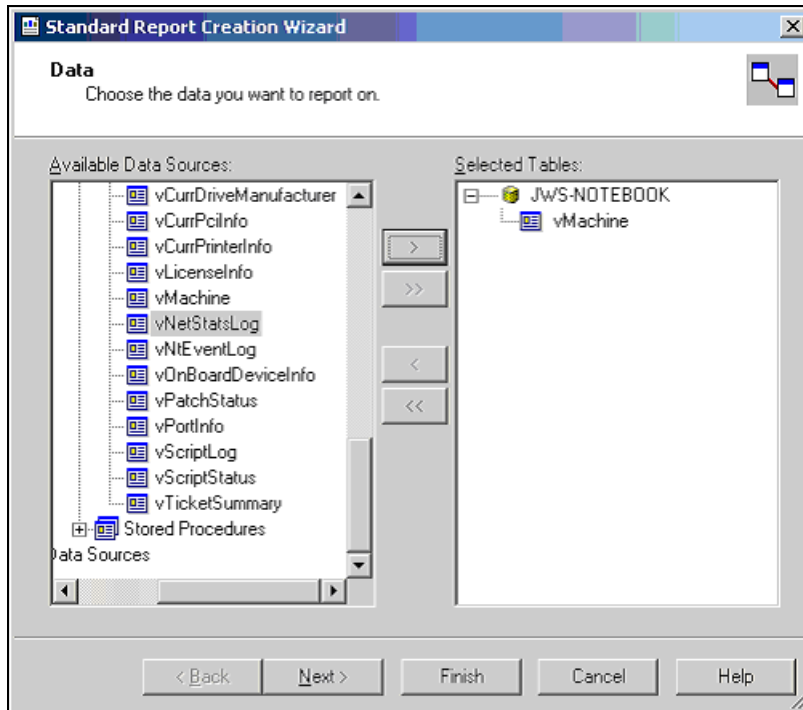


- The next step is providing the credential to make connection to the database. As shown in this dialog, the Server, User Id, Password, and Database must be provided.

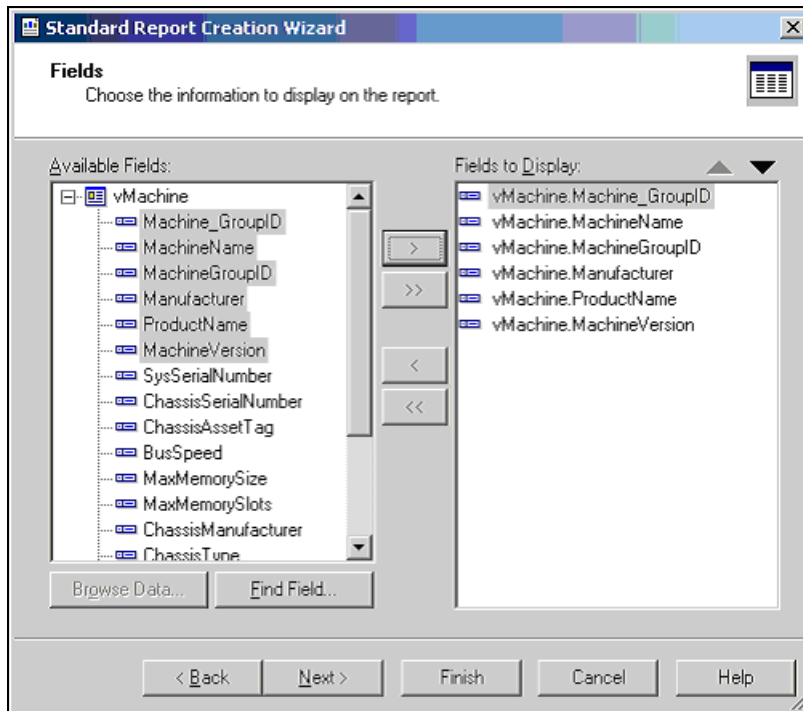


Database Views

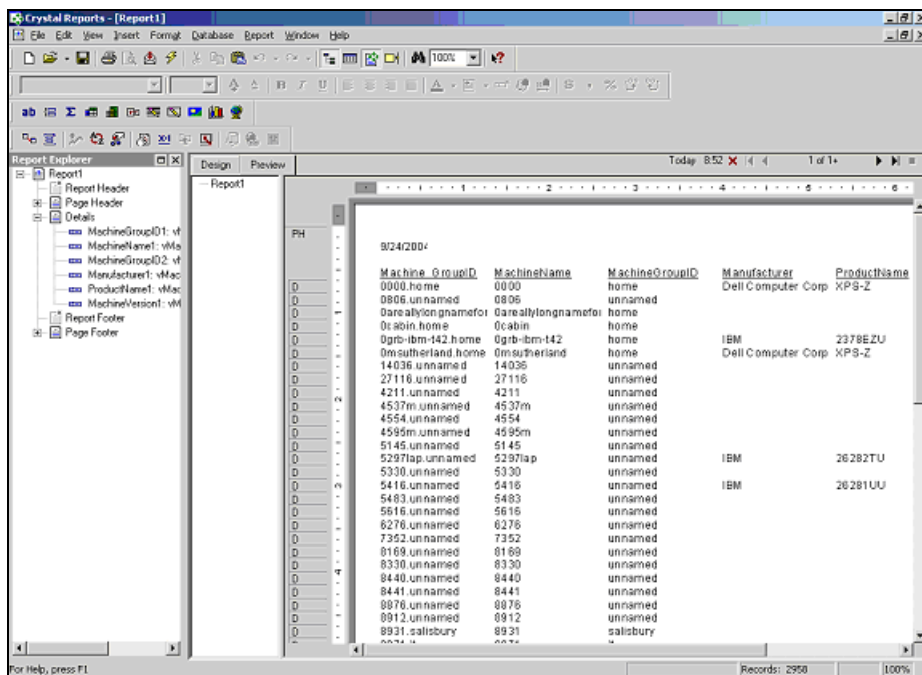
- Once the credentials are provide all the available views are displayed. Pick one or more for the report desired.



- After a view is selected the columns to be included can then be selected. Crystal provides a variety of ways to format this data. This document does not attempt to describe these options. The Crystal documentation should be reviewed for this information.





7. The resulting report can be printed or emailed to the appropriate consumers of the report. The format of the report can be designated. This facility can be used to produce a PDF or a variety of other formats.






Views and Functions Provided

Note: Views can be returned using the API web services operations [GetPublishedViews](#) (page 503), [GetPublishedViewRows](#) (page 501), and [GetPublishedViewColumns](#) (page 500).

Note: Items marked with a flag icon  are parameterized functions that are not available via the API web service operations described above. On premise users can access these flag icon  functions using SQL Server.

Machines Group	
vAddRemoveList (page 427)	Add/remove application list returned by the latest audit.
vBaseApplicationInfo (page 431)	The baseline list of applications on a client desktop machine.
vBaseCpuInfo (page 432)	The baseline list of the CPUs in a client desktop machine.
vBaseDiskInfo (page 432)	The baseline list of the disks in a client desktop machine.
vBaseDriveManufacturer (page 433)	The baseline list of the manufacturers of the disks in a client desktop machine.
vBasePciInfo (page 433)	The baseline list of the PCI cards in a client desktop machine.
vBasePrinterInfo (page 434)	The baseline list of printers in a client desktop machine.
vCollectionMember (page 434)	List the collections each machine ID belongs to (if any)
vCurrApplicationInfo (page 431)	The current list of applications on a client desktop machine.
vCurrCpuInfo (page 432)	The current list of the CPUs in a client desktop machine.
vCurrDiskInfo (page 432)	The current list of the disks in a client desktop machine.

Database Views

vCurrDriveManufacturer (page 433)	The current list of the manufacturers of the disks in a client desktop machine.
vCurrPciInfo (page 433)	The current list of the PCI cards in a client desktop machine.
vCurrPrinterInfo (page 434)	The current list of printers in a client desktop machine.
vLicenseInfo (page 439)	The licenses of applications on this machine.
vMachine (page 440)	The information known about each client desktop machine.
vOnBoardDeviceInfo (page 449)	The current list of on board devices in a client desktop machine.
vPortInf (page 461)	The current list of ports in a client desktop machine.
vSystemInfo (page 462)	Data collected by the Audit > System Info (page 134) function.
vSystemInfoManual (page 463)	Custom fields and values added to the SystemInfo function.
vUptimeHistory (page 465)	Data collected for the uptime history report. Use in conjunction with the getMachUptime web service.
vvProAssetDetails (page 466)	Lists information about a vPro enabled machine, including manufacturing details about the motherboard.
Activity / Status Group	
fnMissingPatchCounts_UsePolicy (page 425) 	Returns the number of patches, using the patch approval policies, for the specified machine group. Tabular data as seen in the missing patch pie charts in the executive summary reports and the View Dashboard page under the Home tab. Only one row is returned.
fnMissingPatchCounts_NoPolicy (page 425) 	Returns the number of patches, without using the patch approval policies, for the specified machine group. Tabular data as seen in the missing patch pie charts in the View Dashboard page under the Home tab. Only one row is returned.
fnOSCounts (page 426) 	Returns the types of operating systems and the counts for each for the specified machine group. Tabular data as seen in the OS pie charts in the executive summary reports and the View Dashboard page under the Home tab. Returns one row for each OSType.
vAdminNotesLog (page 427)	Notes each admin enters manually for a machine or group of machines. Entries in this log never expire.
vAgentConfiguration (page 427)	Lists agent specific configuration data
vAgentLabel (page 428)	Identifies the status of agents. Used for display purposes.
vAlertLog (page 429)	Logs each alert sent out via email. Multiple rows per machine.
vBackupLog (page 430)	Logs all backup related events
vConfigLog (page 435)	Log of all configuration changes. One entry per change.
vEventDetail (page 435)	Provides a description of an event.
vEventInstanceDetail (page 436)	Provides a description of an event instance that was triggered.
vEventInstanceHistoryDetail (page 438)	Provides a history of event instances that were triggered.
vNetStatsLog (page 448)	Network statistics log from the Agent.
vNtEventLog (page 448)	NT Event log data collected from each managed machine.
vPatchApprovalPolicyStatus (page 449)	The patch approval status of a patch by patch policy.
vPatchApprovalStatus (page 450)	Show the approval status of a patch. There is one row for each active patch.
vPatchPieChartCountsNoPolicy (page 453)	Provides patch counts for machines without an assign policy.
vPatchPieChartCountsUsePolicy (page 454)	Provides patch counts for machines with an assigned policy.

vPatchPolicy (page 454)	Show the approval status of a patch. There is one row for each active patch in each patch policy.
vPatchPolicyMember (page 456)	Lists all patch policies to which each machine ID is a member, if any.
vPatchStatus (page 456)	Information on the state of all patches on a per machine basis. There is one row per patch for each machine.
vPatchStatusByAgent (page 458)	Describes the patch status of an individual agent machine.
vScriptLog (page 461)	Log of procedure executions as viewed by the Kaseya Server.
vScriptStatus (page 462)	Procedure status for each client.
Ticketing Group	
vTicketSummary (page 465)	Trouble ticket summary. One row per ticket. Column names are used as the names displayed in the view summary table.
vTicketNote (page 464)	The notes associated with a ticket. Potentially multiple rows per ticket.
vTicketField (page 464)	The fields associated with a ticket. The standard fields, category, status and priority are always attached to a ticket. User fields added will also be included in this view.
Monitor Alarm Group	
vMonitorAlarmAlert (page 442)	The current list of alarms for all alerts.
vMonitorAlarmCounter (page 443)	The current list of alarms for all monitor counters.
vMonitorAlarmProcess (page 444)	The current list of alarms for all monitor processes.
vMonitorAlarmService (page 445)	The current list of alarms for all monitor services.
vMonitorAlarmSNMP (page 446)	The current list of alarms for all monitor SNMP Get objects.
vMonitorAlarmSystemCheck (page 447)	The current list of alarms for all system checks.

fnMissingPatchCounts_UsePolicy / fnMissingPatchCounts_NoPolicy

Both of these functions use the same parameters and return the same columns but each has different filtering based on patch approval policies.

fnMissingPatchCounts_UsePolicy	Returns the number of patches, using the patch approval policies, for the specified machine group. Tabular data as seen in the missing patch pie charts in the executive summary reports and the View Dashboard page under the Home tab. Only one row is returned.	
fnMissingPatchCounts_NoPolicy	Returns the number of patches, without using the patch approval policies, for the specified machine group. Tabular data as seen in the missing patch pie charts in the View Dashboard page under the Home tab. Only one row is returned.	
Parameter	Type	Purpose
@groupName	varchar	Machine group name; Use null or an empty string for all groups
@skipSubGroups	tinyint	When a group name is provided in the above parameter, determines whether to filter the results for only the one specified group or for the specified group and all of its subgroups: 0 = Use specified group and all of its subgroups 1 = Skip subgroups – use only the one specified group

Database Views

Column	Type	Purpose
GroupName	varchar	Machine group name; Returns "All Groups" when the @groupName parameter is null or an empty string
WithSubgroups	varchar	YES when @skipSubGroups = 0 and for "All Groups" NO when @skipSubGroups = 1
FullyPatched	int	Count of fully patched machines in the group specified by the parameters
Missing12	int	Count of machines missing 1-2 patches in the group specified by the parameters
Missing35	int	Count of machines missing 3-5 patches in the group specified by the parameters
MissingMore5	int	Count of machines missing 5 or more patches in the group specified by the parameters
Unscanned	int	Count of unscanned machines in the group specified by the parameters
Unsupported	int	Count of machines for which patching is not supported in the group specified by the parameters

Examples

In the examples below replace `machinegroup` with the name of the machine group you are using. If a machine group is not included then data for All Groups is returned.

```
SELECT FROM * fnMissingPatchCounts_UsePolicy('',0)
SELECT FROM * fnMissingPatchCounts_UsePolicy('machinegroup',0)
SELECT FROM * fnMissingPatchCounts_NoPolicy('',0)
SELECT FROM * fnMissingPatchCounts_NoPolicy('machinegroup',0)
```

fnOSCounts

fnOSCounts	Returns the types of operating systems and the counts for each for the specified machine group. Tabular data as seen in the OS pie charts in the executive summary reports and the View Dashboard page under the Home tab. Returns one row for each OSType.	
Parameter	Type	Purpose
@groupName	varchar	Machine group name; Use null or an empty string for all groups
@skipSubGroups	tinyint	When a group name is provided in the above parameter, determines whether to filter the results for only the one specified group or for the specified group and all of its subgroups: 0 = Use specified group and all of its subgroups 1 = Skip subgroups – use only the one specified group
Column	Type	Purpose
OSType	varchar	Operating system type such as "Win XP", "Win Vista", and "Mac OS X"
OSCount	int	Count of operating system type in the group specified by the parameters

vAddRemoveList

vAddRemoveList		
Column Name	Type	Purpose
add/remove application list returned by the latest audit		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	organization, then machine group the machine is assigned to
applicationName	varchar(260), null	App name from the add/remove programs list

vAdminNotesLog

vAdminNotesLog		
Column Name	Type	Purpose
Notes each admin enters manually for a machine or group of machines. Entries in this log never expire.		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
AdminLogin	varchar(100), not null	Admin logon name. (note: no not name this col adminName)
EventTime	datetime(3), not null	Time stamp string representing the time the action took place. Default is CURRENT_TIMESTAMP so nothing needs to be entered here.
NoteDesc	varchar(200), not null	description of the action

vAgentConfiguration

vAgentConfiguration		
Column Name	Type	Purpose
Logs each alert sent out via email. Multiple rows per machine		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.

Database Views

firstCheckin	datetime(3), null	timestamp recording the first time this agent checked into the system
lastCheckin	datetime(3), null	timestamp recording the most recent time this agent checked into the system
currentUser	varchar(100), null	login name of the currently logged in user. Blank if no one logged in at this time
lastLoginName	varchar(100), not null	login name of the last user to log into this system
workgroupDomainType	tinyint(3), not null	0 (or Null) = unknown 1 = not joined to either 2 = member of workgroup 3 = member of domain 4 = domain controller
workgroupDomainName	nvarchar(32), null	The name of the workgroup or domain
lastReboot	datetime(3), null	timestamp when this system was last rebooted
agentVersion	int(10), null	version number of agent installed on this system
contactName	varchar(100), null	User contact name assigned to this agent
contactEmail	varchar(100), null	User email address assigned to this agent
contactPhone	varchar(100), null	Contact phone number assigned to this agent
contactNotes	varchar(1000), null	Notes associated with the contact information for this agent
enableTickets	int(10), not null	0 if this user does not have access to ticketing through the user interface
enableRemoteControl	int(10), not null	0 if this user does not have access to remote control through the user interface
enableChat	int(10), not null	0 if this user does not have access to chat through the user interface
loginName	varchar(100), not null	Login Name assigned to this user (if any) to access the system user portal interface.
credentialName	varchar(100), not null	The username of the credential set for this agent (if any)
primaryKServer	varchar(111), null	address:port agent connects to for its primary Kaseya Server connection
secondaryKServer	varchar(111), null	address:port agent connects to for its secondary Kaseya Server connection
quickCheckinSecs	int(10), null	interval in seconds between quick checkins
agentTempDir	varchar(200), null	The working directory used by the agent on this system

vAgentLabel

vAgentLabel Identifies the status of agents. Used for display purposes.

Column Name	Type	Purpose
displayName	varchar(201), null	The name of the machine ID.group name.
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
agentGuidStr	varchar(26), null	A string version of agentGuid. Some languages convert the large number numeric to exponential notation. This string conversion prevents that.
online	int(10), null	0 -> offline 1 -> online 2 -> online and user has not used the mouse or keyboard for 10 minutes or more. 198 -> account suspended 199 -> agent never checked in (template account)
transitionTime	datetime(3), null	Applies when online is either 0 or 2. <ul style="list-style-type: none"> When online is 0, the time at which the Agent last checked in. When online is 2, the time when the machine was deemed idle (10 minutes after the last mouse or keyboard entry).
timezoneOffset	int(10), null	The timezone offset for the agent as compared to universal time.
currentLogin	varchar(100), null	The login name of the current user.
toolTipNotes	varchar(1000), not null	The tooltip text displayed for a machine ID.
showToolTip	tinyint(3), not null	0 -> Do not show machine ID tool tips. 1 -> Do show tool machine ID tool tips.
agntTyp	int(10), not null	0 -> windows agent 4 -> mac agent 5 -> linux agent
agentOnlineStatus	int(10), null	

vAlertLog

vAlertLog		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	Logs each alert sent out via email. Multiple rows per machine A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	organization, then machine group the machine is assigned to
EventTime	datetime(3), null	time stamp when the event was recorded

Database Views

AlertEmail	varchar(1000), null	email address to send the alert to
AlertType	int(10), null	Alerts are one of several monitor types (page 558). 1 - Admin account disabled 2 - Get File change alert 3 - New Agent checked in for the first time 4 - Application has been installed or deleted 5 - Agent Procedure failure detected 6 - NT Event Log error detected 7 - Kaseya Server stopped 8 - Protection violation detected. 9 - PCI configuration has been changed 10 - Disk drive configuration change 11 - RAM size changed. 12 - Test email sent by serverInfo.asp 13 - Scheduled report completed 14 - LAN Watch alert type 15 - agent offline 16 - low on disk space 17 - disabled remote control 18 - agent online 19 - new patch found 20 - patch path missing 21 - patch install failed 23 - Backup Alert
EmailSubject	varchar(500), null	Email subject line
EmailBody	varchar(4000), null	Email body

vBackupLog

vBackupLog		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	organization, then machine group the machine is assigned to
EventTime	datetime(3), null	time stamp when the event was recorded
description	varchar(1000), null	description of the reported task
durationSec	int(10), null	number of seconds the reported task took to complete

statusType	int(10), null	0: full volume backup 1: offsite replication (obsolete) 2: incremental volume backup 3: offsite replication suspended (obsolete) 4: offsite replication skipped because backup failed (obsolete) 5: folder full backup 6: offsite folder suspended (obsolete) 7: differential volume backup 8: folder incremental backup 9: folder differential backup 10: volume verification 11: folder verification 12: volume backup skipped because machine offline 13: folder backup skipped because machine offline 14: Informational 15: Diff or Inc ran as full vol when last full vol not found 16: Diff or Inc ran as full folder when last full folder not found 17: volume backup canceled 18: folder backup canceled 19: volume image conversion (in KBU 3.0) 20: volume synthetic full backup (in KBU 3.0) 21: folder synthetic full backup (in KBU 3.0)
result	int(10), null	0: failure 1: success 2: archive incomplete
imageSize	float(53), not null	The size of the backup.

vBaseApplicationInfo / vCurrApplicationInfo

vBaseApplicationInfo vCurrApplicationInfo	audit results for installed applications. One entry per installed application found in the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
ProductName	varchar(128), null	Product name (e.g. Microsoft Office 2000)
ProductVersion	varchar(50), null	Version (e.g. 9.0.3822)
ApplicationName	varchar(128), null	Application name (e.g. Winword.exe)

Database Views

manufacturer	varchar(128), null	Manufacturers name (e.g. Microsoft Corporation)
ApplicationDesc	varchar(512), null	Description (e.g. Microsoft Word for Windows)
LastModifiedDate	varchar(50), null	File date (e.g. 02/24/2000 17:23:44)
ApplicationSize	int(10), null	File size in bytes (e.g. 8810548)
DirectoryPath	varchar(256), null	Directory path on client desktop (e.g. C:\PROGRA~1\MICROS~4\OFFICE)

vBaseCpuInfo / vCurrCpuInfo

vBaseCpuInfo vCurrCpuInfo	audit results for the CPU in a client desktop machine. One entry per audit of a client desktop.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
CpuDesc	varchar(80), null	CPU description (e.g. Pentium III Model 8)
CpuSpeed	int(10), null	CPU speed in MHz (e.g. 601)
CpuCount	int(10), null	Number of processors (e.g. 1)
TotalRam	int(10), null	Amount of RAM in MBytes (e.g. 250)

vBaseDiskInfo / vCurrDiskInfo

vBaseDiskInfo vCurrDiskInfo	audit results for the logical disks found in a client desktop machine. One entry per logical disk from an audit of a client desktop.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
DriveLetter	varchar(100), null	Logical disk drive letter (e.g. C)

TotalSpace	int(10), null	Total MBytes on the disk (e.g. 28609 for 28.609 GB) May be null if unavailable.
UsedSpace	int(10), null	Number of MBytes used (e.g. 21406 for 21.406 GB). May be null if unavailable.
FreeSpace	int(10), null	Number of MBytes free (e.g. 21406 for 21.406 GB). May be null if unavailable.
DriveType	varchar(40), null	Fixed = hard disk Removable = floppy or other removable media CDROM Network = mapped network drive
VolumeName	varchar(100), null	Name assigned to the volume
FormatType	varchar(16), null	NTFS, FAT32, CDFS, etc.

vBaseDriveManufacturer / vCurrDriveManufacturer

vBaseDriveManufacturer vCurrDriveManufacturer	Hardware audit results for the IDE & SCSI drives manufacturer and product info found in a client desktop machine. One entry per drive from an audit of a client desktop.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
DriveManufacturer	varchar(100), null	Manufacturer name (data currently has 8 characters max)
DriveProductName	varchar(100), null	Product identification (data currently has 16 characters max)
DriveProductRevision	varchar(40), null	Product revision (data currently has 4 characters max)
DriveType	varchar(9), not null	Type of disk drive found

vBasePciInfo / vCurrPciInfo

vBasePciInfo vCurrPciInfo	Hardware audit results for the PCI cards manufacturer and product info found in a client desktop machine. One entry per PCI card from an audit of a client desktop.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
VendorName	varchar(200), null	PCI Vendor Name

Database Views

ProductName	varchar(200), null	PCI Product Name
ProductRevision	int(10), null	Product revision
PciBaseClass	int(10), null	PCI base class number
PciSubClass	int(10), null	PCI subclass number
PciBusNumber	int(10), null	PCI bus number
PciSlotNumber	int(10), null	PCI slot number

vBasePrinterInfo / vCurrPrinterInfo

vBasePrinterInfo vCurrPrinterInfo	Printer audit results for the printers found for the current user logged on to a client desktop machine. One entry per printer from an audit of a client desktop. If no user is logged in, then Agent audits the printers for the system account, typically user.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
PrinterName	varchar(100), null	Name given to the printer. Same as shown in the Control Panels printer configuration window.
PortName	varchar(100), null	Name of the port to which the printer is attached. Same as shown in the Control Panels printer configuration window.
PrinterModel	varchar(100), null	Model name is the driver name retrieved from the printer information.

vCollectionMember

vCollectionMember	Lists all collections each machine ID is a member of (if any).	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
collectionName	varchar(100), not null	Collection Name

vConfigLog

vConfigLog		
Column Name	Type	Purpose
Log of all configuration changes. One entry per change.		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Group Name used for each agent
EventTime	datetime(3), null	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year- month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
ConfigDesc	varchar(1000), null	Description of the change

vEventDetail

vEventDetail		
Column Name	Type	Purpose
Provides a description of an event.		
PartitionId	numeric(26,0), not null	Tenant identifier
EventTypeDesc	varchar(256), not null	Description
IntervalTypeDesc	varchar(50), not null	Interval type ID
EventDesc	varchar(256), not null	Description
EventEndpoint	varchar(770), not null	The endpoint name to dispatch
Data	varchar(-1), null	Data payload
DataFileSpec	varchar(200), null	File path to pass along (if any)
EffectiveDate	datetime(3), not null	Date event was first introduced
ExpirationDate	datetime(3), null	Expiration date (if any)
IntervalIncrement	int(10), null	Increment integer
CreateOwnerCalendarEntries	bit, null	If 1, create a full year's worth of scheduling information, starting from the first run date, in the Hermes.EventInstance table. If 0, do not create this scheduling instance.
NotifyOwnerOnStartAndCompletion	bit, not null	Boolean notification flag (future use)
NotifySubscribersOnCom	bit, not null	Boolean notification flag (future use)

Database Views

pletion		
OwnerUserName	varchar(50), null	User Name
OwnerCoveredPassword	varchar(50), null	Covered PW (future use)
StartNotificationNote	varchar(100), null	Notification note (future use)
CompletionNotificationNote	varchar(100), null	Completion note (future use)
SuspenseIntervalTypeID	int(10), null	Suspense interval type as specified in interval type ID table
SuspenseIntervalIncrement	int(10), null	Suspense interval increment
SuspenseExpirationEventID	int(10), null	Upon suspense expiration which event to dispatch (future use)
SuspenseExpirationNote	varchar(100), null	Suspense expiration note (future use)
ErrorEventID	int(10), null	Upon error, which event to dispatch (future use)
ErrorNote	varchar(100), null	Error note (future use)
PreparationEventID	int(10), null	(future use)
PreparationEventData	varchar(200), null	(future use)
CalendarEntriesAllowed	bit, not null	Should year? instance creation be allowed
DefaultEventEndpoint	varchar(770), not null	Default endpoint name
OwnerNotificationAllowed	bit, not null	Notification bit for owner
SubscriberNotificationAllowed	bit, not null	Notification bit for subscriber
SysMinIncrement	int(10), not null	Run count (number of times)
SysMaxIncrement	int(10), not null	Recurrence in seconds
MinIncrement	int(10), not null	Minimum increment
MaxIncrement	int(10), not null	Maximum increment
EventId	int(10), not null	Unique event type ID
Active	bit, not null	Is active bit
RunCount	int(10), null	Run count (number of times)
ScriptId	int(10), null	script ID linking to agent procedures
AgentGuid	numeric(26,0), null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
orgCalendarScheduleId	numeric(26,0), null	Associated ID in orgCalendarSchedule

vEventInstanceDetail

vEventInstanceDetail	Provides a description of an event instance that was triggered.	
Column Name	Type	Purpose
PartitionId	numeric(26,0), not null	Tenant identifier
ScheduledDate	datetime(3), not null	Date/time instance was scheduled
StartedDate	datetime(3), null	Date/time instance was started (running)
CompletedDate	datetime(3), null	Date/time instance completed running

InProcess	bit, not null	If event is running (in progress)
CompletedWithErrors	bit, not null	If completed with errors
EventTypeDesc	varchar(256), not null	Description
IntervalTypeDesc	varchar(50), not null	Interval type ID
EventDesc	varchar(256), not null	Description
EventEndpoint	varchar(770), not null	The endpoing name to dispatch
Data	varchar(-1), null	Data payload
DataFileSpec	varchar(200), null	File path to pass along (if any)
EffectiveDate	datetime(3), not null	Date event was first introduced
ExpirationDate	datetime(3), null	Expiration date (if any)
IntervalIncrement	int(10), null	Increment integer
CreateOwnerCalendarEntries	bit, null	Boolean if year? worth of instances are forward created or not
NotifyOwnerOnStartAndCompletion	bit, not null	Boolean notification flag (future use)
NotifySubscribersOnCompletion	bit, not null	Boolean notification flag (future use)
OwnerUserName	varchar(50), null	User Name
OwnerCoveredPassword	varchar(50), null	Covered PW (future use)
StartNotificationNote	varchar(100), null	Notification note (future use)
CompletionNotificationNote	varchar(100), null	Completion note (future use)
SuspenseIntervalTypeID	int(10), null	Suspense interval type as specified in interval type ID table
SuspenseIntervalIncrement	int(10), null	Suspense interval increment
SuspenseExpirationEventID	int(10), null	Upon suspense expiration which event to dispatch (future use)
SuspenseExpirationNote	varchar(100), null	Suspense expiration note (future use)
ErrorEventID	int(10), null	Upon error, which event to dispatch (future use)
ErrorNote	varchar(100), null	Error note (future use)
PreparationEventID	int(10), null	(future use)
PreparationEventData	varchar(200), null	(future use)
EventInstanceID	numeric(18,0), not null	Event instance unique ID
SuspenseDate	datetime(3), null	Event suspense date
CalendarEntriesAllowed	bit, not null	Should year? instance creation be allowed
DefaultEventEndpoint	varchar(770), not null	Default endpoint name
OwnerNotificationAllowed	bit, not null	Notification bit for owner
SubscriberNotificationAllowed	bit, not null	Notification bit for subscriber
SysMinIncrement	int(10), not null	Minimum increment
SysMaxIncrement	int(10), not null	Maximum increment

Database Views

EventId	int(10), not null	Unique event type ID
Active	bit, not null	Is active bit
ErrorMessage	varchar(500), null	Error message (if any)
InstanceData	varchar(-1), null	Data payload
ConfiguredRunCount	int(10), null	Run count (number of times)
CurrentRunCount	int(10), null	Run count (number of times)
InstanceRunCount	int(10), null	Run count (number of times)
ScriptId	int(10), null	script ID linking to agent procedures
AgentGuid	numeric(26,0), null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
powerUpIfOffline	char(1), null	If true, machine is powered up
skipIfOffline	char(1), null	If true, machine is skipped if offline
runAfterNextReboot	char(1), null	If true, run after reboot
orgCalendarScheduleId	numeric(26,0), null	Associated ID in orgCalendarSchedule

vEventInstanceHistoryDetail

vEventInstanceHistoryDetail Provides a history of event instances that were triggered.

Column Name	Type	Purpose
PartitionId	numeric(26,0), null	Tenant identifier
ScheduledDate	datetime(3), null	Date/time instance was scheduled
StartedDate	datetime(3), null	Date/time instance was started (running)
CompletedDate	datetime(3), null	Date/time instance completed running
InProcess	int(10), not null	If event is running (in progress)
CompletedWithErrors	bit, null	If completed with errors
EventTypeDesc	varchar(256), not null	Description
IntervalTypeDesc	varchar(50), not null	Interval type ID
EventDesc	varchar(256), not null	Description
EventEndpoint	varchar(770), not null	The endpoint name to dispatch
Data	varchar(-1), null	Data payload
DataFileSpec	varchar(200), null	File path to pass along (if any)
EffectiveDate	datetime(3), not null	Date event was first introduced
ExpirationDate	datetime(3), null	Expiration date (if any)
IntervalIncrement	int(10), null	Increment integer
CreateOwnerCalendarEntries	bit, null	Boolean if year? worth of instances are forward created or not
NotifyOwnerOnStartAndCompletion	bit, not null	Boolean notification flag (future use)
NotifySubscribersOnCompletion	bit, not null	Boolean notification flag (future use)
OwnerUserName	varchar(50), null	User Name
OwnerCoveredPassword	varchar(50), null	Covered password (future use)

StartNotificationNote	varchar(100), null	Notification note (future use)
CompletionNotificationNote	varchar(100), null	Completion note (future use)
SuspenseIntervalTypeID	int(10), null	Suspense interval type as specified in interval type ID table
SuspenseIntervalIncrement	int(10), null	Suspense interval increment
SuspenseExpirationEventID	int(10), null	Upon suspense expiration which event to dispatch (future use)
SuspenseExpirationNote	varchar(100), null	Suspense expiration note (future use)
ErrorEventID	int(10), null	Upon error, which event to dispatch (future use)
ErrorNote	varchar(100), null	Error note (future use)
PreparationEventID	int(10), null	(future use)
PreparationEventData	varchar(200), null	(future use)
EventInstanceID	numeric(18,0), null	Event instance unique ID
SuspenseDate	datetime(3), null	Event suspense date
CalendarEntriesAllowed	bit, not null	Should year? instance creation be allowed
DefaultEventEndpoint	varchar(770), not null	Default endpoint name
OwnerNotificationAllowed	bit, not null	Notification bit for owner
SubscriberNotificationAllowed	bit, not null	Notification bit for subscriber
SysMinIncrement	int(10), not null	Minimum increment
SysMaxIncrement	int(10), not null	Maximum increment
EventID	int(10), not null	Unique event type ID
Active	bit, not null	Is active bit
ErrorMessage	varchar(500), null	Error message (if any)
InstanceData	varchar(-1), null	Data payload
ConfiguredRunCount	int(10), null	Run count (number of times)
CurrentRunCount	int(10), null	Run count (number of times)
InstanceRunCount	int(10), null	Run count (number of times)
ScriptID	int(10), null	script ID linking to agent procedures
AgentGuid	numeric(26,0), null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
orgCalendarScheduleID	numeric(26,0), null	Associated ID in orgCalendarSchedule

vLicenseInfo

vLicenseInfo		
License information collected during audit.		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
computerName	varchar(80),	holds the computer name found in the OS

Database Views

	null	
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
Publisher	varchar(100), null	software publisher (usually in the Publisher reg value)
ProductName	varchar(100), null	Software title (usually in DisplayName value but may be the reg key title)
LicenseCode	varchar(100), null	License code (usually in the ProductID value)
ProductKey	varchar(100), null	Product key
LicenseVersion	varchar(100), null	version string returned by the scanner (if any)
InstallDate	varchar(100), null	install date string returned by the scanner (if any)
OperatingSystem	varchar(16), null	Operating system of the computer
OperatingSystemVersion	varchar(150), null	Operating system version information.
loginName	varchar(100), null	Current user logged on.
lastLoginName	varchar(100), null	Previous user logged on.

vMachine

vMachine	The information known about each client desktop machine.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	full machine name. Everything to the left of the left most decimal point is the machine name.
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
Manufacturer	varchar(100), null	Manufacturer string (type 1)
ProductName	varchar(100), null	Product Name string (type 1)
MachineVersion	varchar(100), null	Version string (type 1)
SysSerialNumber	varchar(100), null	Serial Number string (type 1)
ChassisSerialNumber	varchar(100), null	Chassis Serial Number (type 3)
ChassisAssetTag	varchar(100)	Chassis Asset Tag number (type 3)

	, null	
BusSpeed	varchar(100), null	External Bus Speed (in MHz) (type 4)
MaxMemorySize	varchar(100), null	Maximum Memory Module Size (in MB) (type 16 - Maximum Capacity or if type 16 not available, Maximum Memory Module Size type 5)
MaxMemorySlots	varchar(100), null	Number of Associated Memory Slots (Number of Memory Devices in type 16 or if type 16 not available Number of Associated Memory Slots in type 5)
ChassisManufacturer	varchar(100), null	Chassis Manufacturer (type 3)
ChassisType	varchar(100), null	Chassis Type (type 3)
ChassisVersion	varchar(100), null	Chassis Ver (type 3)
MotherboardManufacturer	varchar(100), null	Motherboard Manufacturer (type 2)
MotherboardProductCode	varchar(100), null	Motherboard Product Code (type 2)
MotherboardVersion	varchar(100), null	Motherboard Version (type 2)
MotherboardSerialNumber	varchar(100), null	Motherboard Serial Number (type 2)
ComputerName	varchar(80), null	holds the computer name found in the OS
IpAddress	varchar(20), null	IP Address of the computer in a.b.c.d notation
SubnetMask	varchar(20), null	Subnet mask in a.b.c.d notation. String is empty if data is unavailable
DefaultGateway	varchar(20), null	Default gateway IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer1	varchar(20), null	DNS server #1s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer2	varchar(20), null	DNS server #2s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer3	varchar(20), null	DNS server #3s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer4	varchar(20), null	DNS server #4s IP address in a.b.c.d notation. String is empty if data is unavailable.
DhcpEnabled	int(10), null	0 -> Data is unavailable 1 -> DHCP on client computer is enabled 2 -> Disabled
DhcpServer	varchar(20), null	DHCP servers IP address in a.b.c.d notation. String is empty if data is unavailable.
WinsEnabled	int(10), null	0 -> Data is unavailable 1 -> WINS resolution on client computer is enabled 2 -> Disabled
PrimaryWinsServer	varchar(20), null	Primary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
SecondaryWinsServer	varchar(20), null	Secondary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.

Database Views

ConnectionGatewayIp	varchar(20), null	IP Address in a.b.c.d notation obtained by the Kaseya Server as the source address of the Agent. This IP is the Agents network gateway and will be different from the IpAddress if the computer is behind NAT for example. String is empty if unavailable.
ipv6Address	varchar(40), null	The ipv6 address. Null, if no address is provided.
OsType	varchar(8), null	String contains OS type, such as NT4, 2000, NT3.51, or WIN32s. Derived from portions of MajorVersion, MinorVersion, and PlatformId.
OsInfo	varchar(150), null	String contains additional OS info, such as Build 1381 Service Pack 3. Derived from portions of BuildNumber and CsdVersion.
MajorVersion	int(10), null	Major version number from GetVersionEx() Windows function call.
MinorVersion	int(10), null	Minor version number from GetVersionEx() Windows function call. If PlatformId is Win32 for Windows, then a 0 MinorVersion indicates Windows 95. If PlatformId is Win32 for Windows, then then a MinorVersion > 0 indicates Windows 98.
MacAddr	varchar(40), null	String containing the physical address, i.e. the Media Access Control address, of the connection. A MAC address has the form of: 00-03- 47-12-65-77
LoginName	varchar(100), null	User name of the currently logged on user. This value is updated with every quick check in. The agent error log file is updated with each change.
timezoneOffset	int(10), not null	The timezone offset for the agent as compared to universal time.
agentInstGuid	varchar(40), not null	The unique portion of the path to the K2 (v6.0.0.0 and above) agent directory and to the service name as KA+vMachine.agentInstGuid.

vMonitorAlarmAlert

vMonitorAlarmAlert		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Organization, then machine group the machine is assigned to.
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	4 -> Monitor alert
EventLogType	int(10), null	Only applies to AlertType=6 (NT Event Log) 0 -> Application Event Log 1 -> System Event Log 2 -> Security Event Log

AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
AlertType	int(10), not null	Alerts are one of several monitor types (<i>page 558</i>). 1 - Admin account disabled 2 - Get File change alert 3 - New Agent checked in for the first time 4 - Application has been installed or deleted 5 - Agent Procedure failure detected 6 - NT Event Log error detected 7 - Kaseya Server stopped 8 - Protection violation detected. 9 - PCI configuration has been changed 10 - Disk drive configuration change 11 - RAM size changed. 12 - Test email sent by serverInfo.asp 13 - Scheduled report completed 14 - LAN Watch alert type 15 - agent offline 16 - low on disk space 17 - disabled remote control 18 - agent online 19 - new patch found 20 - patch path missing 21 - patch install failed 23 - Backup Alert
Message	varchar(300 0), null	Message created from alarm, email message body
AlarmSubject	varchar(500) , null	Subject of alarm and email subject
AlarmEmail	varchar(100 0), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
MonitorAlarmState	smallint(5), null	0 -> Stopped 1 -> Running
AdminName	varchar(100) , null	User who assigned monitor alert to machine

vMonitorAlarmCounter

vMonitorAlarmCounter		
Column Name	Type	Purpose
Machine_GroupID	varchar(201) , null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100) , null	Machine Name used for each agent

Database Views

GroupName	varchar(100), null	Organization, then machine group the machine is assigned to.
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	0 -> Monitor Counter
MonitorName	varchar(100), not null	Name of monitor counter object
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Message	varchar(3000), null	Message created from alarm, email message body
AlarmSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
LogValue	float(53), null	Value causing alarm
MonitorAlarmState	smallint(5), null	0 -> Stopped 1 -> Running
AdminName	varchar(100), null	User who assigned monitor counter to machine

vMonitorAlarmProcess

vMonitorAlarmProcess		Listing of all alarms created by monitor processes.
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Organization, then machine group the machine is assigned to.
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	2 -> Monitor Process
MonitorName	varchar(100), not null	Name of monitor process object
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Message	varchar(300)	Message created from alarm, email message body

	0), null	
AlarmSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
LogValue	float(53), null	Value causing alarm, below are process values:
MonitorAlarmState	smallint(5), null	0 -> Stopped 1 -> Running
AdminName	varchar(100), null	Username of the administrator.

vMonitorAlarmService

vMonitorAlarmService	Listing of all of the alarms created by monitor services.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Organization, then machine group the machine is assigned to.
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	0 -> Monitor Service
MonitorName	varchar(100), not null	Name of monitor service object
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Message	varchar(3000), null	Message created from alarm, email message body
AlarmSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
LogValue	float(53), null	Value causing alarm, below are service values: -1 -> Does not exist

Database Views

		0 -> Reserved 1 -> Stopped 2 -> Start Pending 3 -> Stop Pending 4 -> Running 5 -> Continue Pending 6 -> Pause Pending 7 -> Paused
MonitorAlarmState	smallint(5), null	0 -> Stopped 1 -> Running
AdminName	varchar(100), null	User who assigned monitor service to machine

vMonitorAlarmSNMP

vMonitorAlarmSNMP		Listing of all alarms created by monitor SNMP Get objects.
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Organization, then machine group the machine is assigned to.
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	3 -> Monitor SNMP Get
MonitorName	varchar(100), not null	Name of monitor SNMP Get object
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Message	varchar(3000), null	Message created from alarm, email message body
AlarmSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
LogValue	float(53), null	Value causing alarm, if the return value of the SNMP Object Get command is a string the value will be the the Message
SNMPName	varchar(50), null	Name returned from SNMP Device on scan

SNMPCustomName	nvarchar(100), null	Custom name for SNMP Device
MonitorAlarmState	smallint(5), null	0 -> Stopped 1 -> Running
AdminName	varchar(100), null	User who assigned monitor SNMP Get to machine

vMonitorAlarmSystemCheck

vMonitorAlarmSystemCheck		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar(100), null	Machine Name used for each agent
GroupName	varchar(100), null	Organization, then machine group the machine is assigned to.
MonitorAlarmID	int(10), not null	unique monitor alarm number
MonitorType	tinyint(3), not null	5 -> Monitor system check
SystemCheckType	int(10), null	1 -> Web Server 2 -> DNS Server 4 -> Port Connection 5 -> Ping 6 -> Custom
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trending
Parameter1	varchar(1000), null	First parameter used in system check
Parameter2	varchar(1000), null	(Optional) Second parameter used by system check
Message	varchar(3000), null	Message created from alarm, email message body
AlertSubject	varchar(500), null	Subject of alarm and email subject
AlarmEmail	varchar(1000), null	Email Address(es) alarm is sent to
EventTime	datetime(3), not null	Date and Time of alarm
TicketID	varchar(30), null	Ticket ID created from alarm
MonitorAlarmState	smallint(5), null	0 -> Stopped 1 -> Running
AdminName	varchar(100)	User who assigned of monitor counter to machine

	, null	
--	--------	--

vNetStatsLog

vNetStatsLog		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
EventTime	datetime(3), null	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year-month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
BytesRcvd	int(10), null	Number of bytes received during this statistics period
BytesSent	int(10), null	Number of bytes sent during this statistics period
ApplicationName	varchar(800), null	Application name using the network

vNtEventLog

vNtEventLog		
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
logType	int(10), null	1 -> Application Log 2 -> Security Log 3 -> System Log
eventType	int(10), null	1 -> Error 2 -> Warning 4 -> Informational 8 -> Success Audit 16 -> Failure Audit
eventTime	datetime(3), null	Time the event occurred

	null	
ApplicationName	nvarchar(200), null	event log source
EventCategory	nvarchar(200), null	event log category
eventId	int(10), null	event log event ID
username	nvarchar(200), null	event log user
computerName	nvarchar(200), null	event log computer name
EventMessage	nvarchar(2000), null	event log message

vOnBoardDeviceInfo

vOnBoardDeviceInfo	Data collected by KaSmBios.exe during an audit for on-board device information. There is one row per active slot. All information is retrieved from Type 10.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
DeviceType	varchar(100), null	Device Type
DeviceDesc	varchar(100), null	Device Description

vPatchApprovalPolicyStatus

vPatchApprovalPolicyStatus	The patch approval status of a patch by patch policy.	
Column Name	Type	Purpose
UpdateClassificationCode	smallint(5), not null	Update classification: 100 -> Security Update – Critical 101 -> Security Update – Important 102 -> Security Update – Moderate 103 -> Security Update – Low 104 -> Security Update – Unrated 110 -> Critical Update 120 -> Update Rollup 200 -> Service Pack

Database Views

		210 -> Update 220 -> Feature Pack 230 -> Tool 900 -> Unclassified 999 -> Kaseya Patch Test
UpdateClassification	varchar(43), not null	Same as UpdateClassification in string format.
Approved	int(10), null	Number of patch policies in which this patch is approved
Denied	int(10), null	Number of patch policies in which this patch is denied
Pending	int(10), null	Number of patch policies in which this patch is pending
Totals	int(10), null	Total number of patch policies in which this patch is approved, denied or pending
Product	varchar(300), null	Product to which patch is associated
Policy	varchar(100), null	Patch Policy Name
UpdateClassificationDefaultApprovalCode	smallint(5), not null	0 – Approved 1 - Denied 2 - Pending
UpdateClassificationDefaultApproval	varchar(8), not null	Approved, Pending, Denied
ProductDefaultApprovalCode	smallint(5), not null	0 – Approved 1 - Denied 2 - Pending
ProductDefaultApproval	varchar(8), not null	Approved, Pending, Denied
partitionId	numeric(26,0), not null	Tenant identifier (see partnerPartition table)

vPatchApprovalStatus

vPatchApprovalStatus		
Column Name	Type	Purpose
patchDataId	int(10), not null	Unique identifier for this patch within the database
KBArticle	varchar(12), not null	Microsoft knowledge base article number
SecurityBulletin	varchar(40), not null	Microsoft security bulleting number
Title	varchar(250), not null	Patch title

UpdateClassificationId	smallint(5), not null	Numeric representation of the patch update classification; included to make filtering easier; Values are: 100 = Critical Security Update (High Priority) 101 = Important Security Update (High Priority) 102 = Moderate Security Update (High Priority) 103 = Low Security Update (High Priority) 104 = Non-rated Security Update (High Priority) 110 = Critical Update (High Priority) 120 = Update Rollup (High Priority) 200 = Service Pack (Optional) 210 = Update (Optional) 220 = Feature Pack (Optional) 230 = Tool (Optional)
UpdateClassification	varchar(43), not null	Textual representation of the patch update classification
Product	varchar(300) , null	Product this to which this patch is associated
PublishedDate	datetime(3), null	Date that this patch was last update by Microsoft, if available
Language	varchar(30), not null	Language support for the patch
numApproved	int(10), null	Number of patch policies in which this patch is approved
numDenied	int(10), null	Number of patch policies in which this patch is denied
numPending	int(10), null	Number of patch policies in which this patch is pending approval
InstallationWarning	varchar(27), not null	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', or an empty string.
partitionId	numeric(26, 0),not null	The unique tenant partition identifier for a shared Kaseya Server and database.

vPatchConfiguration

Column Name	Type	Purpose
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineID	varchar(201) , null	The machine name, machine group and organization assigned to a machine.
Machine_GroupID	varchar(201) , null	A concatenated representation of the machine id and the group id it is associated with.
MachineName	varchar(80), null	Machine Name used for each agent
ComputerName	varchar(80), null	holds the computer name found in the OS
ReverseGroupName	varchar(100) , null	Machine group, then organization the machine is assigned to.
GroupName	varchar(100) , not null	Organization, then machine group the machine is assigned to.

Database Views

OperatingSystem	varchar(16), null	Operating system of the computer.
OSInformation	varchar(150), null	Operating system information.
CurrentUser	varchar(100), null	Currently logged on user.
LastLoggedOnUser	varchar(100), null	Previously logged on user.
PatchScanTypeSetting	int(10), not null	Type of patch scan: -1 = OS not supported for patch scans 0 = Legacy Patch Scan 1 = WUA Patch Scan (32-bit) 2 = WUA Patch Scan (64-bit)
PatchScanType	varchar(300), null	Type of patch scan description
RebootSetting	int(10), not null	Post patch installation reboot action: 0 = Reboot immediately 1 = Ask - Do nothing if user does not respond in <RebootWarnMinutes> minutes 2 = Do not reboot after update; If exists, send email to <RebootWarningEmailAddress> 3 = Ask - Reboot if user does not respond in <RebootWarnMinutes> minutes 4 = Warn user that machine will reboot in <RebootWarnMinutes> minutes 5 = Skip reboot if user logged in 6 = Reboot on <RebootDay> at <RebootTime> after install 7 = Ask to reboot every <RebootWarnMinutes> minutes
RebootAction	varchar(143), null	Post patch installation reboot action description
PreRebootScript	varchar(260), not null	scriptId of script to execute immediately before the reboot step in the Patch Reboot script
PostRebootScript	varchar(260), not null	scriptId of script to execute immediately after the patch reboot (from scriptAssignmentReboot)
RebootWarnMinutes	int(10), null	Warning wait period in minutes for RebootSetting 1,3,4,7
RebootDay	int(10), null	Day to force patch reboot for RebootSetting 6: 0 = Everyday 1 = Sunday 2 = Monday 3 = Tuesday 4 = Wednesday 5 = Thursday 6 = Friday 7 = Saturday
RebootTime	varchar(10), null	Time to force patch reboot for RebootSetting 6
RebootWarningEmailAddress	varchar(100), null	Email address to send email for post patch installation reboot for RebootSetting 2

FileSourceSetting	int(10), not null	Patch installation file source: 0 = From Internet 1 = From system server 2 = From file server
FileSourceConfig	varchar(169), not null	Patch installation file source description
UseAgentTempDirOnDriveMostFreeSpace	int(10), not null	Destination for downloaded patch file: 0 = Use configured Agent working drive/directory 1 = Use configured Agent working directory on local disk drive having most free space
DeleteAfterInstall	int(10), not null	Delete downloaded patch file after installation: 0 = Do not delete 1 = Delete
FileSourceMachineld	varchar(201), null	MachineGroup_ID for the file server for FileSourceSetting 2
FileSourceUNCPath	varchar(300), null	UNC path for the file server for FileSourceSetting 2
FileSourceLocalPath	varchar(300), null	Local machine path for the file server for FileSourceSetting 2
LanCacheName	varchar(200), null	The name of the LAN Cache.
LanCacheMachineld	varchar(201), null	The machine id of the machine hosting the LAN Cache.
LanCacheUNCPath	varchar(260), null	The UNC path to the LAN Cache.
LanCacheLocalPath	varchar(260), null	The local directory path to the LAN Cache.
UseInternetSourceAsFallback	int(10), null	If file server not accessible, fall back to use the Internet for FileSourceSetting 2
WinAutoUpdateSetting	int(10), not null	Windows Automatic Update setting 0 = Windows automatic Updates configuration set; Cannot be changed by user on the machine 1 = Windows automatic Updates disabled; Cannot be changed by user on the machine 2 = User control
WinAutoUpdateConfig	varchar(93), null	Windows Automatic Update description

vPatchPieChartCountsNoPolicy

vPatchPieChartCountsNoPolicy Provides patch counts for machines without an assign policy.

Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id to which it is associated
agentGuid	numeric(26,0), not null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
Machineld	varchar(201), null	Machine Name used for each agent

Database Views

ComputerName	varchar(80), null	holds the computer name found in the OS
ReverseGroupName	varchar(100), null	Machine group, then organization the machine is assigned to.
GroupName	varchar(100), not null	Organization, then machine group the machine is assigned to.
OperatingSystem	varchar(16), null	Operating system of the computer.
OSInformation	varchar(150), null	Operating system information
CurrentUser	varchar(100), null	Currently logged on user.
LastLoggedOnUser	varchar(100), null	Previously logged on user.
Category	varchar(26), not null	<ul style="list-style-type: none">• Not Scanned• Missing Patches: 6 or more• OS Not Supported

vPatchPieChartCountsUsePolicy

vPatchPieChartCountsUsePolicy	Provides patch counts for machines with an assigned policy.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id to which it is associated
agentGuid	numeric(26,0), not null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
Machineld	varchar(201), null	Machine Name used for each agent
ComputerName	varchar(80), null	holds the computer name found in the OS
ReverseGroupName	varchar(100), null	Machine group, then organization the machine is assigned to.
GroupName	varchar(100), not null	Organization, then machine group the machine is assigned to.
OperatingSystem	varchar(16), null	Operating system of the computer.
OSInformation	varchar(150), null	Operating system information
CurrentUser	varchar(100), null	Currently logged on user.
LastLoggedOnUser	varchar(100), null	Previously logged on user.
Category	varchar(26), not null	Not Scanned Missing Patches: 6 or more OS Not Supported

vPatchPolicy

vPatchPolicy	Show the approval status of a patch. There is one row for each active patch in each patch policy.	
Column Name	Type	Purpose
patchDataId	int(10), not null	Unique identifier for this patch within the database
Policy	varchar(100), null	Name of patch policy

KBArticle	varchar(12), not null	Microsoft knowledge base article number
SecurityBulletin	varchar(40), not null	Microsoft security bulleting number
Title	varchar(250) , not null	Patch title
UpdateClassificationId	smallint(5), not null	Numeric representation of the patch update classification; included to make filtering easier; Values are: 100 = Critical Security Update (High Priority) 101 = Important Security Update (High Priority) 102 = Moderate Security Update (High Priority) 103 = Low Security Update (High Priority) 104 = Non-rated Security Update (High Priority) 110 = Critical Update (High Priority) 120 = Update Rollup (High Priority) 200 = Service Pack (Optional) 210 = Update (Optional) 220 = Feature Pack (Optional) 230 = Tool (Optional)
UpdateClassification	varchar(43), not null	Textual representation of the patch update classification
Product	varchar(300) , null	Product this to which this patch is associated
PublishedDate	datetime(3), null	Date that this patch was last update by Microsoft, if available
Language	varchar(30), not null	Language support for the patch
ApprovalStatusId	smallint(5), not null	Numeric representation of the patch approval status; included to make filtering easier; Values are: 0 = Approved 1 = Denied 2 = Pending Approval
ApprovalStatus	varchar(16), not null	Textual representation of the patch approval status
Admin	varchar(100) , not null	Name of user that made the most recent status change ("*System*" indicates that the approval status was set by the system based upon patch policy default approval status or by KB Override)
Changed	datetime(3), not null	Timestamp of most recent approval status change
InstallationWarning	varchar(20), not null	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', or an empty string.
StatusNotes	varchar(500) , not null	Notes added by Admin concerning the patch approval status
partitionId	numeric(26, 0),not null	The unique tenant partition identifier for a shared Kaseya Server and database.

vPatchPolicyMember

vPatchPolicyMember		
Column Name	Type	Purpose
Lists all patch policies to which each machine ID is a member, if any.		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id to which it is associated
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent
MachineID	varchar(201), null	Machine Name used for each agent
ComputerName	varchar(80), null	holds the computer name found in the OS
ReverseGroupName	varchar(100), null	Machine group, then organization the machine is assigned to.
GroupName	varchar(100), not null	Organization, then machine group the machine is assigned to.
OperatingSystem	varchar(16), null	Operating system of the computer.
OSInformation	varchar(150), null	Operating system information
CurrentUser	varchar(100), null	Currently logged on user.
LastLoggedOnUser	varchar(100), null	Previously logged on user.
PolicyName	varchar(100), not null	Patch Policy Name

vPatchStatus

vPatchStatus		
Column Name	Type	Purpose
Shows the state of all patches on a per machine basis. There is one row per patch for each machine.		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineID	varchar(201), null	Machine name used for each agent.
ComputerName	varchar(80), null	holds the computer name found in the OS
ReverseGroupName	varchar(100), null	Machine group, then organization the machine is assigned to.
GroupName	varchar(100), not null	Organization, then machine group the machine is assigned to.
OperatingSystem	varchar(16), null	Operating system of the computer.
OSInformation	varchar(150)	Operating system information.

	, null	
CurrentUser	varchar(100), null	Currently logged on user.
LastLoggedOnUser	varchar(100), null	Previously logged on user.
KBArticle	varchar(10), not null	Microsoft KB article number reported from the patch scanner.
SecurityBulletin	varchar(40), not null	Bulletin ID string reported from the patch scanner.
Title	varchar(250), not null	Update title.
Product	varchar(300), not null	Product to which patch is associated
Language	varchar(30), null	Language of the product.
UpdateClassification	smallint(5), not null	Update classification: 100 -> Security Update – Critical 101 -> Security Update – Important 102 -> Security Update – Moderate 103 -> Security Update – Low 104 -> Security Update – Unrated 110 -> Critical Update 120 -> Update Rollup 200 -> Service Pack 210 -> Update 220 -> Feature Pack 230 -> Tool 900 -> Unclassified 999 -> Kaseya Patch Test
UpdateClassificationDescription	varchar(43), not null	Same as UpdateClassification in string format.
ReleaseDate	datetime(3), null	Patch release date
ApprovalStatus	smallint(5), not null	0 -> approved 1 -> disapproved 2 -> pending approval
ApprovalStatusDescription	varchar(16), not null	Same as ApprovalStatus in string format.
InstallSeparate	tinyint(3), not null	0 -> this can be installed together with other patches 1 -> this must be installed separately (its own reboot) from other patches
IsSuperseded	tinyint(3), not null	0 -> update is not superseded 1 -> update is superseded by a subsequent update
PatchAppliedFlag	int(10), not null	0 -> patch has not been applied 1 -> patch has been applied

Database Views

PatchStatus	int(10), not null	0 -> this patch not scheduled to be installed 1 -> schedule this patch for install. Flags used to bundle all patches into a single script. Set when installation scripts are generated. 2 -> patch install failed, no alert sent 3 -> patch install failed and alert has been sent 4 -> patch installed and awaiting a reboot to reconfirm 5 -> schedule rollback for this patch 6 -> "/install-as-user" patch not installed; User not logged in 7 -> Office patch not installed; User request to install declined or timed out 8 -> patch get/install failed, client login credential is invalid
PatchStatusDescription	varchar(42), not null	Same as PatchStatus is string format.
PendingManualInstall	int(10), not null	Patch selected by manual update (Machine Update or Patch Update): 0 -> not selected for installation 1 -> selected for installation
PatchIgnoreFlag	int(10), not null	0 -> process this patch 1 -> ignore this patch
InstallationWarning	varchar(22), not null	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', "Internet-based Install", or an empty string.
InstallDate	datetime(3), null	timestamp when this patch was applied by the VSA
InstalledBy	varchar(100), null	Name of admin (if we installed the patch) or value from registry (if scanner returned the value)
Description	varchar(1500), null	Patch description
UninstallNotes	varchar(1500), null	Uninstall notes for the patch
patchDataId	int, not null	Key to the patchData table.

vPatchStatusByAgent

Column Name	Type	Purpose
vPatchStatusByAgent	Describes the patch status of an individual agent machine.	
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id to which it is associated
agentGuid	numeric(26,0), not null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
MachineId	varchar(201), null	Machine Name used for each agent
ComputerName	varchar(80), null	holds the computer name found in the OS
ReverseGroupName	varchar(100), null	Machine group, then organization the machine is assigned to.
GroupName	varchar(100), not null	Organization, then machine group the machine is assigned to.
OperatingSystem	varchar(16), null	Operating system of the computer.

OSInformation	varchar(150), null	Operating system information
CurrentUser	varchar(100), null	Currently logged on user.
LastLoggedOnUser	varchar(100), null	Previously logged on user.
LastCheckinTime	datetime(3), not null	Date/time the agent last checked in.
LastRebootTime	datetime(3), null	Date/time the agent machine last rebooted.
totalPatches	int(10), not null	total patches reported for agentGuid
installed	int(10), not null	total installed patches reported for agentGuid
missingApproved	int(10), not null	total missing approved patches reported for agentGuid
missingDenied	int(10), not null	total missing denied/ignored patches reported for agentGuid
missingManual	int(10), not null	total missing approved patches that require manual installations reported for agentGuid
pending	int(10), not null	total patches that are pending installation reported for agentGuid
notReady	int(10), not null	total patches that required the user to be logged in for installation and the condition was not met reported for agentGuid
failed	int(10), not null	total patches that failed installation reported for agentGuid
rebootPending	int(10), not null	total patches whose final installation status cannot be determined until after the next reboot reported for agentGuid
initialUpdateRunning	int(10), not null	If true, initial update is running.
testStatus	int(10), null	This flag tells whether the current patch settings for this user have been tested or not. Every time the patch source path or user credential is changed, this flag gets reset. -2 – test pending -1,null – untested 0 – test passed >0 – test failed where bit 0 is set for a registry test error, bit 1 for a file test error (Credential might not have admin rights). 1 – Patch Test Failed (registry) 2 – Patch Test Failed (file) 4 – Patch Test Failed (registry and file) else – Patch file failed to install. 10000 – no exe file was downloaded 10001 – patch failed to copy from LAN server. 10002 – local credential failure 10003 – missing network credential failure 10004 – invalid network credential failure or LAN server was not available 10005 – file source configuration for this machine is invalid 10006 – invalid LAN Cache configuration or LAN Cache server was not available 61440 – exe file was downloaded but would not execute; credential might be invalid
testStatusDescription	varchar(89), not null	Description of above.
lastScanType	smallint(5), not null	Type of last patch scan; 0 -> Legacy scan 1 -> WUA scan (online) 3 -> WUA offline scan (WSUSSCN2.CAB) 4 -> Macintosh scan
lastScanTypeDescription	varchar(12), not null	Description of above.

Database Views

	null	
scanStatus	varchar(20), not null	Unscanned Patch Scanned Succeeded Undetermined
nonSupportedOS	varchar(300), not null	Null if the machine's OS is supported for patching; OS element value from patchscn.xml if the OS is not supported for patching
lastPatchScan	datetime(3), null	Date/time the last patch scan occurred
nextPatchScan	datetime(3), null	Date/time the next patch scan is scheduled
patchScanRecurrenceLabel	nvarchar(512), not null	
patchScanRecurrenceDetailsLabel	nvarchar(512), not null	
patchScanExcludeTimeRangeLabel	nvarchar(512), not null	
patchScanRecurrenceEndLabel	nvarchar(512), not null	
patchScanOfflineLabel	nvarchar(256), not null	
lastAutomaticUpdate	datetime(3), null	Date/time automatic update last occurred
nextAutomaticUpdate	datetime(3), null	Date/time automatic update is next scheduled
autoUpdateRecurrenceLabel	nvarchar(512), not null	
autoUpdateRecurrenceDetailsLabel	nvarchar(512), not null	
autoUpdateExcludeTimeRangeLabel	nvarchar(512), not null	
autoUpdateRecurrenceEndLabel	nvarchar(512), not null	
autoUpdateOfflineLabel	nvarchar(256), not null	
wuaSelfUpdateRequired	tinyint(3), not null	WUA client self-update: 0 - Unknown 1 - Required 2 - NOT Required
wuaSelfUpdateRequiredDescription	varchar(12), not null	Description of code above.
online	int(10), null	0 -> offline 1 -> online 2 -> online and user has not used the mouse or keyboard for 10 minutes or more. 198 -> account suspended 199 -> agent never checked in (template account)

vPortInfo

vPortInfo		Data collected by KaSmBios.exe during an audit on port connector information. There is one row per active slot. All information is retrieved from Type 8.
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
InternalDesc	varchar(100), null	Internal Description
ExternalDesc	varchar(100), null	External Description
ConnectionType	varchar(100), null	Connection Type
PortType	varchar(100), null	Port Type

vScriptLog

vScriptLog		Log of procedure executions as viewed by the Kaseya Server
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
EventTime	datetime(3), null	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year- month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
ScriptName	varchar(260), null	Name of procedure
ScriptDesc	varchar(1000), null	Event description
AdminName	varchar(100), null	Admin name that scheduled this procedure.

vScriptStatus

vScriptStatus		procedure status for each client
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
scriptName	varchar(260), null	Name of procedure
LastExecTime	datetime(3), null	Time stamp string representing the last time that the procedure was executed
lastExecStatus	varchar(1000), null	Status of the last execution. The string will be one of the following: <ul style="list-style-type: none"> • Procedure Summary: Success <ELSE or THEN> • Procedure Summary: Failed <ELSE or THEN> in # step String replacements: <ul style="list-style-type: none"> • <ELSE or THEN> is replaced with the respective word ELSE or THEN. • # is replaced by the number of steps that failed in the procedure. (This is not useful unless the process is allowed to continue after a failure.) • step is replaced by the work steps if the procedure failed more than 1 step.
AdminLogin	varchar(100), null	Admin name that last scheduled this procedure. (Dont name this column adminName because that is a primary key used by database migration. adminName and emailAddr should not appear in the same table.

vSystemInfo

vSystemInfo		Data collected by the System Info (page 134) function.
Column Name	Type	Purpose
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
Manufacturer	varchar(100), null	System manufacturer string
Product Name	varchar(100), null	Name or model number of the machine supplied by the manufacturer
System Version	varchar(100)	Machine version string

	, null	
System Serial Number	varchar(100) , null	Machine serial number string entered by the manufacturer
Chassis Serial Number	varchar(100) , null	Serial number string supplied by the manufacturer
Chassis Asset Tag	varchar(100) , null	Asset tag string supplied by the manufacturer
External Bus Speed	varchar(100) , null	Motherboard bus speed
Max Memory Size	varchar(100) , null	Max memory this system may be configured with
Max Memory Slots	varchar(100) , null	Max number of memory slots this system has
Chassis Manufacturer	varchar(100) , null	Name of manufacturer of the chassis
Chassis Type	varchar(100) , null	system chassis type
Chassis Version	varchar(100) , null	version string of the chassis
Motherboard Manufacturer	varchar(100) , null	Name of motherboard manufacturer
Motherboard Product	varchar(100) , null	Motherboard model name
Motherboard Version	varchar(100) , null	Motherboard version number
Motherboard Serial Num	varchar(100) , null	Motherboard serial number
Processor Family	varchar(100) , null	processor family name
Processor Manufacturer	varchar(100) , null	processor manufacturer name
Processor Version	varchar(100) , null	processor version string
CPU Max Speed	varchar(100) , null	max speed of this processor
CPU Current Speed	varchar(100) , null	configured speed of this processor

* Custom columns defined using Audit > [System Info](#) (page 134) display in the [vSystemInfoManual](#) (page 463) database view.

vSystemInfoManual

vSystemInfo	Custom fields and values added to the System Info (page 134) function.	
Column Name	Type	Purpose
Machine_GroupID	varchar(201) , null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), not null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
fieldName	nvarchar(10)	The name of the custom field.

Database Views

	0), not null	
fieldValue	varchar(100), null	The value of the custom field.

vTicketField

vTicketField	Each ticket will have a set of fields associated with it. Three of these fields are standard fields, status, priority, and category. Also, a series of user fields can be added that will also be seen in this view. Each field has a datatype. All lists are stored as integer values. The view vTicketField has the associated text for each list value.	
Column Name	Type	Purpose
TicketID	int(10), null	unique trouble ticket ID number within a single partition.
TicketLabel	varchar(50), null	The label of the field
IntegerValue	int(10), null	The value of a integer field
NumberValue	numeric(15, 4), null	The value of a number field
StringValue	varchar(500), null	The value of a string field
ListValue	varchar(50), null	The value of a list field

vTicketNote

vTicketNote	Trouble ticket notes are stored in the database. Each ticket summary can have multiple notes. There is a timestamp that identifies the order they were attached.	
Column Name	Type	Purpose
TicketID	int(10), null	unique trouble ticket ID number
author	varchar(100), null	person who wrote this note in the ticket
TicketNoteTime	datetime(3), not null	Timestamp identifying when the note was added
TicketNote	varchar(2000), not null	Contents of the ticket note
HiddenNote	int(10), not null	0 if the note is visible. 1 if the note is hidden.
partitionId	numeric(26, 0), not null	Tenant identifier.
CreationDate	datetime(3), null	The date/time the ticket was created.
DueDate	datetime(3), null	The due date of the ticket.

vTicketSummary

vTicketSummary		
Column Name	Type	Purpose
Trouble ticket summary. One row per ticket. Column names are used as the names displayed in the view summary table.		
TicketID	int(10), null	unique trouble ticket ID number
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26, 0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
TicketSummary	varchar(256), not null	summary string briefly describing the ticket
Assignee	varchar(100), null	Admin name this ticket is assigned to
CreatedBy	varchar(100), null	admin name (or machine ID if entered by user) of the person that created this ticket
CreationDate	datetime(3), null	timestamp when the ticket was created
DueDate	datetime(3), null	ticket due date
LastModifiedDate	datetime(3), null	Date of the most recent note entered for this ticket
ResolutionDate	datetime(3), null	timestamp when the ticket was closed
UserName	varchar(100), null	The name of the submitter
UserEmail	varchar(200), null	The email address of the submitter
UserPhone	varchar(100), null	The phone number of the submitter
TicketInternalId	int(10), not null	An internal unique trouble ticket ID throughout all partitions.
partitionId	numeric(26, 0), not null	The unique tenant partition identifier for a shared Kaseya Server and database.

vUptimeHistory

vUptimeHistory		
Column Name	Type	Purpose
Data collected for the uptime history report. Use in conjunction with the getMachUptime web service		
Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.

Database Views

Machine_GroupID	varchar(201), null	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric(26,0), null	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar(100), null	Machine Name used for each agent
groupName	varchar(100), null	Organization, then machine group the machine is assigned to.
eventTime	datetime(3), null	timestamp of the beginning of the time segment
duration	int(10), null	Number of seconds this time segment lasted
type	int(10), null	1 – Agent on but cannot connect to Kaseya Server 2 – Agent on and connected to Kaseya Server 3 – Agent off normally 4 – Abnormal agent termination 5 – Agent alarms suspended (do not count suspended time when computing total uptime (function getMachUptime) 6 – Suspend ended
loginName	varchar(100), null	Name of the user logged on during this time segment. (SYSTEM if no one was logged on).

vvProAssetDetails

Column Name	Type	Purpose
vvProAssetDetails	Lists information about a vPro enabled machine, including manufacturing details about the motherboard.	
agentGuid	numeric(26,0), null	Unique 26 digit random number identifying this agent. Master record stored in machNameTab.
displayName	varchar(201), null	If the vPro machine has an agent on it then the display name is the machine.GroupId of a normal agent listing. Otherwise it is blank.
hostName	varchar(255), null	name of the machine on the LAN
computerName	varchar(255), null	holds the computer name found in the OS
assetId	varchar(50), not null	the asset Id is part of the basic hardware information
computerModel	varchar(65), null	Model designation of the computer
computerManufacturer	varchar(65), null	Manufacturer of the computer
computerVersion	varchar(65), null	Version number of the computer
computerSerialNumber	varchar(65), null	Serial number of the computer
mbManufacturer	varchar(65), null	Motherboard manufacturer
mbProductName	varchar(65), null	Product name of the motherboard
mbVersion	varchar(65), null	Version number of the motherboard
mbSerialNumber	varchar(65), null	Serial number of the motherboard
mbAssetTag	varchar(65), null	Asset tag for the motherboard
mbReplaceable	tinyint(3), null	True or false if the motherboard is replaceable
biosVendor	varchar(65), null	Vendor for the BIOS
biosVersion	varchar(65), null	Version number of the BIOS

Database Views

biosReleaseDate	datetime(3), null	BIOS release date
biosSupportedFunctions	varchar(1000), null	List of BIOS supported features
ipAddress	varchar(19), null	ipAddress of the vPro machine used by power management and remote ISO boot

Chapter 12

API Web Services

In This Chapter

VSA API Web Service470
Agent Procedure API Web Service517
Monitoring API Web Service518
KSD API Web Service523

VSA API Web Service

In This Section

VSA API Web Service - Overview	470
VSA API Web Service - Operations	482

VSA API Web Service - Overview

The VSA [API Web Service](#) provides a generalized interface for a client to programmatically interface to the VSA. This API facilitates a client being able to interface a third party package. The API focuses on the following services:

- **Connect** - This service facilitates the consumer of the API to authenticate and receive a GUID to use throughout the communication. This GUID ages off similarly to how users age off.
- **Tickets** - This service provides basic facilities for the user to be notified of new tickets. This facility allows users to update fields on a ticket.
- **Alarms** - This service provides basic facilities for the user to be notified of new alarms and mark an alarms as closed.
- **Machines** - This service provides a request to collect a set of data about one or more machines.

The VSA [API Web Service](#) is based on the [Web Services Description Language \(WSDL\)](#). The WSDL displays in a browser and provides an abstract description of the data being exchanged to and from a web service. A client program connecting to a web service can read the WSDL to determine what functions are available on the server. Any special datatypes used are embedded in the WSDL file in the form of XML Schema. The client can then use SOAP to actually call one of the functions listed in the WSDL.

The following is an example of vsaWS output:

KaseyaWS

GetMachine

Returns machine detail for the submitted Machine_GroupID.

Test

The test form is only available for requests from the local machine.

SOAP 1.1

The following is a sample SOAP 1.1 request and response. The **placeholders** shown need to be replaced with actual values.

```

POST /vsaWS/kaseyaWS.asmx HTTP/1.1
Host: 192.168.214.224
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "KaseyaWS/GetMachine"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <soap:Body>
    <GetMachine xmlns="KaseyaWS">
      <req>
        <Machine_GroupID>string</Machine_GroupID>
        <SessionID>decimal</SessionID>
      </req>
    </GetMachine>
  </soap:Body>
</soap:Envelope>

```

```

HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <soap:Body>
    <GetMachineResponse xmlns="KaseyaWS">
      <GetMachineResult>
        <Machine_GroupID>string</Machine_GroupID>
        <machName>string</machName>
        <groupName>string</groupName>
        <Manufacturer>string</Manufacturer>
        <ProductName>string</ProductName>
        <MachineVersion>string</MachineVersion>
      </GetMachineResult>
    </GetMachineResponse>
  </soap:Body>
</soap:Envelope>

```

Enabling VSA API Web Service

To enable the VSA API Web Service:

- Display the System > **Configure** (page 377) page in the VSA.
- Check the **Enable VSA API Web Service** checkbox.
- Access the VSA API web service using `http://<your-KServer>/vsaWS/KaseyaWS.asmx`

Note: The **KSD API Web Service** (<http://help.kaseya.com/webhelp/EN/KSD/7000000/index.asp#5761.htm>) describes additional **Service Desk API** operations.

Special Fields

The following fields are included in the response to every request.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

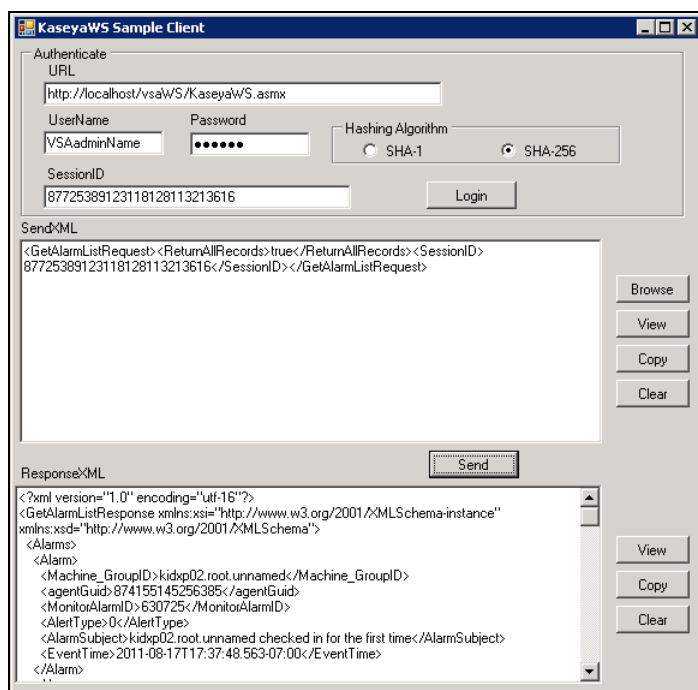
A **Session ID** is created by the web service and returned to the client the first time a method is invoked by the client. That same session ID must be returned by the client with every method invoked during the

session. The SessionID is only valid when received from the same IP address the authentication originates from.

Sample API C# Application

A GUI test client and set of test XMLs are distributed with the VSA API Web Service to help you familiarize yourself with the various API operations. The C# source code for the **Sample API C# Application** is provided to you without restriction. You can use it to see how the client was constructed and incorporate any part of its code into your own application.

Note: A Sample API ASP Page (page 474) is also provided.



To run the sample client:

1. Run the sample client located on your Kaseya Server:
`<Install Dir>\vsaWS\TestClient\KaseyaWStestClient.exe`
2. Enter the **UserName** and **Password** of a user authorized to connect with the Kaseya Server.
3. Select the **Hashing Algorithm** option to use. See **Authenticate** (page 485) for details.

Note: This is the same username and password that an administrator uses to login into the Kaseya Server.

4. Click the **Login** button to display a value in the **SessionID** field.
5. Click the **Browse** button to select a test XML file. This populates the **SendXML** textbox with the text of the XML file.

Note: You do not have to enter a value between the `<SessionID>` element tags of the test XML message. The **Sample Client** automatically inserts the displayed **SessionID** into any XML message when you click the **Send** button.

6. Click the **Send** button to send the XML message to the target URL. A response XML message displays in the **ResponseXML** textbox.

Sample API ASP Page

A test client ASP page is also distributed with the VSA API Web Service to help you familiarize yourself with the various API operations. You can use it to see how the ASP client was constructed and incorporate any part of its code into your own application. Users can browse to the actual /vsaWS/KaseyaWS.asmx page of any Kaseya Server, select a web method and copy and paste the exact XML SOAP request structure specified in the WSDL.

Authentication is in its own frame at the top of the page. The sessionID from a successful authentication is exposed and can be copied and pasted in subsequent XML requests.

Note: This page does not automatically incorporate the displayed sessionID into subsequent request statements like the [Sample API C# Application](#) (page 472) does.

Example 1: Authentication

1. Access the VSA API web service asp test client using `http://<your-KServer>/vsaWS/TestClient/TestClient.asp`
2. Enter a valid VSA administrator UserName and Password and click Login.
3. Select the **Hashing Algorithm** option to use. See [Authenticate](#) (page 485) for details.

The screenshot shows a web browser window titled "Test Client" with the address bar displaying "10.10.32.158/vsaWS/TestClient/TestClient.asp". The form contains the following fields and controls:

- Authentication** (Section Header)
- URL**:
- UserName**:
- Password**:
- Hashing Algorithm**: SHA-256 SHA-1
- Login**:
- Session ID**:

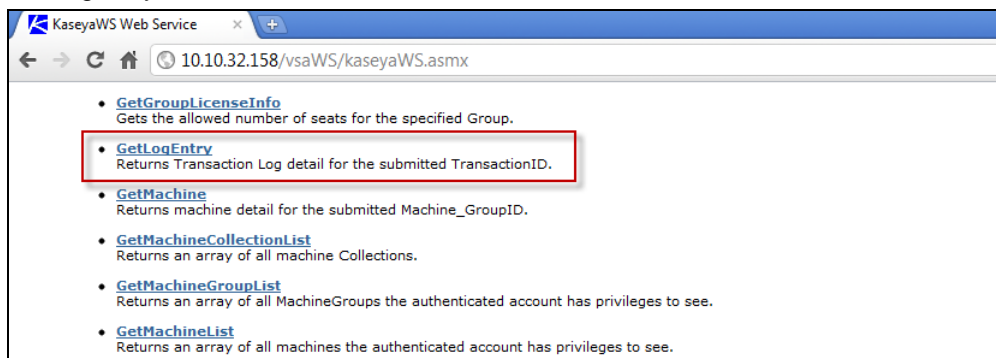
The Session ID textbox is populated with the session ID generated by your login. You will need to copy and paste this session ID into subsequent XML requests.

The screenshot shows the same web browser window after a successful login. The Session ID field is now populated with the value "75323933851132319513213616".

- Authentication** (Section Header)
- URL**:
- UserName**:
- Password**:
- Hashing Algorithm**: SHA-256 SHA-1
- Login**:
- Session ID**:

Example 2 - Creating a Get Request

1. In a second browser window, use the /vsaWS/KaseyaWS.asmx page to select a method, such as GetLogEntry.



2. Each method displays the XML SOAP structure for that method's request. Copy just the portion of the method's request structure that starts with <req> and ends with </req>.

KaseyaWS

GetLogEntry

Returns Transaction Log detail for the submitted TransactionID.

Test

The test form is only available for requests from the local machine.

SOAP 1.1

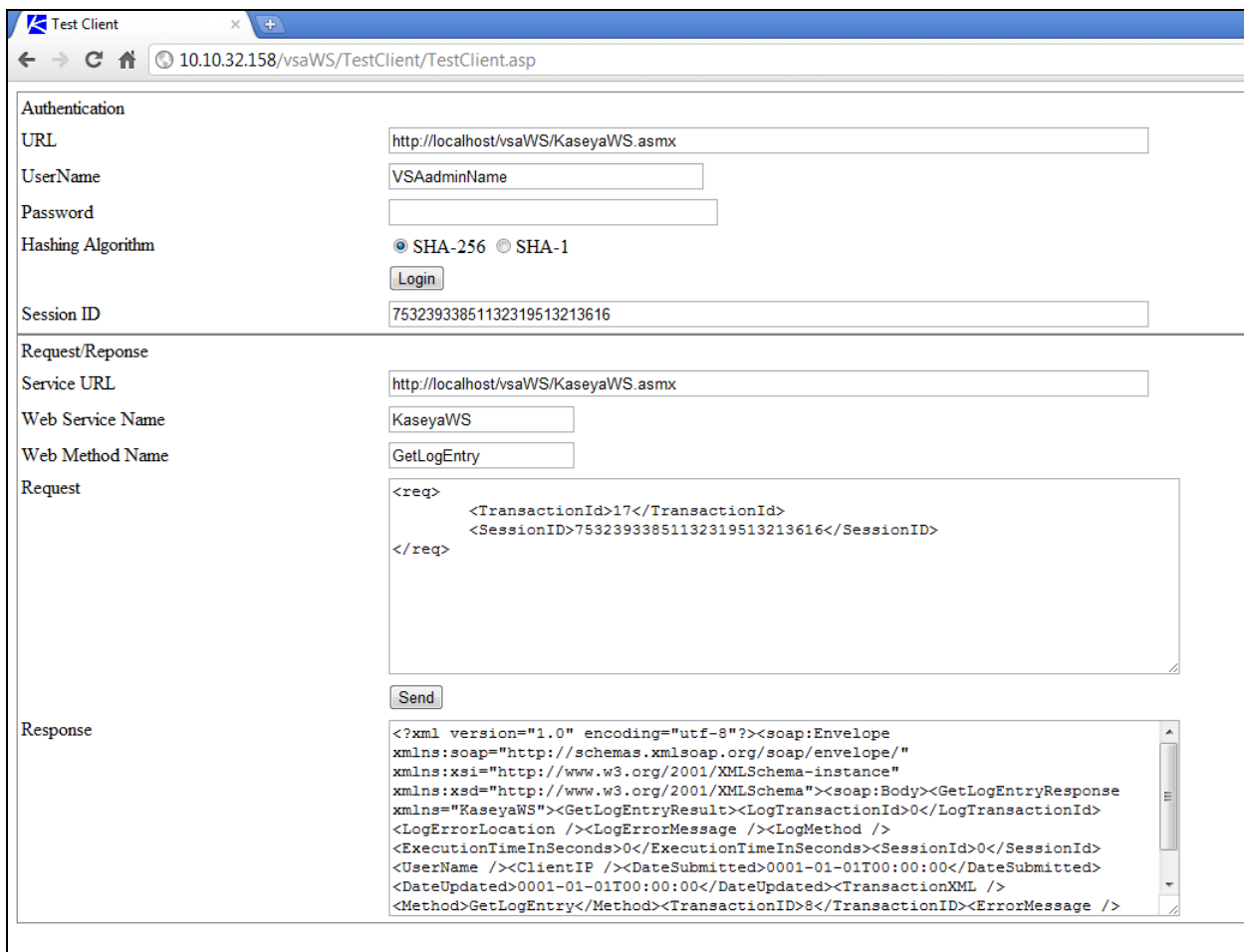
The following is a sample SOAP 1.1 request and response. The placeholders shown need to be replaced with actual values.

```
POST /vsaWS/kaseyaWS.asmx HTTP/1.1
Host: 10.10.32.158
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "KaseyaWS/GetLogEntry"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:so
<soap:Body>
  <GetLogEntry xmlns="KaseyaWS">
    <req>
      <TransactionId>decimal</TransactionId>
      <SessionID>decimal</SessionID>
    </req>
  </GetLogEntry>
</soap:Body>
</soap:Envelope>
```

- Paste the request structure into the Request pane of the TestClient.asp page. Enter the name of the method in the Web Method Name field. Replace the placeholder decimal with the sessionID string you obtained during authentication. Replace any other placeholder content with valid data as required. Then click the Send button.

Note: The `<BrowserIP>/<BrowserIP>` element in any method can be ignored. See [Limiting Requests by IP Address and User](#) (page 481) for more information.



The results display in the Response pane.

VSA API Web Service Security

General

The VSA API Web Service is accessible, by default, from any IP address in the world using any valid VSAUser credentials. In this default configuration, valid username /password combinations are considered for authentication originating from any machine.

In any configuration, the `hash.dll` provided by the VSA must be used to encrypt the password for submission. Implementation details for the `hash.dll` are contained in the sample source code provided.

Once a successful **Authentication** request issues a SessionID, this SessionID must be submitted with every service invocation, and is only valid when received from the IP address it was issued to. The issued SessionID expires after a period of inactivity.

Security can be enhanced by preparing and deploying an `AccessRules.xml` file. This file is used by the VSA API Web Service to define access rules based on the IP addresses requests are received from. IP filtering is a mechanism commonly used in business-to-business systems to ensure that requests are honored only from the partner's servers.

The `AccessRules.xml` file is divided into three sections:

- Default Access Rules
- IP Ranges
- User Mapping

Note: 127.0.0.1 (localhost) always has access for any account, regardless of configuration.

XML Structure

```
<AccessRules>
  <DefaultAccessRules>
    <GrantAnyIPToUndefinedUsers/>
    <GrantAllIPRangesToUndefinedUsers/>
    <DenyAccessToUndefinedUsers/>
  </DefaultAccessRules>
  <IPRanges>
    <IPRange RangeID="" FromIPAddress="" ToIPAddress="" RangeDescription=""/>
    <IPRange RangeID="" FromIPAddress="" ToIPAddress="" RangeDescription=""/>
  </IPRanges>
  <UserMapping>
    <User UserName="" RangeID="" GrantAllRanges="" GrantAnyIP="" DenyAccess=""/>
    <User UserName="" RangeID="" GrantAllRanges="" GrantAnyIP="" DenyAccess=""/>
  </UserMapping>
</AccessRules>
```

Default Access Rules

The elements in this section define the access rules for those accounts that are not specifically addressed in the User Mapping section.

`<GrantAnyIPToUndefinedUsers/> true/false`

true: Any user not in UserMapping gets access from any IP address.

`<GrantAllIPRangesToUndefinedUsers/> true/false`

true: Any user not in UserMapping gets access from any IP address contained in IPRanges.

`<DenyAccessToUndefinedUsers/> true/false`

true: Any user not in UserMapping denied access.

IP Ranges

This section is used to define specific machines, or ranges of machines, by IP, that are used to assign user access.

`RangeID="integer"`

API Web Services

An arbitrary, user assigned integer used to refer to the Range in UserMapping.

`FromIPAddress="string"`

Starting IP address, inclusive. First three positions of the quartet must match ToIPAddress.

`ToIPAddress=" string"`

Ending IP address, inclusive. First three positions of the quartet must match FromIPAddress.

`RangeDescription=" string"`

Description of the IP Range. For example: "Production Servers".

User Mapping

`UserName="string"`

The VSA Admin name. The VSA API Web Service uses the same credentials and password encryption as VSA. So, if you change your password in VSA, be sure to change it in your VSA API Web Service client implementation, as well.

`RangeID="integer"`

Used to point to a defined IP Range in the IP Ranges section. A user can have multiple UserMapping elements to express all the IP Ranges he has access from. Not used when one of the Grant / Deny attributes below are used.

`GrantAllRanges="true/false"`

true: User has access from any range defined in the IP Ranges section.

`GrantAnyIP=" true/false"`

true: User has access from any IP address.

`DenyAccess=" true/false"`

true: User has no access at all.

Sample Access Configuration XML

```
<AccessRules>
  <DefaultAccessRules>
    <GrantAnyIPToUndefinedUsers>>false</GrantAnyIPToUndefinedUsers>
    <GrantAllIPRangesToUndefinedUsers>>false</GrantAllIPRangesToUndefinedUsers>
    <DenyAccessToUndefinedUsers>>true</DenyAccessToUndefinedUsers>
  </DefaultAccessRules>
  <IPRanges>
    <IPRange RangeID="1" FromIPAddress="192.168.214.01" ToIPAddress="192.168.214.10"
    RangeDescription="Partner X Production Web Farm"/>
    <IPRange RangeID="2" FromIPAddress="192.168.15.102" ToIPAddress="192.168.15.102"
    RangeDescription="Senior Developer Machine"/>
    <IPRange RangeID="3" FromIPAddress="192.168.15.105" ToIPAddress="192.168.15.109"
    RangeDescription="Sales Demo Machines"/>
    <IPRange RangeID="4" FromIPAddress="192.168.210.35" ToIPAddress="192.168.210.35"
    RangeDescription="Internal QA Machine"/>
  </IPRanges>
  <UserMapping>
    <User UserName="B2BMasterAdmin" RangeID="1" GrantAllRanges="false" GrantAnyIP="false"
    DenyAccess="false"/>
    <User UserName="DevTestAccount" RangeID="2" GrantAllRanges="false" GrantAnyIP="false"
    DenyAccess="false"/>
    <User UserName="SalesTestAccount" RangeID="3" GrantAllRanges="false" GrantAnyIP="false"
    DenyAccess="false"/>
    <User UserName="SalesTestAccount2" RangeID="3" GrantAllRanges="false" GrantAnyIP="false"
    DenyAccess="false"/>
    <User UserName="QAMasterAdmin" RangeID="4" GrantAllRanges="false" GrantAnyIP="false"
    DenyAccess="false"/>
    <User UserName="SalesTravellingTestAccount" RangeID="" GrantAllRanges="false"
    GrantAnyIP="true" DenyAccess="false"/>
    <User UserName="Bob" RangeID="" GrantAllRanges="true" GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="Sally" RangeID="" GrantAllRanges="false" GrantAnyIP="false"
    DenyAccess="true"/>
  </UserMapping>
</AccessRules>
```

Web Links - Inbound and Outbound

Aside from API operations described later in the document, the Kaseya Server also supports the following inbound and outbound links:

Inbound

The URL to display the **Ticket** web page for a specific ticket ID is:

`http://...?ticipid=<TicketID>`

For example:

`http://demo.kaseya.com?ticipid=1234`

Ticket ID: 1041 Associate ticket with: mt-ws002_unnamed

Summary: mt-ws002_unnamed has 10.6% free space left

Submitter Information (Update)

Name:
 Email:
 Phone:

Date Created: 7:33:49 pm 12-Oct-07
 Age: 12 days 22 hrs
 Date Due: 7:33:49 pm 1-Nov-07

Assignee: < unassigned >
 Category: Workstation configuration
 Status: Open
 Priority: High
 SLA Type: None
 Dispatch Tech: Yes
 Approval: Not required
 Hours Worked: 0.00
 On site: Yes
 Warranty Work: Yes
 Billable: Yes
 Phone Number:
 Contact Email:
 Hardware type: Laptop
 Blood type: ab-
 Number of Siblings: 0

Enter new note Suppress email notifications

Time/Admin	Note	Hide
7:33:49 pm 12-Oct-07	D: on mt-ws002_unnamed has 2356MB free space (10.6%) on a 115718MB disk drive *Alert*	<input type="checkbox"/>

Outbound

To customize **New Ticket** links on the **Live Connect** page, fill out the `externalLink.xml` file as described in the comments section of the XML below. To activate the new ticket link, place the `externalLink.xml` file in the `\WebPages\install\` directory of your Kaseya Server.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<externalLinks>
  <!--
  URL STRING SUBSTITUTIONS: The URL string displayed is associated
  with a particular machine ID. The string is searched for the following
  case sensitive values and substituted for the values below.
  machineNameVal - the machine name for the active machine is substituted
                   in the URL string.
  groupNameVal - the group name for the active group.
  -->
  <ticketLink displayName="Ext Ticket"
  url="http://192.168.212.52/?mname=machineNameVal&gname=groupNameVal"/>
</externalLinks>
```


Chapter 13

Limiting Requests by IP Address and User

Certain operations—like `AddTicRequest` (page 484)—include an `<BrowserIP>` element in the request.

```
<BrowserIP>string</BrowserIP>
```

This element can be used to limit requests to a specified IP address range. It can also limit requests to selected users. Otherwise this element can be ignored.

To enable this feature:

1. Locate the `AccessRights.xml` file in the `<KaseyInstallationDirectory>\vsawS` directory.
2. Update the file with specified IP ranges and optionally users.
3. Move the file to `<KaseyInstallationDirectory>\vsawS\bin` directory.
4. Restart IIS.

AccessRights.xml

```
<AccessRules>
  <DefaultAccessRules>
    <GrantAnyIPToUndefinedUsers>>false</GrantAnyIPToUndefinedUsers>
    <GrantAllIPRangesToUndefinedUsers>>false</GrantAllIPRangesToUndefinedUsers>
    <DenyAccessToUndefinedUsers>>true</DenyAccessToUndefinedUsers>
  </DefaultAccessRules>
  <IPRanges>
    <IPRange RangeID="1" FromIPAddress="192.168.214.01" ToIPAddress="192.168.214.10" RangeDescription="Partner X
Production Web Farm"/>
    <IPRange RangeID="2" FromIPAddress="192.168.15.102" ToIPAddress="192.168.15.102" RangeDescription="Senior
Developer Machine"/>
    <IPRange RangeID="3" FromIPAddress="192.168.15.105" ToIPAddress="192.168.15.109" RangeDescription="Sales Demo
Machines"/>
    <IPRange RangeID="4" FromIPAddress="192.168.210.35" ToIPAddress="192.168.210.35" RangeDescription="Internal QA
Machine"/>
  </IPRanges>
  <UserMapping>
    <User UserName="B2BMasterAdmin" RangeID="1" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="DevTestAccount" RangeID="2" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="SalesTestAccount" RangeID="3" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="SalesTestAccount2" RangeID="3" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="QAMasterAdmin" RangeID="4" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="SalesTravellingTestAccount" RangeID="" GrantAllRanges="false" GrantAnyIP="true"
DenyAccess="false"/>
    <User UserName="Bob" RangeID="" GrantAllRanges="true" GrantAnyIP="false" DenyAccess="false"/>
    <User UserName="Sally" RangeID="" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="true"/>
  </UserMapping>
</AccessRules>
```

VSA API Web Service - Operations

The following operations can be performed using the [VSA API Web Service](#).

AddMachGroupToScope

Adds a machine by `GroupName` to `ScopeName`.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddOrg

Adds an organization.

A single record of the following fields is returned.

orgOutId	decimal	The organization ID of the newly added organization.
orgOutRef	string	The fully qualified name of the organization. Uses dot notation if parent or child organizations exists. Examples: <ul style="list-style-type: none"> ▪ <code>neworgname</code> ▪ <code>parentorgname.neworgname</code> ▪ <code>parentorgname.childorgname.neworgname</code>
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddOrgDepartment

Adds a department to an organization.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddOrgDeptStaff

Adds a staff member to the department of an organization.

Selected Request Fields

- **Status** - Enter 0 or leave blank. Not used by the VSA.
- **View All Tickets** - If true, the VSA user associated with this staff member can view all tickets in his or her scope as well as tickets associated with this specific staff member record. If false, this VSA

user can only view tickets associated with this specific staff member record. For more information see System > Orgs/Groups/Depts/Staff > Manage > [Manage - Staff tab](#) (page 375)

Response

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddOrgToScope

Adds an organization to a scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddScope

Adds a scope.

A single record of the following fields is returned.

scopeOutId	decimal	The identifier of the scope created.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddScopeOrg

Adds an organization and a scope in one pass and associates the organization to the scope.

A single record of the following fields is returned.

orgOutId	decimal	The identifier of the org created.
orgOutRef	string	The fully qualified name of the organization. Uses dot notation if parent or child organizations exists. Examples: <ul style="list-style-type: none"> neworgname parentorgname.neworgname parentorgname.childorgname.neworgname
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddTicRequest

Adds a provisional TicketRequest.

A single record of the following fields is returned.

newId	string	Unique identifier.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddUserToRole

Add a user to a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddUserToScope

Add a user to a scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AdminGroupAccess

Assigns a machine group to a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AssignRole

Assigns or removes a user to a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
--------	--------	---

TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AssignScope

Assigns or removes a user to a scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Authenticate

Required to begin the VSA API Web Service session. The SessionID returned must be submitted with every method invoked during session. The SessionID is only valid when received from the same machine the authentication originates from.

A single record of the following fields is returned.

SessionID	decimal	The unique session ID assigned to a user connection with the target URL.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Automatic Logon During Authentication

When you authenticate through the API, you are automatically logged into VSA as well. If you are already logged into the VSA at authentication time, the 2 sessions are synchronized. Either way, the result is the same – you end up with valid sessions in both worlds.

The VSA looks for the API's 26 digit SessionID on the query string of every VSA page. If the application redirects to a VSA page, the page displays without forcing the user to log in again. The syntax is:

URL?apiLogonGuid=12345678901234567890123456

For example:

http://someServer:123/Systemtab/SomePage?apiLogonGuid=12345678901234567890123456&SomeVar=SomeValue

API activity keeps the VSA session alive. However, since VSA does not assume there is always a need for an API session, VSA activity does not keep the API session alive.

The API uses the same timeout value as the VSA, which is maintained using the VSA's System > [Logon Policy](#) (page 391) page, and has a system default value of 30 minutes.

Hashing Algorithm

With release 6.2, K2 has adopted the SHA-256 hashing algorithm for secure authentications.

Previously the standard was SHA-1. See the [Changing Passwords Used by External Applications](#) (page 363) topic of System online help for a general introduction to this enhancement.

- A newly created or reset password is hashed using SHA-256.
- Legacy passwords that have not been reset continue to require SHA-1.
- The `HashingAlgorithm` parameter in [Authenticate](#) defaults to `SHA-1`, if left blank.

- The [Sample API C# Application](#) (page 472) and [Sample API ASP Page](#) (page 474) provide an option to switch the hashing algorithm between SHA1 and SHA-256.
- VSA passwords can only be reset using the VSA application, not by the API.

Warning: Changing a password used by a legacy external application will **disable the integration** until either the external application is updated to use the required SHA-256 hashing algorithm or a new SHA-1 credential is created and implemented. Ensure passwords used by external applications are not changed before the update is implemented. See [Creating a New SHA-1 Credential for a Legacy External Application](#) below.

Best Practices

To ensure a smooth migration from prior releases to this release, Kaseya recommends web services API client code be written or modified to attempt authentication using SHA-256 first, then SHA-1 second, in succession. This will ensure that the client code will be compatible with passwords created under current and prior versions of the VSA.

1. Set the `HashingAlgorithm` parameter in the **Authenticate** request to SHA-256. Ensure the password is hashed using SHA-256. Issue the **Authenticate** request. Check to see if a valid session ID was returned.
 - Authentication is successful if the `SessionID` parameter returns a non-zero value and the `ErrorMessage` parameter is blank.
 - Authentication is not successful if the `SessionID` parameter returns a zero value. Perform step 2.
2. Set the `HashingAlgorithm` parameter to SHA-1. Rehash the password value using SHA-1. Re-issue the **Authenticate** request. Check to see if a valid session ID was returned.

Creating a New SHA-1 Credential for a Legacy External Application

If you are running VSA v6.2 or later, and need to create an SHA-1 username and password that is compatible with a legacy external application, and that has not yet been updated to be compatible with v6.2 passwords, use one of the following procedures. You can either create a new master user and password, or reset just the password of an existing master user.

Note: You must have administrator privileges on the Kaseya Server. For security reasons, you cannot perform the following procedure remotely.

Creating a New Master User Account

1. Log in to the machine running the Kaseya Server.
2. Access the following web page:
`http://localhost/localAuth/setAccountV61.asp`
3. Enter a new account name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Enter an email address in the **Email Address**.
6. Click **Create**.

The external application can now be updated to use the new user account and SHA-1 password to connect to the VSA.

Reset the Password of an Existing Master User Account

Note: The master user account cannot be disabled.

1. Log in to the machine running the Kaseya Server.
2. Access the following web page:
`http://localhost/localAuth/setAccountV61.asp`

3. Enter an existing, enabled master account user name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Skip the **Email Address**. You cannot reset the email address of an existing user using this web page.
6. Click **Create**.

The external application can now be updated to use the new SHA-1 password to connect to the VSA.

AuthenticateWithAppSessionID

Gets API SessionID from a valid AppSession. Only available from local server.

A single record of the following fields is returned.

SessionID	decimal	The unique session ID assigned to a user connection with the target URL.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Note: See [Authenticate](#) (page 485) to initiate a new session.

CloseAlarm

Closes the alarm for the submitted MonitorAlarmID. Within the VSA user interface, alarms are closed manually using the Monitor > **Alarm Summary** (page 227) page.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

CreateAdmin

Creates a VSA user. The password must be hashed.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

CreateAgentInstallPackage

Creates an agent installation package.

Request

```
<?xml version="1.0" encoding="utf-8"?>
```

API Web Services

```
<req>
  <GroupName>string</GroupName>
  <DefaultAccount>decimal</DefaultAccount>
  <AgentType>int</AgentType>
  <CommandLineSwitches>string</CommandLineSwitches>
  <PackageName>string</PackageName>
  <PackageDescription>string</PackageDescription>
  <BrowserIP>string</BrowserIP>
  <SessionID>decimal</SessionID>
</req>
```

Where:

- **GroupName** - Name of machine group, existing or new. (step 2 in Create Package wizard)
- **DefaultAccount** - Optional. Agent guid for existing agent or template to copy setting. (step 4)
- **AgentType** - -1=Auto, 0=Windows, 4=MAC, 5=Linux (step 5)
- **CommandLineSwitches** - Self explanatory. (step 3)
- **PackageName, PackageDescription** - Self explanatory. (step 7)

Response

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

CreateMachineGroup

Creates a machine group.

A single record of the following fields is returned.

machGroupGuid	decimal	The GUID of the machine group created.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

CreateRole

Creates a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteAdmin

Deletes the specified user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteAgent

Deletes the agent on the target machine and corresponding machine ID account in the VSA.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteAgentInstallPackage

Deletes an agent install package.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteMachineGroup

Deletes the specified machine group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteOrg

Deletes the specified organization.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteRole

Deletes the specified user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteScope

Deletes the specified scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DisableAdmin

Disables a specified user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Echo

Test method for connectivity test and benchmarking. Does not require authentication. Returns the submitted string.

A single record of the following field is returned.

EchoResult	string	This value should match the input included in the request.
------------	--------	--

EchoMt

Test method for connectivity test and benchmarking into the middle-tier. Requires authentication. Returns the submitted string. Returns back (echoes) the submitted payload string.

A single record of the following fields is returned.

Payload	string	The string submitted with the request.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.

ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

EnableAdmin

Enables a specified user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetAlarm

Returns alarm detail for the submitted MonitorAlarmID.

A single record of the following fields is returned.

Machine_GroupID	string	A concatenated representation of the machine id and the group ID it is associated with
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	string	Machine Name used for each agent
GroupName	string	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	int	0 - Counter 1 - Service 2 - Process 3 - SNMP 4 - Alert - Alerts are further classified using alert types (page 550). 5 - System Check 6 - EPS 7 - Log Monitoring
AlarmType	string	0 - Alarm 1 - Trending
Message	string	Message created from alarm, email message body
AlarmSubject	string	Subject of alarm and email subject
AlarmEmail	string	Email Address(es) alarm is sent to
EventTime	string	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
AdminName	string	User who assigned monitor counter to machine
MonitorName	string	Name of monitor SNMP Get object
LogType		1 - Application Log 2 - Security Log 3 - System Log

API Web Services

EventType	int	1 - Error 2 - Warning 4 - Informational 8 - Success Audit 16 - Failure Audit
LogValue	decimal	Value causing alarm, if the return value of the SNMP Object Get command is a string the value will be the the Message
SNMPName	string	Name returned from SNMP Device on scan
SNMPCustomName	string	Custom name for SNMP Device
SystemCheckParam1	string	First parameter used in system check
SystemCheckParam2	string	(Optional) Second parameter used by system check
MonitorAlarmStateId	int	1-Open, 2-Closed
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetAlarmList

Returns an array of new alarms added since last request by default. Returns all alarms when ReturnAllRecords is set to true.

Multiple records of the following fields are returned, if applicable.

Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
MonitorAlarmID	int	unique monitor alarm number
AlertType	int	Alerts are one of several monitor types (<i>page 558</i>). 1 - Admin account disabled 2 - Get File change alert 3 - New Agent checked in for the first time 4 - Application has been installed or deleted 5 - Agent Procedure failure detected 6 - NT Event Log error detected 7 - Kaseya Server stopped 8 - Protection violation detected. 9 - PCI configuration has been changed 10 - Disk drive configuration change 11 - RAM size changed. 12 - Test email sent by serverInfo.asp 13 - Scheduled report completed 14 - LAN Watch alert type 15 - agent offline 16 - low on disk space 17 - disabled remote control 18 - agent online 19 - new patch found 20 - patch path missing 21 - patch install failed 23 - Backup Alert
AlarmSubject	string	Subject of alarm and email subject
EventTime	dateTime	Date and time of alarm

MonitorAlarmStateId	int	1-Open, 2-Closed
---------------------	-----	------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetGroupLicenseInfo

Gets the allowed number of seats for the specified group.

A single record of the following fields is returned.

MaxAgents	int	The maximum number of agents that can be installed for this machine group.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetLogEntry

Returns transaction log detail for the submitted TransactionID.

A single record of the following fields is returned.

LogTransactionId	decimal	The log transactionID.
LogErrorLocation	string	The log error location.
LogErrorMessage	string	The log error message.
LogMethod	string	The log operation that requested a response.
ExecutionTimeInSeconds	decimal	The log time required to respond to the request.
SessionId	decimal	The log session ID.
UserName	string	The log user name.
ClientIP	string	The log IP address of the client.
DateSubmitted	dateTime	The log date and time the request was submitted.
DateUpdated	dateTime	The log date and time the response was returned.
TransactionXML	string	The XML message used to submit the request.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetMachine

Returns machine detail for the submitted Machine_GroupID.

A single record of the following fields is returned.

API Web Services

Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
machName	string	full machine name. Everything to the left of the left-most decimal point is the machine name.
groupName	string	full group name for this account. Everything to the right of the left most decimal point is the group name.
Manufacturer	string	Manufacturer string (type 1)
ProductName	string	Product Name string (type 1)
MachineVersion	string	Version string (type 1)
SysSerialNumber	string	Serial Number string (type 1)
ChassisSerialNumber	string	Chassis Serial Number (type 3)
ChassisAssetTag	string	Chassis Asset Tag number (type 3)
ChassisType	string	Chassis Type (type 3)
BusSpeed	string	External Bus Speed (in MHz) (type 4)
MaxMemorySize	string	Maximum Memory Module Size (in MB) (type 16 - Maximum Capacity or if type 16 not available, Maximum Memory Module Size type 5)
MaxMemorySlots	string	Number of Associated Memory Slots (Number of Memory Devices in type 16 or if type 16 not available Number of Associated Memory Slots in type 5)
ChassisManufacturer	string	Chassis Manufacturer (type 3)
ChassisVersion	string	Chassis Ver (type 3)
MotherboardManufacturer	string	Motherboard Manufacturer (type 2)
MotherboardProductCode	string	Motherboard Product Code (type 2)
MotherboardVersion	string	Motherboard Version (type 2)
MotherboardSerialNumber	string	Motherboard Serial Number (type 2)
ComputerName	string	Name of the Computer
IpAddress	string	IP Address of the computer in a.b.c.d notation
SubnetMask	string	Subnet mask in a.b.c.d notation. String is empty if data is unavailable
DefaultGateway	string	Default gateway IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer1	string	DNS server #1s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer2	string	DNS server #2s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer3	string	DNS server #3s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer4	string	DNS server #4s IP address in a.b.c.d notation. String is empty if data is unavailable.
DhcpEnabled	int	0 -> Data is unavailable, 1 -> DHCP on client computer is enabled, 2 -> Disabled
DhcpServer	string	DHCP servers IP address in a.b.c.d notation. String is empty if data is unavailable.
WinsEnabled	string	0 -> Data is unavailable, 1 -> WINS resolution on client computer is enabled, 2 -> Disabled
PrimaryWinsServer	string	Primary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.

SecondaryWinsServer	int	Secondary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
ConnectionGatewayIp	int	IP Address in a.b.c.d notation obtained by the Kaseya Server as the source address of the Agent. This IP is the Agents network gateway and will be different from the IpAddress if the computer is behind NAT for example. String is empty if unavailable.
OsType	string	String contains OS type, such as NT4, 2000, NT3.51, or WIN32s. Derived from portions of MajorVersion, MinorVersion, and PlatformId.
OsInfo	string	String contains additional OS info, such as Build 1381 Service Pack 3. Derived from portions of BuildNumber and CsdVersion.
MajorVersion	decimal	Major version number from GetVersionEx() Windows function call.
MinorVersion	string	Minor version number from GetVersionEx() Windows function call. If PlatformId is Win32 for Windows, then a 0 MinorVersion indicates Windows 95. If PlatformId is Win32 for Windows, then then a MinorVersion > 0 indicates Windows 98.
MacAddr	string	String containing the physical address, i.e. the Media Access Control address, of the connection. A MAC address has the form of: 00-03-47-12-65-77
LoginName	string	User name of the currently logged on user. This value is updated with every quick check in. The agent error log file is updated with each change.
firstCheckin	dateTime	timestamp recording the first time this agent checked into the system
lastCheckin	dateTime	timestamp recording the most recent time this agent checked into the system
currentUser	string	login name of the currently logged in user. Blank if no one logged in at this time
lastLoginName	string	login name of the last user to log into this system
lastReboot	dateTime	timestamp when this system was last rebooted
agentVersion	int	version number of agent installed on this system
contactName	string	User contact name assigned to this agent
contactEmail	string	User email address assigned to this agent
contactPhone	string	User email address assigned to this agent
contactNotes	string	Notes associated with the contact information for this agent
enableTickets	int	0 if this user does not have access to ticketing through the user interface
enableRemoteControl	int	0 if this user does not have access to remote control through the user interface
enableChat	int	0 if this user does not have access to chat through the user interface
credentialName	string	The username of the credential set for this agent (if any)
primaryKServer	string	address:port agent connects to for its primary Kaseya Server connection
secondaryKServer	string	address:port agent connects to for its secondary Kaseya Server connection
quickCheckinSecs	int	the time to wait, in secs, before performing another agent quick check-in
agentTempDir	string	The working directory used by the agent on this system

Multiple records of the following fields are returned, if applicable.

CpuDesc	string	CPU description (e.g. Pentium III Model 8)
---------	--------	--

CpuSpeed	int	CPU speed in MHz (e.g. 601)
CpuCount	int	Number of processors (e.g. 1)
TotalRam	int	Amount of RAM in MBytes (e.g. 250)

Multiple records of the following fields are returned, if applicable.

DriveLetter	string	Logical disk drive letter (e.g. C)
TotalSpace	int	Total MBytes on the disk (e.g. 28609 for 28.609 GB) May be null if unavailable.
UsedSpace	int	Number of MBytes used (e.g. 21406 for 21.406 GB). May be null if unavailable.
FreeSpace	int	Number of MBytes free (e.g. 21406 for 21.406 GB). May be null if unavailable.
DriveType	string	Fixed = hard disk Removable = floppy or other removable media CDROM Network = mapped network drive
VolumeName	string	Name assigned to the volume
FormatType	string	NTFS, FAT32, CDFS, etc.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetMachineCollectionList

Returns an array of all machine collections. Items returned can be used as arguments on GetMachineList to filter output.

Multiple records of the following field are returned, if applicable.

collectionName	string	The name of the collection.
----------------	--------	-----------------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetMachineGroupList

Returns an array of all MachineGroups the authenticated account has privileges to see. Items returned can be used as arguments on GetMachineList to filter output.

Multiple records of the following field are returned, if applicable.

groupName	string	The machine group ID.
-----------	--------	-----------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.

ErrorLocation	string	If blank, no error was returned.
---------------	--------	----------------------------------

GetMachineList

Returns an array of all the machines that the authenticated user has access rights to see. Supports optional filtering of the return by submitted MachineGroup or MachineCollection. Multiple records of the following fields are returned, if applicable.

Multiple records of the following fields are returned, if applicable.

MachineGroupID	string	A currently existing Machine group. If this field is left blank all machines will be returned.
IpAddress	string	the IP address of the agent machine
MacAddr	string	the MAC address of the agent machine
groupName	string	Group Name used for each agent
firstCheckin	datetime	the first time an agent checks into the VSA
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetMachineUptime

Returns an array of machine uptime statistics for a submitted AgentGuid or MachineGroup or all machines when ReturnAllRecords is set to true. rptDate sets the starting sample date of the calculation to current.

All outputs are subjected to security filtering, including the agentGuid singleton and MachineGroup sub grouping. So if you submit an agentGuid or MachineGroup you do not have permissions to view, you will get nothing back.

Multiple records of the following field are returned, if applicable.

agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
machineName	string	Full machine name. Everything to the left of the left-most decimal point is the machine name.
totalOnline	int	Total seconds system was online across the measurement time.
measureTime	int	Total seconds system was measured (latest - oldest - suspend alarm times).
latestStatDate	dateTime	Latest time the system was measured, usually the last agent log entry for an offline system.
olderStatDate	dateTime	Earliest time system was measured.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetNotesList

Returns an array of new ticket notes added since last request. Generates a maximum of 500 records in date order and records the most recent note output. User can just keep executing this method until no records are returned.

- **AddedSince** - Including this date in the request overrides the system default "since last read" behavior.

Multiple records of the following fields are returned, if applicable.

TicketID	int	The ticket ID.
Author	string	The author of the note.
DateEntered	dateTime	The date the note was created or last modified.
NoteText	string	The text of the note.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetOrgLocation

Returns an organization's street address, including its longitude and latitude.

A single record of the following fields is returned.

orgId	string	Unique identifier.
orgRef	string	Unique name.
partitionId	string	Tenant identifier.
orgName	string	The name of the organization.
street	string	The street address.
city	string	The city.
usState	string	The state.
postalCode	string	The zip code.
country	string	The country.
countryCode	string	The country code.
longitude	string	The longitude of the organization location.
latitude	string	The latitude of the organization's location.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetOrgTypes

Returns machine detail for the submitted Machine_GroupID.

Multiple records of the following fields are returned.

orgTypeID	decimal	Unique identifier.
orgTypeRef	string	The unique name of the organization type.
status	int	1=Active
description	string	A description of the organization type.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetOrgs

Returns the organizations the logged on VSA user can access.

Multiple records of the following field are returned, if applicable.

orgID	string	Unique identifier.
orgName	string	The organization's name.
orgRef	string	Unique name.
CustomerID	string	Unique customer identifier.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetOrgsByScopeID

Returns the organizations a specified scope can access.

Multiple records of the following field are returned, if applicable.

orgID	string	Unique identifier.
orgName	string	The organization's name.
orgRef	string	Unique name.
CustomerID	string	Unique customer identifier.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetPackageURLs

Gets a list of all agent deploy package URLs available to the logged on user.

Multiple records of the following fields are returned, if applicable.

URL	string	The URL.
PackageName	string	The agent deploy package name.
Description	string	The description of the agent deploy package.
AgentType	string	The type of agent checking in. 0 = Windows 4 = Apple 5 = Linux

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetPartnerUserLocation

Returns the the location of a tenant-specific VSA user, including the VSA user's longitude and latitude.

A single record of the following fields is returned.

adminId	string	The VSA user's unique identifier.
adminName	string	The VSA user's name.
partitionId	string	The tenant identifier.
longitude	string	The longitude of the VSA user's location.
latitude	string	The latitude of the VSA user's location.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetPublishedViewColumns

Returns an array of all columns for a published database view.

Note: You can review documentation for available database views in [Database Views > Views Provided](#) (page 423).

Multiple records of the following fields are returned.

name	string	Name of the database view column.
dataType	string	Datatype of the database view column.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.

ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Example

Note: The following example was executed using the test page published with every installation, located at <http://localhost/vsaWS/testClient/testClient.asp>.

Request

```
<req>
  <viewName>vScriptLog</viewName>
  <SessionID>42131527423841487151422001</SessionID>
</req>
```

Response

```
<GetPublishedViewColumnsResponse>
  <GetPublishedViewColumnsResult>
    <PublishedViewColumns>
      <PublishedViewColumn>
        <name>AdminName</name>
        <dataType>varchar(100)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>agentGuid</name>
        <dataType>numeric(26,0)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>EventTime</name>
        <dataType>datetime</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>groupName</name>
        <dataType>varchar(100)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>Machine_GroupID</name>
        <dataType>varchar(201)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>machName</name>
        <dataType>varchar(100)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>ScriptDesc</name>
        <dataType>varchar(1000)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>ScriptName</name>
        <dataType>varchar(260)</dataType>
      </PublishedViewColumn>
    </PublishedViewColumns>
    <Method>GetPublishedViewColumns</Method>
    <TransactionID>3</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </GetPublishedViewColumnsResult>
</GetPublishedViewColumnsResponse>
```

GetPublishedViewRows

Returns an array of all rows for a published database view given a WHERE clause.

Note: You can review documentation for available database views in [Database Views > Views Provided](#) (page 423).

A single record of the following fields is returned.

PublishedViewRows	string	Array of row data.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Example

Note: The following example was executed using the test page published with every installation, located at <http://localhost/vsaWS/testClient/testClient.asp>.

Request

```
<req>
  <viewName>vScriptLog</viewName>
  <columnsList>AdminName,agentGuid,EventTime,Machine_GroupID,ScriptDesc,ScriptName</columnsList>
  <whereClause>EventTime > DATEADD(hour,4,getdate())</whereClause>
  <orderByList>agentGuid,EventTime</orderByList>
  <ReturnAllRows>>false</ReturnAllRows>
  <SessionID>42131527423841487151422001</SessionID>
</req>
```

SQL Equivalent

```
select top 5000 AdminName,agentGuid,EventTime,Machine_GroupID,ScriptDesc,ScriptName
from vScriptLog
where EventTime > DATEADD(hour,-4,getdate())
order by agentGuid,EventTime
```

Selects 6 of 8 available columns from `vScriptLog` where activity occurred within the past 4 hours and sorts the results by machine, then activity date.

Note: When `<ReturnAllRows>` is set false, a rowset maximum of 5000 is applied to protect the database from overly large resultsets.

Response

```
<GetPublishedViewRowsResponse>
  <GetPublishedViewRowsResult>
    <PublishedViewRows>
      <vScriptLog>
        <Row>
          <AdminName>*System*</AdminName>
          <agentGuid>517481450374694</agentGuid>
          <EventTime>20100913T09:24:1905:00</EventTime>
          <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
          <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
          <ScriptName>KES Update AVG via Internet</ScriptName>
        </Row>
        <Row>
          <AdminName>*System*</AdminName>
          <agentGuid>517481450374694</agentGuid>
          <EventTime>20100913T09:24:20.00305:00</EventTime>
          <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
          <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
          <ScriptName>KES Update</ScriptName>
        </Row>
      </vScriptLog>
    </PublishedViewRows>
  </GetPublishedViewRowsResult>
</GetPublishedViewRowsResponse>
```

```

    <Row>
      <AdminName>*System*</AdminName>
      <agentGuid>517481450374694</agentGuid>
      <EventTime>20100913T09:24:20.00705:00</EventTime>
      <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
      <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
      <ScriptName>Run Now KES Update</ScriptName>
    </Row>
  </vScriptLog>
</PublishedViewRows>
<Method>GetPublishedViewRows</Method>
<TransactionID>4</TransactionID>
<ErrorMessage/>
<ErrorLocation/>
</GetPublishedViewRowsResult>
</GetPublishedViewRowsResponse>

```

GetPublishedViews

Returns an array of all published database views.

Note: You can review documentation for available database views in [Database Views > Views Provided](#) (page 423).

Multiple records of the following fields are returned.

viewName	string	Name of the database view.
----------	--------	----------------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Example

Note: The following example was executed using the test page published with every installation, located at <http://localhost/vsaWS/testClient/testClient.asp>.

Usage details for each view in this list are published in [Database Views](#) (page 423) in the online help and the user guide. There may be more total views documented than the list published via the API.

Request

```

<req>
  <SessionID>42131527423841487151422001</SessionID>
</req>

```

Response

```

<GetPublishedViewsResponse>
  <GetPublishedViewsResult>
    <PublishedViews>
      <PublishedView>
        <viewName>vAddRemoveList</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAdminNotesLog</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAgentConfiguration</viewName>
      </PublishedView>
      <PublishedView>

```

API Web Services

```
<viewName>vAgentLabel</viewName>
</PublishedView>
<PublishedView>
  <viewName>vAlertLog</viewName>
</PublishedView>
<PublishedView>
  <viewName>vBackupLog</viewName>
</PublishedView>
<PublishedView>
  <viewName>vBaseApplicationInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vBaseCpuInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vBaseDiskInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vBaseDriveManufacturer</viewName>
</PublishedView>
<PublishedView>
  <viewName>vBasePciInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vBasePrinterInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vCollectionMember</viewName>
</PublishedView>
<PublishedView>
  <viewName>vConfigLog</viewName>
</PublishedView>
<PublishedView>
  <viewName>vCurrApplicationInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vCurrCpuInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vCurrDiskInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vCurrDriveManufacturer</viewName>
</PublishedView>
<PublishedView>
  <viewName>vCurrPciInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vCurrPrinterInfo</viewName>
</PublishedView>
<PublishedView>
  <viewName>vEventDetail</viewName>
</PublishedView>
<PublishedView>
  <viewName>vEventInstanceDetail</viewName>
</PublishedView>
<PublishedView>
  <viewName>vEventInstanceHistoryDetail</viewName>
</PublishedView>
<PublishedView>
  <viewName>vkadComputers</viewName>
</PublishedView>
<PublishedView>
  <viewName>vkadUsers</viewName>
</PublishedView>
<PublishedView>
  <viewName>vLicenseInfo</viewName>
</PublishedView>
<PublishedView>
```

```

    <viewName>vMachine</viewName>
  </PublishedView>
</PublishedView>
  <viewName>vMonitorAlarmAlert</viewName>
</PublishedView>
</PublishedView>
  <viewName>vMonitorAlarmCounter</viewName>
</PublishedView>
</PublishedView>
  <viewName>vMonitorAlarmProcess</viewName>
</PublishedView>
</PublishedView>
  <viewName>vMonitorAlarmService</viewName>
</PublishedView>
</PublishedView>
  <viewName>vMonitorAlarmSNMP</viewName>
</PublishedView>
</PublishedView>
  <viewName>vMonitorAlarmSystemCheck</viewName>
</PublishedView>
</PublishedView>
  <viewName>vNetStatsLog</viewName>
</PublishedView>
</PublishedView>
  <viewName>vNtEventLogs</viewName>
</PublishedView>
</PublishedView>
  <viewName>vOnBoardDeviceInfo</viewName>
</PublishedView>
</PublishedView>
  <viewName>vPatchApprovalStatus</viewName>
</PublishedView>
</PublishedView>
  <viewName>vPatchPolicy</viewName>
</PublishedView>
</PublishedView>
  <viewName>vPatchPolicyMember</viewName>
</PublishedView>
</PublishedView>
  <viewName>vPatchStatus</viewName>
</PublishedView>
</PublishedView>
  <viewName>vPortInfo</viewName>
</PublishedView>
</PublishedView>
  <viewName>vScriptLog</viewName>
</PublishedView>
</PublishedView>
  <viewName>vScriptStatus</viewName>
</PublishedView>
</PublishedView>
  <viewName>vSystemInfo</viewName>
</PublishedView>
</PublishedView>
  <viewName>vTicketField</viewName>
</PublishedView>
</PublishedView>
  <viewName>vTicketNote</viewName>
</PublishedView>
</PublishedView>
  <viewName>vTicketSummary</viewName>
</PublishedView>
</PublishedView>
  <viewName>vUptimeHistory</viewName>
</PublishedView>
</PublishedView>
  <viewName>vProAssetDetails</viewName>
</PublishedView>
</PublishedViews>

```

API Web Services

```
<Method>GetPublishedViews</Method>  
<TransactionID>2</TransactionID>  
<ErrorMessage/>  
<ErrorLocation/>  
</GetPublishedViewsResult>  
</GetPublishedViewsResponse>
```

GetRoles

Returns the roles the logged on VSA user can access.

Multiple records of the following field are returned, if applicable.

RoleID	string	Unique identifier
IsActive	boolean	Role is active or inactive.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetScopes

Returns the scopes the logged on VSA user can access.

Multiple records of the following field are returned, if applicable.

ScopeID	string	Unique identifier.
---------	--------	--------------------

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetSessionDetails

Gets Session details from either a submitted AppSessionID or valid API SessionID. AppSessionID variant only available from local server.

A single record of the following fields is returned.

adminId	int	VSA user identifier
partitionId	decimal	partition identifier
machineIdFil	string	session value of machine filter
activeViewId	int	session value of machine view
groupIdFil	string	session value of group filter
rowPerPage	int	session value of rows per page
startRow	int	starting position in result set
sortField	string	current data document sort field
sortOrder	int	current data document sort order
RoleId	int	role identifier

AdminRole	string	the name of the role
Scopeld	decimal	scope identifier
AdminScope	string	the name of the scope
AppSessionExpiration	dateTime	expiration of session
adminName	string	VSA user name
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetTicket

Returns ticket detail for the submitted MonitorTicketID.

TicketID	int	unique trouble ticket ID number
Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
machName	string	Machine Name used for each agent
groupName	string	Group Name used for each agent
TicketSummary	string	summary string briefly describing the ticket
Assignee	string	Admin name this ticket is assigned to
CreatedBy	string	admin name (or machine ID if entered by user) of the person that created this ticket
CreationDate	string	timestamp when the ticket was created
DueDate	string	ticket due date
LastModifiedDate	string	Date of the most recent note entered for this ticket
ResolutionDate	string	timestamp when the ticket was closed
UserName	string	The name of the submitter
UserEmail	string	The email address of the submitter
UserPhone	string	The phone number of the submitter
MonitorAlarmID	int	The identifier of the monitor alarm.

Multiple records of the following fields are returned, if applicable.

TicketLabel	string	The label of the field
IntegerValue	int	The value of a integer field
NumberValue	decimal	The value of a number field
StringValue	string	The value of a string field
ListValue	string	The value of a list field

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetTicketList

Returns an array of new tickets added since last request by default. Returns all tickets when ReturnAllRecords is set to true.

Multiple records of the following fields are returned, if applicable.

TicketID	int	unique trouble ticket ID number
Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
TicketSummary	string	summary string briefly describing the ticket

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetTicketNotes

Returns an array of notes belonging to the submitted ticket.

Multiple records of the following fields are returned, if applicable.

TicketID	int	The ticket ID.
Author	string	The author of the note.
DateEntered	dateTime	The date the note was created or last modified.
NoteText	string	The text of the note.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetTicketRequestTicket

Returns the ticketID associated with a ticket request ID.

A single record of the following fields is returned.

ticketId	string	unique identifier for ticket
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetVerboseMachineGroupList

Multiple records of the following field are returned, if applicable.

groupName	string	The machine group ID.
machGroupGuid	string	GUID of the machine group.
parentGroupGuid	string	GUID of the parent machine group, in one exists.
orgFK	string	Foreign key to the organization containing the machine group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

LockFunctionAccess

Locks function access of the submitted user role to the submitted base user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

MergeAgent

Merges an offline machine ID account with another machine ID account.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

MoveMachineToAnotherGroup

Moves machines to another group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Primitives

The following primitive Datatype operations are also provided. Each primitive operation uses the same xml contract as their corresponding multiple-columns operation. Each primitive returns a string value that requires subsequent processing.

Primitive	Result	Datatype
PrimitiveAddMachGroupToScope	PrimitiveAddMachGroupToScopeResult	string
PrimitiveAddOrg	PrimitiveAddOrgResult	string
PrimitiveAddOrgDepartment	PrimitiveAddOrgDepartment	string
PrimitiveAddOrgDeptStaff	PrimitiveAddOrgDeptStaffResult	string
PrimitiveAddOrgToScope	PrimitiveAddOrgToScopeResult	string
PrimitiveAddScope	PrimitiveAddScopeResult	string
PrimitiveAddScopeOrg	PrimitiveAddScopeOrgResult	string
PrimitiveAddTicRequest	PrimitiveAddTicRequestResult	string
PrimitiveAddUserToRole	PrimitiveAddUserToRoleResult	string
PrimitiveAddUserToScope	PrimitiveAddUserToScopeResult	string
PrimitiveAssignRole	PrimitiveAssignRoleResult	string
PrimitiveAssignScope	PrimitiveAssignScopeResult	string
PrimitiveAuthenticate	PrimitiveAuthenticateResult	string
PrimitiveCloseAlarm	PrimitiveCloseAlarmResult	string
PrimitiveCreateMachineGroup	PrimitiveCreateMachineGroupResult	string
PrimitiveCreateRole	PrimitiveCreateRoleResult	string
PrimitiveDeleteMachineGroup	PrimitiveDeleteMachineGroupResult	string
PrimitiveDeleteOrg	PrimitiveDeleteOrgResult	string
PrimitiveDeleteScope	PrimitiveDeleteScopeResult	string
PrimitiveEchoMt	PrimitiveEchoMtResult	string
PrimitiveGetAlarm	PrimitiveGetAlarmResult	string
PrimitiveGetAlarmList	PrimitiveGetAlarmResult	string
PrimitiveGetLogEntry	PrimitiveGetLogEntryResult	string
PrimitiveGetMachine	PrimitiveGetMachineResult	string
PrimitiveGetMachineCollectionList	PrimitiveGetMachineCollectionListResult	string
PrimitiveGetMachineGroupList	PrimitiveGetMachineGroupListResult	string
PrimitiveGetMachineList	PrimitiveGetMachineListResult	string
PrimitiveGetMachineUptime	PrimitiveGetMachineUptimeResult	string
PrimitiveGetNotesList	PrimitiveGetNotesListResult	string
PrimitiveGetOrgLocation	PrimitiveGetOrgLocationResult	string
PrimitiveGetOrgTypes	PrimitiveGetOrgTypesResult	string
PrimitiveGetOrgs	PrimitiveGetOrgsResult	string
PrimitiveGetOrgsByScopeID	PrimitiveGetOrgsByScopeIDResult	string
PrimitiveGetPartnerUserLocation	PrimitiveGetPartnerUserLocationResult	string
PrimitiveGetPublishedViewColumns	PrimitiveGetPublishedViewColumnsResult	string
PrimitiveGetPublishedViewRows	PrimitiveGetPublishedViewRowsResult	string

PrimitiveGetPublishedViews	PrimitiveGetPublishedViewsResult	string
PrimitiveGetRoles	PrimitiveGetRolesResult	string
PrimitiveGetScopes	PrimitiveGetScopesResult	string
PrimitiveGetTicRequestTicket	PrimitiveGetTicRequestTicketResult	string
PrimitiveGetTicket	PrimitiveGetTicketResult	string
PrimitiveGetTicketList	PrimitiveGetTicketListResult	string
PrimitiveGetTicketNotes	PrimitiveGetTicketNotesResult	string
PrimitiveGetVerboseMachineGroupList	PrimitiveGetVerboseMachineGroupListResult	string
PrimitiveMoveMachineToAnotherGroup	PrimitiveMoveMachineToAnotherGroupResult	string
PrimitiveRemoveUserFromRole	PrimitiveRemoveUserFromRoleResult	string
PrimitiveRemoveUserFromScope	PrimitiveRemoveUserFromScopeResult	string
PrimitiveRenameMachine	PrimitiveRenameMachineResult	string
PrimitiveResetPassword	PrimitiveResetPasswordResult	string
PrimitiveSetLicenseByOrg	PrimitiveSetLicenseByOrgResult	string
PrimitiveSetPartnerUserLocation	PrimitiveSetPartnerUserLocationResult	string
PrimitiveUpdateOrg	PrimitiveUpdateOrgResult	string
PrimitiveUpdateTicket	PrimitiveUpdateTicketResult	string
PrimitiveUpdateUser	PrimitiveUpdateUserResult	string

RemoveUserFromRole

Removes a VSA user from a role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

RemoveUserFromScope

Removes a VSA user from a scope.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

RenameMachine

Renames a machine and optionally assigns it to a different machine group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
--------	--------	---

API Web Services

TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

ResetPassword

Resets the specified user's password.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

RoleMembership

Assigns a user to a user role.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

SendAdminMessage

Send a message to a user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

SetAdminPassword

Resets the password for a specified user.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

SetGroupLicenseInfo

Sets the maximum number of agents allowed for a specified group.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

SetLicenseByOrg

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

SetPartnerUserLocation

Sets the current longitude and latitude of the VSA user

A single record of the following fields is returned.

AdminId	decimal	Unique identifier of the VSA user.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

UpdateOrg

Updates the information for an organization.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

UpdateTicket

Updates one or more fields of a ticket. Only fields listed on the Ticketing > [Edit Fields](#) (page 412) page can be updated.

Updating List Fields

In the example below the `Origin` field is a `List` type field with four possible values. A request passes

the name of the field, `Origin`, and a number representing the position of the value in the list, *counting from 1*. For example, the value `Phone` is in the second position in the list, so the value passed to change the `Origin` field to `Phone` is `2`.

Warning: Changing the order of field drop-down list values by re-sequencing them or by entering a new value in the middle of the list will change the value selected by the `UpdateTicket` operation. Ensure users are aware of this integration constraint before changes are made to `Edit Fields` field values.

Define ticketing fields and default values		
Field Label	Type	Default Value
Status	List	Under Investigation
Category	List	Support Request
Priority	List	2-Normal
Customer ID	String	
Forum	List	No Article Applies
Feature	List	Core - Agent Tab
Origin	List	Email
Related Tickets	String	<div style="border: 1px solid gray; padding: 2px;"> Email Phone Manually Entered Web Site < Edit List > <not resolved> </div>
Current Tier	List	
Resolution	List	

Closing a Ticket

Updating a ticket can include closing a submitted `MonitorTicketID` by updating the `Status` field with a value of `3`, which represents the third value in the `Status` field drop-down list. An example is shown below. Additional `<TicketField>` name/value elements could be added to the example below to update multiple fields.

```

<UpdateTicketRequest>
  <TicketID>1</TicketID>
  <TicketFields>
    <TicketField>
      <Name>Status</Name>
      <Value>3</Value>
    </TicketField>
  </TicketFields>
  <SessionID>13642146236194247244181221</SessionID>
</UpdateTicketRequest>
    
```

Updating Other Types of Fields

The following other types of ticket fields can be updated:

- `String` - Can contain any text up to 500 characters in length. Best used to hold things like problem location or other variables that do not belong in the summary line.
- `Integer` - Can contain any positive or negative integer value.
- `Number (nn.d)` - A number that always shows one digit to the right of the decimal point.
- `Number (nn.dd)` - A number that always shows two digits to the right of the decimal point.
- `Number (nn.ddd)` - A number that always shows three digits to the right of the decimal point.
- `Number (nn.dddd)` - A number that always shows four digits to the right of the decimal point.
- `AddNote` - Adds a plain text note to the specified ticket.
- `HideNote` - Sets hidden property to the note being added.

Fields being modified by the fields array write a hidden audit note to the ticket specified with field name, old value and new value. For example, `~API~ [CR] Status has changed from Open to Closed.`

Returned Fields

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Ticket Attachments

The API Web Service cannot be used to get or update ticket file attachments. Ticket file attachments are typically located in C:\Kaseya\WebPages\ManagedFiles directory of the Kaseya Server. API developers are responsible for writing code to place attachment files in this directory before making Web Service API calls that reference these attachments.

UpdateUser

Updates user information.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Hashing Algorithm

With release 6.2, K2 has adopted the SHA-256 hashing algorithm for secure authentications. Previously the standard was SHA-1. See the [Changing Passwords Used by External Applications](#) (page 363) topic of System online help for a general introduction to this enhancement.

- A newly created or reset password is hashed using SHA-256.
- Legacy passwords that have not been reset continue to require SHA-1.
- The HashingAlgorithm parameter in [Authenticate](#) defaults to SHA-1, if left blank.
- The [Sample API C# Application](#) (page 472) and [Sample API ASP Page](#) (page 474) provide an option to switch the hashing algorithm between SHA1 and SHA-256.
- VSA passwords can only be reset using the VSA application, not by the API.

Warning: Changing a password used by a legacy external application will [disable the integration](#) until either the external application is updated to use the required SHA-256 hashing algorithm or a new SHA-1 credential is created and implemented. Ensure passwords used by external applications are not changed before the update is implemented. See [Creating a New SHA-1 Credential for a Legacy External Application](#) below.

Best Practices

To ensure a smooth migration from prior releases to this release, Kaseya recommends web services API client code be written or modified to attempt authentication using SHA-256 first, then SHA-1 second, in succession. This will ensure that the client code will be compatible with passwords created under current and prior versions of the VSA.

1. Set the HashingAlgorithm parameter in the [Authenticate](#) request to SHA-256. Ensure the password is hashed using SHA-256. Issue the [Authenticate](#) request. Check to see if a valid session ID was returned.
 - Authentication is successful if the SessionID parameter returns a non-zero value and the ErrorMessage parameter is blank.

API Web Services

- Authentication is not successful if the `SessionID` parameter returns a zero value. Perform step 2.
- 2. Set the `HashingAlgorithm` parameter to `SHA-1`. Rehash the password value using `SHA-1`. Re-issue the `Authenticate` request. Check to see if a valid session ID was returned.

Agent Procedure API Web Service

In This Section

Enabling the Agent Procedure API Web Service	517
Agent Procedure API Web Service - Operations	517

Enabling the Agent Procedure API Web Service

See the [VSA API Web Service](#) (page 470) online help or user guide for a general introduction to the Kaseya API.

To enable the Agent Procedure API Web Service:

- Display the System > **Configure** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#248.htm>) page in the VSA.
- Check the **Enable VSA API Web Service** checkbox.
- Access the Agent Procedure API web service using <http://<your-KServer>/vsawS/AgentProcwS.asmx>

Agent Procedure API Web Service - Operations

The following operations can be performed using the [Agent Procedure API Web Service](#).

AddScriptAssignment

Adds a scriptAssignment row to perform a RunNow script execution. The authenticated user must have view access to the script and the current role must be allowed the Enable Scheduling function.

A single record of the following field is returned.

ScriptAssignmentId	int	A unique identifier for a row in the scriptAssignmentTable, representing the combination of an agentGUID and a scriptID.
--------------------	-----	--

AddScriptPrompt

Adds agent procedure prompt variables to an agent procedure. Scripts that prompt for variables at schedule time store the values in a table. These variables are unique for each scheduled instance of the script (not the script). This allows different people to schedule the same script using different variable values. The authenticated user must have view access to the agent procedure to which prompts are being added.

A single record of the following field is returned.

AddScriptPromptResult		There is no response other than an error message, if applicable.
-----------------------	--	--

Echo

Test Method for connectivity test and benchmarking. Does not require Authentication. Returns the submitted string.

A single record of the following field is returned.

Echo	string	This value should match the input included in the request.
------	--------	--

EchoMt

Test method for connectivity test and benchmarking into the middle-tier. Requires authentication. Returns the submitted string. Returns back (echoes) the submitted payload string.

A single record of the following fields is returned.

Payload	string	The string submitted with the request.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetScriptAssignmentId

Gets the scriptAssignmentId for a scriptId/agentGuid combination.

A single record of the following field is returned.

ScriptAssignmentId	int	A unique identifier for a row in the scriptAssignmentTable, representing the combination of an agentGUID and a scriptID.
--------------------	-----	--

GetScriptIdFromScriptName

Returns an array of script objects with basic information about all scripts with the requests name. Only scripts with view access for the authenticated user are returned.

A single record of the following fields are returned.

ScriptId	int	Unique identifier of the script.
ScriptName	string	Name of the script.
TreePath	string	Location of the script in the folder tree.

Monitoring API Web Service

In This Section

Enabling the Monitoring API Web Service	518
Monitoring API Web Service - Operations.....	519

Enabling the Monitoring API Web Service

See the [VSA API Web Service](#) (page 470) online help or user guide for a general introduction to the Kaseya API.

To enable the Monitoring API Web Service:

- Display the System > **Configure** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#248.htm>) page in the VSA.

- Check the [Enable VSA API Web Service](#) checkbox.
- Access the Monitoring API web service using `http://<your-KServer>/vsawS/monitoringWS.asmx`

Monitoring API Web Service - Operations

The following operations can be performed using the [Monitoring API Web Service](#).

AssignEventAlertToMachine

Assigns an event alert to a machine.

A single record of the following fields is returned.

NewId	int	A unique identifier of the event alert.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AssignEventLogMachineSettings

Assigns event log settings to a machine.

A single record of the following fields is returned.

NewId	int	A unique identifier of the event log setting assignment.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

CreateEventSet

Create a new event set. Returns the new event set ID.

A single record of the following fields is returned.

NewId	int	A unique identifier of the new event set.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

CreateEventSetDefinition

Creates an event set definition.

A single record of the following fields is returned.

NewId	int	A unique identifier of the new event set definition.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.

API Web Services

ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteAllEventAlertsFromMachine

Deletes all event alerts assigned to a machine.
A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteAllEventLogMachineSettings

Deletes all windows event log machine settings assigned to a machine.
A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteEventAlertFromMachine

Deletes specific event alert from machine, by event log type and category.
A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteEventLogMachineSettings

Deletes windows event log machine settings assigned to a machine, by event log type.
A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteEventSet

Deletes an event set and all of its definitions.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

DeleteEventSetDefinition

Deletes an event set definition by event set definition ID.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetEventAlertList

Gets alert events assigned to a machine.

Multiple records of the following fields are returned.

AgentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
AlertEmail	string	Email addresses an alert email is sent to.
EventLogTypeid	int	Unique id number associated with this event log. For example: Application -> 796450521 DNS Server -> 1208407329 Security -> 1664713117 System -> 1380569194 When the event log type is pulled from a windows machine, if it doesn't exist it will be created in this table with a unique id. This Id will be the same across all systems, this is accomplished by using the name in the creation of the Id.
EventLogCategoryValue	int	1 - Error 2 - Warning 4 - Informational 8 - Success Audit 16 - Failure Audit 256 - Critical 512 - Verbose
EventSetId	int	A unique identifier of the event set.
AgentProcedureid	int	Unique identifier of agent procedure to run if an alert is created. 0 or null = do not run a script
AgentProcedureMachGuid	decimal	The unique identifier of the machine the agent procedure is run on.
CreateTicket	boolean	If true, a ticket is created if an alert is created.
SendEmail	boolean	If true, email is sent if an alert is created.
CreateAlarm	boolean	If true, an alarm is created if an alert is created.

API Web Services

CriteriaType	int	The criteria to meet to trigger an alert. 0, null = single event 1 = multiple events for duration 2 = missing event for duration.
EventCount	int	Number of events to occur before an alert is triggered
AlarmDurationSecs	int	Number of seconds to wait before an alert is triggered.
AlarmRearmSec	int	Number of seconds to wait after an alert has occurred before a new alert is triggered for the same criteria.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetEventLogMachineSettingsList

Returns event log settings for a specific machine.

Multiple records of the following fields are returned.

MachineName	string	Full machine name. Everything to the left of the left most decimal point is the machine name.
AgentGuid	decimal	A unique identifier for a machine ID.group ID account and its corresponding agent.
EventLogTypeId	int	Unique id number associated with this event log. For example: Application -> 796450521 DNS Server -> 1208407329 Security -> 1664713117 System -> 1380569194 When the event log type is pulled from a windows machine, if it doesn't exist it will be created in this table with a unique Id. This Id will be the same across all systems, this is accomplished by using the name in the creation of the Id.
EventLogName	string	The event log type name.
EventAssignValue	int	Value determining the types of events to pull from the event log. Stored as a bitmap with the following weights: 1 – error 2 – warning 4 – info 8 – success audit 16 – failure audit 256 – critical 512 – verbose

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetEventSetDefinitionList

Returns an event set definition.

Multiple records of the following fields are returned.

EventSetId	int	A unique identifier of the event set.
Ignore	int	0,null – to apply these filter settings using LIKE 1 – to apply these filter settings using NOT LIKE
Source	string	Filter used to match the event log source field.
Category	string	Filter used to match the event log category field.
EventId	int	Filter used to match the event log event ID field.
UserName	string	Filter used to match the event log username field.
Description	string	Filter used to match the event log description field.
EventSetDefId	int	A unique identifier of the event set definition.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetEventSetList

Returns a list of event sets.

Multiple records of the following fields are returned.

SetName	string	The name of the event set.
EventSetId	int	A unique identifier of the event set.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

KSD API Web Service

In This Section

Enabling KSD API Web Service	523
KSD API Web Service Data Types	524
KSD API Web Service - Operations	530
Sample Messages	534

Enabling KSD API Web Service

See the [VSA API Web Service](http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#3433.htm) (<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#3433.htm>) online help or user guide for a general introduction to the Kaseya API.

API Web Services

To enable the KSD API Web Service:

- Display the System > **Configure** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#248.htm>) page in the VSA.
- Check the **Enable VSA API Web Service** checkbox.
- Access the KSD API web service using `http://<your-KServer>/vsawS/vsaServiceDeskWS.asmx`

KSD API Web Service Data Types

The following are the major data types used in the **KSD API Web Service**. These data types are defined in the XML schema document in the XML\Schemas\ServiceDesk\ServiceDeskDefinition.xsd file located in the directory where the Kaseya software is installed.

Note: In the descriptions that follow, where the name says (content) that means the value is the content of the element.

Legend

- A - AddIncident
- G - GetIncident
- L - ListIncidents
- U - UpdateIncident

RefItem

The **RefItem** describes an item that is a reference item in the service desk. These have an internal database ID value, an internal name, an optional description and the display value.

G	ref	string	The internal name of the item. This is usually prefixed by the service desk name and , such as Standard Open.
G	id	string	The internal database key for the item.
G	description	string	The optional description for the item.
G	(content)	string	The user readable form of the item.

CustomField

The **CustomField** describes the value of a custom field in an incident.

AGU	fieldName	string	The name of the field within the service desk.
AGU	(content)	string	The value of the custom field.

Note

The **Note** describes a single note attached to a ticket.

G	User	string	The name of the user that created the note.
G	Timestamp	dateTime	The time the note was created.
AG	Text	string	The content of the note. This may be HTML formatted, and may include references to attachments.
AG	Hidden	boolean	True if the note should be hidden.
AG	HoursWorked	Decimal	The number of hours worked in this update of the ticket.

AG	SuppressNotify	Boolean	True if notifications for this update should be suppressed.
----	----------------	---------	---

Attachment

The **Attachment** describes a single attachment for the ticket.

A	Name	string	A unique identifying string for this attachment.
A	DisplayName	string	The name of the attachment as seen by the user.
A	FileName	string	The original name of the file or URL.
A	DocumentType	string	The MIME format of the attachment.
A	Content	Base64Binary	The base 64 encoded content for the attachment.

RelatedIncident

The **RelatedIncident** is another incident that has been related to this current incident

AGU	IncidentNumber	string	The unique identifier for the incident.
G	Summary	string	The summary of the related incident.
G	Status	string	The user readable status of the related incident.
G	Description	string	The description field of the incident.

ServiceDeskDefinition

The following **ServiceDeskDefinition** elements returned describe the desk definition used to edit the ticket. This provides each of the possible values for each field in the ticket.

A single record of the following elements returned.

ServiceDeskDefinition	id="decimal"	A unique identifier.
Name	string	The name of the desk definition.
Description	string	A brief description of the desk definition.
RequireTime	boolean	If true, entering hours worked is required.
DisplayMachineInfo	boolean	If true, machine lookup field is displayed.
RequireMachineInfo	boolean	If true, machine lookup association is required.
DisplayOrgInfo	boolean	If true, organization lookup field is displayed.
RequireOrgInfo	boolean	If true, organization lookup association is required.
DisplayCI	boolean	obsolete
RequireCI	boolean	obsolete
AllAdmins	boolean	obsolete
AutoStartClock	boolean	If true, a clock is automatically started when the user starts to edit the ticket.
AutoSaveClock	boolean	If true, when the ticket is saved, the difference between the current time and the start time is entered as the Hours Worked.
AutoInsertNote	boolean	If true, notes are automatically added to each ticket for the changes made to the ticket.
AutoInsertNoteHidden	boolean	If true, automatically generated notes are made hidden.

API Web Services

NeedStatusNote	boolean	obsolete
SDPrefix	string	The prefix code added to the beginning of the ticket ID.
DefaultStatus	decimal	Default status value. Refers to one of the elements with the matching id attribute in the Status section.
DefaultStage	decimal	Default stage value. Refers to one of the elements with the matching id attribute in the Stage section.
DefaultPriority	decimal	Default priority value. Refers to one of the elements with the matching id attribute in the Priority section.
DefaultSeverity	decimal	Default severity value. Refers to one of the elements with the matching id attribute in the Severity section.
DefaultResolution	decimal	Default resolution value. Refers to one of the elements with the matching id attribute in the Resolution section.
DefaultCategory	decimal	Default category value. Refers to one of the elements with the matching id attribute in the Category section.
DefaultSubCategory	decimal	Obsolete
DefaultServiceDesk	boolean	If true, this is the default service desk, the first one selected when creating new tickets.
TemplateName	string	The template file used to initially create the service desk. Not used otherwise.
TemplateType	int	The type of service desk: 1=ticket, 3=knowledge base.
SequenceName	string	For internal development use only.
EditingTemplate	string	The name of the form used to edit tickets for the service desk.
ShowNotesPane	boolean	If true, notes pane displays in lower pane of Tickets table.
ShowWorkOrders	boolean	If true, display work order and work order line in ticket editor.
ShowSessionTimers	boolean	If true, display session timers in ticket editor.
ShowTasks	boolean	If true, display tasks tab and task related fields.
EstimatedHours	double	Total number of hours worked estimated to resolve this ticket.
ActualHours	double	Total number of hours entered to resolve this ticket.
EmailReader	string	The email reader associated with the service desk.
Administrator	string	The user that is the "desk administrator" of the service desk. The desk administrator is notified of certain errors within the service desk.
DefaultPolicy	string	The default policy assigned to the desk.
Status	RefItem	Returns a list of child elements of each Status value in the service desk.
Priority	RefItem	Returns a list of child elements of each Priority value in the service desk.
Severity	RefItem	Returns a list of child elements of each Severity value in the service desk.
Resolution	RefItem	Returns a list of child elements of each Resolution value in the service desk.
TaskStatus	RefItem	Returns a list of child elements of each TaskStatus value in the service desk.
Categories	RefItem	Returns a list of child elements of each Category value in the service desk.

Stages		<p>Returns a list of child elements of each Stage value in the service desk. Each Stage is identified by a Begin, Middle, or End stagetype attribute. Each stage has the following child elements:</p> <ul style="list-style-type: none"> • Item - The name of the stage. • Initialization - The Stage Entry procedure linked to the stage. • Escalation - The Escalation procedure linked to the stage. Time and Units are specified as attributes. • Goal - The Goal linked to the stage. The Goal procedure linked to the stage. Time and Units are specified as attributes. • NextStage – One of the next stages that this stage may transition to.
Participants	RefItem	The list of users as pools that may be assignees or owners for the service desk.
CurrentContact		<p>Contact information about the user logged on during this transaction. If the user is associated with a staff record, then the CurrentContact information is culled from the staff record. If the currently logged on user is a machine user using Portal Access, then CurrentContact information is culled from the Home > Change Profile tab of Portal Access.</p> <ul style="list-style-type: none"> • ContactName • PhoneNumber • Organization • EmailAddress
SubmitterTypes	string	<p>Type of person submitting the ticket:</p> <ul style="list-style-type: none"> • UNKNOWN • PARTICIPANT - A participant is a VSA user. • USER - Someone not known to VSA.
CustomFields		<p>Returns zero or more Field elements, each with the following hierarchy:</p> <ul style="list-style-type: none"> • Caption - Screen caption. • Title - Report title. • Fieldname - Name of the field. • FieldFormat - Data type. • DefaultValue - Default value, if a List data type. • Values - collection element, if a List data type. <p>Item - List item value.</p>
AccessRights		<p>Returns a hierarchy of child elements:</p> <ul style="list-style-type: none"> • ViewHiddenNotes - true or false • ChangeHiddenNotes - true or false • Field Rights>Field Right - collection elements <p>FieldName - Name of the ticket field AccessType - Required, Edit, View Only, Hidden</p>
NoteTemplates		Returns a list of note templates, each representing standard text that can be added to ticket notes.
ChangeProcedure	string	The Change Ticket procedure associated with the service desk.
GoalProcedure	decimal	<p>The Goal procedure associated with the service desk.</p> <ul style="list-style-type: none"> • time – the amount of time for goal • unit – The units of time • (content) – the name of the goal procedure.
ResourceTypes		The list of resource types that can be assigned to a ticket.
TaskDefinitions		The list of task values that can be assigned to a task status.
AssocPolicies		The list of policies that can be associated with a ticket.

Incident Summary

The **IncidentSummary** contains the basic description of a ticket.

AGLU	ServiceDeskName	string	The name of the desk definition.
GLU	IncidentNumber	string	The ticket identifier.
AGLU	Summary	string	The ticket summary text.
AGLU	Description	string	The ticket description. text.
AGLU	Status	string	The ref status of the ticket.
AGLU	Priority	string	The ref priority of the ticket.
AGLU	Resolution	string	The ref resolution type of the ticket.
AGLU	Stage	string	The ref stage of the ticket.
AGLU	Severity	string	The ref severity of the ticket.
AGLU	Category	string	The ref category of the ticket.
AGLU	SubCategory	string	The ref subcategory of the ticket.
GL	Policy	string	The policy of the ticket.
GL	CreateDateTime	dateTime	The date time the ticket was created.
GL	LastEditDateTime	dateTime	The date time the ticket was last edited.
GL	CloseDateTime	dateTime	The date time the ticket was closed.
AGLU	OrgID	decimal	Unique identifier of the organization associated with the ticket.
AGLU	OrganizationName	string	The organization name associated with the ticket.
AGLU	Organization	string	The organization ID associated with the ticket.
AGLU	OrganizationStaffName	string	The organization staff member name associated with the ticket.
AGLU	OrganizationStaff	string	The organization staff member unique ID associated with the ticket.
AGLU	OrganizationStaffEmail	string	The email of the organization staff member associated with the ticket.
AGLU	Machine	string	The machine associated with the ticket.
AGLU	MachineGuid	decimal	The GUID of the machine associated with the ticket.
AGLU	MachineGroup	string	The machine group of the machine associated with the ticket.
AGLU	MachineGroupGuid	decimal	The GUID of the machine group associated with the the ticket.
AGLU	Submitter	string	The name of the submitter who submitted the ticket.
AGLU	SubmitterEmail	string	The email of the ticket submitter.
AGLU	SubmitterPhone	string	The phone of the ticket submitter.
AGLU	SubmitterType	string	Type of person submitting the ticket: <ul style="list-style-type: none"> • UNKNOWN • PARTICIPANT - A participant is a VSA user. • USER - Someone not known to VSA.
GL	IsUnread	boolean	If true, the ticket has not been viewed by the currently logged on user.

Incident

The **Incident** is derived from the **IncidentSummary** and contains all of the fields of the **IncidentSummary** in addition to these fields.

G	IsParticipant	boolean	obsolete
G	IsClosed	boolean	True if closed.
G	CurrentStageEscalation DateTime	dateTime	Stage escalation date and time.
G	CurrentGoalDateTime	dateTime	Stage goal date and time.
AGU	Owner	string	Owner of the ticket.
	Participant	string	obsolete
AGU	AssigneeType	string	Type of assignee: <ul style="list-style-type: none"> • UNKNOWN • PARTICIPANT - individual assignee • POOL - a pool of users
AGU	Assignee	string	Assignee name.
AGU	AssigneeEmail	string	Assignee email.
G	ActualCompletionDate	dateTime	obsolete
G	ExpectedCompletion Date	dateTime	Date time the ticket is or was expected to be closed, (the ticket goal due date).
G	ActualResolutionDate	dateTime	Date time a resolution type was set for the ticket.
AGU	PromisedDate	dateTime	Date time promise date entered by the customer representative to resolve the ticket.
G	IsArchived	boolean	True if ticket is archived.
G	IsError	boolean	obsolete
G	IsPoolAssignee	boolean	obsolete
	ErrorMessage	string	obsolete
	Notify	boolean	obsolete
G	CurrentStage	string	The current stage.
AGU	ResolutionNote	string	Descriptive text entered with the resolution type.
G	LockTime	dateTime	Date time the ticket was locked by opening the ticket for editing.
G	LockUser	string	User locking the ticket by opening the ticket for editing.
G	StageGoalTime Remaining	int	The time remaining before the stage goal timer executes the goal procedure. Rrelevant when the stage goal has been paused.
AGU	SourceType	string	The source type, either a system event or email, that generated a ticket request. <ul style="list-style-type: none"> • Email • Backup • KES • Patch • Monitor • Alarm • Portal • ServiceDesk • Other
	OrgAddress/Address	string	Org address 1
	OrgAddress/Address	string	Org address 2
	OrgAddress/City	string	Org city
	OrgAddress/State	string	Org state

	OrgAddress/Zip	string	Org zip
	OrgAddress/Country	string	Org address
AGLU	Field	CustomField	Zero or more custom fields values
AGU	Notes	Note	Zero or more notes.
AGU	Attachments	Attachment	Zero or more attachments
AGU	RelatedIncidents	Related Incident	Zero or more related incidents
	StartDate	datetime	start date/time of the task
	EndDate	datetime	end date/time of the task
	UpdateTime	datetime	last date/time this task was updated
	FollowupDate	datetime	date/time to followup on this task
	CompletionDate	datetime	completion date/time of this task
	ApprovalDate	datetime	approval date/time of this task
	PromiseDate	datetime	promise date/time for this task
	PercentCompletion	int	percent completion of this task
	TaskStatus	string	status of this task
	ActualHours	double	total hours worked for this task
	Resource	Resource	Zero or more resources
	Assignee	string	assignee assigned to this task
	EstimatedHours	decimal	Estimated total hours worked for this ticket.
	TotalHours	decimal	Actual hours worked for this ticket.
	PreviousStage	string	PreviousStage of this ticket.
	WorkPerformedDateTim e	datetime	Datetime work was performed on this ticket.
	EditingTemplate	string	Editing template used to edit this ticket.
GU	ServiceDeskDefinition	ServiceDesk Definition	

KSD API Web Service - Operations

The following operations can be performed using the [KSD API Web Service](#).

AddIncident

The request is:

AddSDIncident	Incident	The content of the new incident to create. Only fields marked with an A in the first column can be set.
SessionId	Decimal	The web service session ID.

A single record of the following fields is returned.

IncidentNumber	string	The unique identifier of the ticket.
IncidentID	decimal	The identifier of the ticket.
Method	string	The operation that requested this response.

TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

AddServDeskToScope

The request is:

servDeskName	string	The name of the service desk.
scopeName	string	The name of the scope.
SessionId	decimal	The web service session ID.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetIncident

Retrieves a single incident from the database. The request is:

IncidentRequest		The incident to retrieve. This has the following fields: <ul style="list-style-type: none"> • IncidentNumber – The ticket ID as seen by the user, such as STD000001 • IncidentId – The database ID of the ticket to retrieve. • IncludeNotes – true to include notes in the retrieved ticket • IncludeDefinition – true to include the desk definition in the response • IncludeAttachment - true to include attachments in the retrieved ticket
SessionId	Decimal	The web service session ID.

A single record of the following fields is returned.

IncidentResponse	Incident	The retrieved incident.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetIncidentList

Retrieves a list of incidents matching the request criteria.

The request is:

IncidentRequest		The incident to retrieve. This has the following fields: <ul style="list-style-type: none"> • ServiceDeskName – The name of the service desk to query. • Status – One or more status values to match. If no status
-----------------	--	--

		<p>values are supplied, then tickets are retrieved regardless of status.</p> <ul style="list-style-type: none"> • Priority – One or more priority values to match. If no priority values are supplied, then tickets are retrieved regardless of priority. • Stage – One or more stage values to match. If no stage values are supplied, then tickets are retrieved regardless of stage. • SummarySearch – a string or expression to search the summary of tickets. • Organization – The name or partial name of organizations to match. If not supplied, then tickets are retrieved for all organizations within the scope. • OrganizationStaff – The name of an organizational staff member associated with tickets. If not supplied, then tickets are retrieved for all organizations within the scope. • Machine – The name of a machine to match. If not supplied, then tickets are retrieved for all machines within the scope. • MachineGroup – The name of a machine group to match. If not supplied, then tickets are retrieved for all machine groups within the scope. • Assignee – The name or partial name of assignees to match. If not supplied, then tickets are retrieved for all assignees within scope. • StartingIncident – When paging, this is the next incident number to retrieve. This value comes from the nextStartingIncident value of a previous GetIncidentList request. • IncidentCount – When present, specifies the number of incidents to retrieve. • SortField – When present, sorts the results on the field name.
SessionId	Decimal	The web service session ID.

The response is the following:

IncidentList		<p>The list of matching incidents. This has the following attributes and elements:</p> <ul style="list-style-type: none"> • totalIncidents – The total number of incidents that match the request. • nextStartingIncident – the Id of the next incident to retrieve. • Incident – zero or more incident matching the request criteria.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetIncidentList2

Returns all values in [GetIncidentList](#) (page 531) plus the custom fields and values per incident. Multiple records of the following field is returned, if applicable.

CustomFields	string or null	The value of the custom field that was specified in the request.
--------------	----------------	--

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetServiceDesk

Retrieves the definition of a service desk. This should be called prior to creating a user interface to allow the user to enter a ticket. The request is:

ServiceDeskDefinitionRequest		The service desk to retrieve. This has the following elements: <ul style="list-style-type: none"> ServiceDeskName – The name of the service desk to retrieve. ServiceDeskID – the database of the service desk to retrieve. Should not be used.
SessionId	Decimal	The web service session ID.

A single record of the following elements returned.

ServiceDeskDefinitionResponse	ServiceDeskDefinition	The retrieved desk definition.
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

GetServiceDesks

Multiple records of the following fields are returned, if applicable. The request is:

IsDefault	boolean	If true, the service desk is the default service desk.
ServiceDeskID	decimal	A unique identifier.
ServiceDeskName	string	The name of the service desk.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Primitives

The following primitive Datatype operations are also provided. Each primitive operation uses the same xml contract as their corresponding multiple-columns operation. Each primitive returns a string value that requires subsequent processing. You are strongly discouraged from using these methods.

Primitive	Result	Datatype
PrimitiveAddIncident	PrimitiveAddIncidentResult	string
PrimitiveAddServDeskToScope	PrimitiveAddServDeskToScopeResult	string
PrimitiveGetIncident	PrimitiveGetIncidentResult	string
PrimitiveGetIncidentList	PrimitiveGetIncidentListResult	string
PrimitiveGetServiceDesk	PrimitiveGetServiceDeskResult	string
PrimitiveGetServiceDesks	PrimitiveGetServiceDesksResult	string
PrimitiveUpdateIncident	PrimitiveUpdateIncidentResult	string

QueueAddIncident

Queues an **AddIncident** (page 530) request. This is normally used in high volume situations where many tickets are being created via the API in a small amount of time, so the system does not time out. The add incident request gets added to a table and an ongoing event will pull from this table to create tickets, so the request does not need to wait for the ticket to be created.

The request is:

AddSDIncident	Incident	The incident to add.
SessionId	Decimal	The web service session ID.

A single record of the following fields are returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

UpdateIncident

Updates a single incident in the database. The request is:

UpdateSDIncident	Incident	The incident to update. See the first column of the Incident data type for the fields that are valid on update.
SessionId	Decimal	The web service session ID.

A single record of the following fields is returned.

Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

Sample Messages

Sample data is included in the following XMLs.

GetServiceDesks Request

```
<GetServiceDesks xmlns="vsaServiceDeskWS">
  <req>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetServiceDesks>
```

GetServiceDesks Response

```
<GetServiceDesksResponse xmlns="vsaServiceDeskWS">
  <GetServiceDesksResult>
    <ServiceDesks>
      <ServiceDesk>
        <IsDefault>false</IsDefault>
        <ServiceDeskID>291273277175176</ServiceDeskID>
        <ServiceDeskName>KnowledgeBase</ServiceDeskName>
      </ServiceDesk>
      <ServiceDesk>
        <IsDefault>false</IsDefault>
        <ServiceDeskID>696191121914314</ServiceDeskID>
        <ServiceDeskName>Standard</ServiceDeskName>
      </ServiceDesk>
    </ServiceDesks>
    <Method>GetServiceDesks</Method>
    <TransactionID>144</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </GetServiceDesksResult>
</GetServiceDesksResponse>
```

GetServiceDesk Request

```
<GetServiceDesk xmlns="vsaServiceDeskWS">
  <req>
    <ServiceDeskDefinitionRequest>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName>
      <ServiceDeskID
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">696191121914314</ServiceDeskID>
    </ServiceDeskDefinitionRequest>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetServiceDesk>
```

GetServiceDesk Response

```
<GetServiceDeskResponse xmlns="vsaServiceDeskWS">
  <GetServiceDeskResult>
    <ServiceDeskDefinitionResponse id="696191121914314">
      <Name xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</Name>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard
SD</Description>
      <RequireTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</RequireTime>
      <DisplayMachineInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</DisplayMachineInfo>
      <RequireMachineInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</RequireMachineInfo>
      <DisplayOrgInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</DisplayOrgInfo>
      <RequireOrgInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</RequireOrgInfo>
      <DisplayCI xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</DisplayCI>
      <RequireCI xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</RequireCI>
      <AllAdmins xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</AllAdmins>
      <AutoStartClock
```

```

xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</AutoStartClock>
  <AutoSaveClock
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</AutoSaveClock>
  <AutoInsertNote
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</AutoInsertNote>
  <AutoInsertNoteHidden
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</AutoInsertNoteHidden>
  <NeedStatusNote
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</NeedStatusNote>
  <SDPrefix xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD</SDPrefix>
  <DefaultStatus
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">218924116119912</DefaultStatus>
  <DefaultStage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">831768438118427</DefaultStage>
  <DefaultPriority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">693719171716599</DefaultPriority>
  <DefaultSeverity
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultSeverity>
  <DefaultResolution
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultResolution>
  <DefaultCategory
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultCategory>
  <DefaultServiceDesk
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</DefaultServiceDesk>
  <TemplateType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">1</TemplateType>
  <SequenceName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">SEQ129</SequenceName>
  <EditingTemplate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Fixed_Width_Tabbed.xml</EditingTe
mplate>
  <Status xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="Standard|AwaitingHardware" id="541491145218711">Awaiting Hardware</Item>
    <Item ref="Standard|AwaitingUserFeedback" id="281767467828324">Awaiting User Feedback</Item>
    <Item ref="Standard|Closed" id="989295147216226">Closed</Item>
    <Item ref="Standard|Escalated" id="551271771474242">Escalated</Item>
    <Item ref="Standard|Hold" id="172151822788151">Hold</Item>
    <Item ref="Standard|InProgress" id="111313126312233">In Progress</Item>
    <Item ref="Standard|New" id="218924116119912">New</Item>
  </Status>
  <Priority xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="Standard|CriticalHigh" id="744512181719881">Critical High</Item>
    <Item ref="Standard|High" id="982525519923522">High</Item>
    <Item ref="Standard|Low" id="291721863176342">Low</Item>
    <Item ref="Standard|Medium" id="693719171716599">Medium</Item>
    <Item ref="Standard|Planning" id="176222131631332">Planning</Item>
  </Priority>
  <Severity xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="Standard|CompanyWide(High)" id="315477225242249">Whole Company (High)</Item>
    <Item ref="Standard|MultipleUsers(Medium)" id="262164368749722">Multiple users (Medium)</Item>
    <Item ref="Standard|OneUser(Low)" id="917688316816914">Single User (Low)</Item>
  </Severity>
  <Resolution xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Item ref="Standard|AdviceGiven" id="498162732192611">Advice Given</Item>
    <Item ref="Standard|CannotDuplicate" id="262514419248621">Cannot Duplicate</Item>
    <Item ref="Standard|ClosedbyCustomerRequest" id="525192125718333">Closed by Customer
Request</Item>
    <Item ref="Standard|HardwareReplaced" id="432262321578326">Hardware Replaced</Item>
    <Item ref="Standard|HotFixReleased" id="189239616133249">Hot Fix Released</Item>
    <Item ref="Standard|InstallationCompleted" id="139764799836252">Installation Completed</Item>
    <Item ref="Standard|NewSoftwareInstalled" id="521637923418319">New Software Installed</Item>
    <Item ref="Standard|Noreponsefromuser" id="115424612244857">No response from user</Item>
    <Item ref="Standard|OSReinstalled" id="531617444692623">OS Reinstalled</Item>
    <Item ref="Standard|Other" id="711261961631328">Other</Item>
    <Item ref="Standard|PassedtoSales" id="191482475814123">Passed to Sales</Item>
    <Item ref="Standard|Pendingscriptcleared" id="762515513181192">Pending script cleared</Item>
    <Item ref="Standard|ReapplySchema" id="525317525441497">Reapply Schema</Item>
    <Item ref="Standard|Reboot" id="832182442825238">Reboot</Item>
    <Item ref="Standard|ResolvedbyCustomer" id="243623591961272">Resolved by Customer</Item>

```

```

    <Item ref="Standard||ResolvedbyTechnition" id="423939164212169">Resolved</Item>
    <Item ref="Standard||SolvedwithKBarticle" id="272199179212412">Solved with KB article</Item>
    <Item ref="Standard||TrainingGiven" id="622224812237126">Training Given</Item>
  </Resolution>
  <Categories xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Category>
      <Item ref="Standard||Advice&Guidance" id="161211171768212">Advice & Guidance</Item>
      <SubCategory ref="Standard||Advice&Guidance||General"
id="561699795215782">General</SubCategory>
    </Category>
    <Category>
      <Item ref="Standard||Kaseya" id="641881726251641">Kaseya</Item>
      <SubCategory ref="Standard||Kaseya||AgentIcon" id="821781865922435">Agent Icon</SubCategory>
      <SubCategory ref="Standard||Kaseya||Alarm" id="481422361723261">Alarm</SubCategory>
      <SubCategory ref="Standard||Kaseya||ApplicationChanges" id="525187874623717">Application
Changes</SubCategory>
      <SubCategory ref="Standard||Kaseya||Disk" id="919621482151882">Disk</SubCategory>
      <SubCategory ref="Standard||Kaseya||Eventlog" id="814714713317798">Eventlog</SubCategory>
      <SubCategory ref="Standard||Kaseya||GetFile" id="322618792314914">Get File</SubCategory>
      <SubCategory ref="Standard||Kaseya||Hardware" id="176166136238942">Hardware</SubCategory>
      <SubCategory ref="Standard||Kaseya||Lanwatch" id="214791394922624">Lanwatch</SubCategory>
      <SubCategory ref="Standard||Kaseya||Logon_Admin"
id="943315515116292">Logon_Admin</SubCategory>
      <SubCategory ref="Standard||Kaseya||Logon_User"
id="636613429245187">Logon_User</SubCategory>
      <SubCategory ref="Standard||Kaseya||NewAgent" id="557214511134217">New Agent</SubCategory>
      <SubCategory ref="Standard||Kaseya||Other" id="631281678197153">Other</SubCategory>
      <SubCategory ref="Standard||Kaseya||PatchManagement" id="462824113621914">Patch
Management</SubCategory>
      <SubCategory ref="Standard||Kaseya||Procedure" id="274262311559714">Procedure</SubCategory>
      <SubCategory ref="Standard||Kaseya||RCDisabled" id="641624812335116">RC
Disabled</SubCategory>
      <SubCategory ref="Standard||Kaseya||Script" id="471482131991414">Script</SubCategory>
      <SubCategory ref="Standard||Kaseya||SystemOffline" id="11341118222324">System
Offline</SubCategory>
      <SubCategory ref="Standard||Kaseya||SystemOnline" id="251814418923368">System
Online</SubCategory>
      <SubCategory ref="Standard||Kaseya||Unidentified"
id="617313577253122">Unidentified</SubCategory>
    </Category>
    <Category>
      <Item ref="Standard||Network" id="414766231875111">Network</Item>
      <SubCategory ref="Standard||Network||Connectivity"
id="122145211361321">Connectivity</SubCategory>
      <SubCategory ref="Standard||Network||Design" id="495611529142242">Design</SubCategory>
      <SubCategory ref="Standard||Network||Firewall" id="812515316323522">Firewall</SubCategory>
      <SubCategory ref="Standard||Network||Other" id="946227769167531">Other</SubCategory>
      <SubCategory ref="Standard||Network||Performance"
id="941891772111717">Performance</SubCategory>
    </Category>
    <Category>
      <Item ref="Standard||Printer" id="155243642251342">Printer</Item>
      <SubCategory ref="Standard||Printer||Other" id="341431321188813">Other</SubCategory>
      <SubCategory ref="Standard||Printer||PrinterProblem" id="851831547314111">Printer
Problem</SubCategory>
      <SubCategory ref="Standard||Printer||PrinterSetup" id="619395216749723">Printer
Setup</SubCategory>
      <SubCategory ref="Standard||Printer||Toner" id="161984536861723">Toner</SubCategory>
    </Category>
    <Category>
      <Item ref="Standard||ServiceRequest" id="541124124415221">Service Request</Item>
      <SubCategory ref="Standard||ServiceRequest||EquipmentMove" id="862712311517672">Equipment
Move</SubCategory>
      <SubCategory ref="Standard||ServiceRequest||NewLaptop" id="266812518245792">New
Laptop</SubCategory>
      <SubCategory ref="Standard||ServiceRequest||NewServer" id="322872913227349">New
Server</SubCategory>
      <SubCategory ref="Standard||ServiceRequest||NewWorkstation" id="224115236352441">New
Workstation</SubCategory>

```



```

    </Category>
  </Categories>
  <Stages xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Stage stageType="End">
      <Item ref="Standard||Closed" id="213813735111171" description="Auto Generated">Closed</Item>
      <Initialization>Standard Enters Closed</Initialization>
    </Stage>
    <Stage stageType="Begin">
      <Item ref="Standard||Identified" id="831768438118427" description="New ticket is
received">Identified</Item>
      <Initialization>Standard Enters Identified</Initialization>
      <Escalation time="15" unit="MINUTE">Incident is Escalated</Escalation>
      <Goal time="1" unit="HOURL">Identified Goal</Goal>
      <NextStage ref="Standard||Tier1" id="546812745461511" description="Tier 1
Support">Tier1</NextStage>
    </Stage>
    <Stage stageType="Middle">
      <Item ref="Standard||Tier1" id="546812745461511" description="Tier 1 Support">Tier1</Item>
      <Initialization>Standard Enters Tier1</Initialization>
      <Escalation time="3" unit="HOURL">Incident is Escalated</Escalation>
      <Goal time="2" unit="HOURL">Tier1 Goal</Goal>
      <NextStage ref="Standard||Closed" id="213813735111171" description="Auto
Generated">Closed</NextStage>
      <NextStage ref="Standard||Tier2" id="318527191192719" description="Tier 2 Specialist
Support">Tier2</NextStage>
    </Stage>
    <Stage stageType="Middle">
      <Item ref="Standard||Tier2" id="318527191192719" description="Tier 2 Specialist
Support">Tier2</Item>
      <Initialization>Standard Enters Tier2</Initialization>
      <Escalation time="3" unit="HOURL">Incident is Escalated</Escalation>
      <Goal time="4" unit="HOURL">Tier2 Goal</Goal>
      <NextStage ref="Standard||Closed" id="213813735111171" description="Auto
Generated">Closed</NextStage>
    </Stage>
  </Stages>
  <Participants xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Participant ref="garyw" id="67511883639135112891416313" isPool="false">garyw</Participant>
    <Participant ref="jschenck" id="72381729521421633172123416"
isPool="false">jschenck</Participant>
    <Participant ref="NickT" id="96171921315349923924634249" isPool="false">NickT</Participant>
    <Participant ref="Standard||SupportManager" id="654222596258293" isPool="true">SupportManager
(Pool)</Participant>
    <Participant ref="Standard||Tier1Support" id="352161952139188" isPool="true">Tier1Support
(Pool)</Participant>
    <Participant ref="Standard||Tier2Support" id="921522231318131" isPool="true">Tier2Support
(Pool)</Participant>
  </Participants>
  <CustomFields xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Field id="221552971661261">
      <Caption>Source</Caption>
      <Title>Source</Title>
      <FieldName>Source</FieldName>
      <FieldFormat>List</FieldFormat>
      <DefaultValue>Call</DefaultValue>
      <Values>
        <Item ref="Call" id="0">Call</Item>
        <Item ref="EMail" id="0">EMail</Item>
        <Item ref="Text" id="0">Text</Item>
      </Values>
    </Field>
    <Field id="818831117157241">
      <Caption>Urgency</Caption>
      <Title>Urgency</Title>
      <FieldName>Urgency</FieldName>
      <FieldFormat>List</FieldFormat>
      <DefaultValue>Medium</DefaultValue>
      <Values>
        <Item ref="High" id="0">High</Item>

```



```

        <Item ref="Low" id="0">Low</Item>
        <Item ref="Medium" id="0">Medium</Item>
    </Values>
</Field>
<Field id="513119818455188">
    <Caption>KB Article created</Caption>
    <Title>KB Article Created</Title>
    <FieldName>KB_Article</FieldName>
    <FieldFormat>List</FieldFormat>
    <DefaultValue>No</DefaultValue>
    <Values>
        <Item ref="No" id="0">No</Item>
        <Item ref="Yes" id="0">Yes</Item>
    </Values>
</Field>
<Field id="291214644251233">
    <Caption>Dept</Caption>
    <Title>Department</Title>
    <FieldName>Dept</FieldName>
    <FieldFormat>List</FieldFormat>
    <DefaultValue>IT</DefaultValue>
    <Values>
        <Item ref="Accounting" id="0">Accounting</Item>
        <Item ref="Accounts Payable" id="0">Accounts Payable</Item>
        <Item ref="Facilities" id="0">Facilities</Item>
        <Item ref="HR" id="0">HR</Item>
        <Item ref="IT" id="0">IT</Item>
        <Item ref="Other" id="0">Other</Item>
        <Item ref="Payroll" id="0">Payroll</Item>
        <Item ref="Sales" id="0">Sales</Item>
        <Item ref="Telecom" id="0">Telecom</Item>
    </Values>
</Field>
</CustomFields>
<AccessRights xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <ViewHiddenNotes>true</ViewHiddenNotes>
    <ChangeHiddenNotes>true</ChangeHiddenNotes>
    <FieldRights>
        <FieldRight>
            <FieldName>ID</FieldName>
            <AccessType>Required</AccessType>
        </FieldRight>
        <FieldRight>
            <FieldName>Summary</FieldName>
            <AccessType>Required</AccessType>
        </FieldRight>
        <FieldRight>
            <FieldName>Description</FieldName>
            <AccessType>Edit</AccessType>
        </FieldRight>
        <FieldRight>
            <FieldName>CreationDtTm</FieldName>
            <AccessType>ViewOnly</AccessType>
        </FieldRight>
        <FieldRight>
            <FieldName>SubmitterName</FieldName>
            <AccessType>Edit</AccessType>
        </FieldRight>
        <FieldRight>
            <FieldName>SubmitterEmailAddr</FieldName>
            <AccessType>Edit</AccessType>
        </FieldRight>
        <FieldRight>
            <FieldName>ContactPhone</FieldName>
            <AccessType>Edit</AccessType>
        </FieldRight>
        <FieldRight>
            <FieldName>OrgName</FieldName>
            <AccessType>Edit</AccessType>
        </FieldRight>
    </FieldRights>

```

```

</FieldRight>
<FieldRight>
  <FieldName>OrgID</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>StaffID</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>ContactEmail</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>MachineID</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>Note</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>ClosedDtTm</FieldName>
  <AccessType>ViewOnly</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>PromiseDtTm</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>DueDtTm</FieldName>
  <AccessType>ViewOnly</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>ActualCompletedDate</FieldName>
  <AccessType>ViewOnly</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>HiddenNote</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>Owner</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>LockUser</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>EditDtTm</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>current_esc_datetime</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>current_goal_datetime</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>lockTime</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>
<FieldRight>
  <FieldName>sourceType</FieldName>
  <AccessType>Edit</AccessType>
</FieldRight>

```

```

    <FieldRight>
      <FieldName>Status</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Priority</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Severity</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Category</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>SubCategory</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Stage</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Resolution</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Assignee</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Source</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Urgency</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>KB_Article</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
    <FieldRight>
      <FieldName>Dept</FieldName>
      <AccessType>Edit</AccessType>
    </FieldRight>
  </FieldRights>
</AccessRights>
<NoteTemplates xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
  <Item ref="My Note" id="196429316815241">My Note</Item>
  <Item ref="Note 2" id="167218821431219">Second note</Item>
</NoteTemplates>
<ChangeProcedure xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard is
Changed</ChangeProcedure>
  <GoalProcedure time="1" unit="DAY"
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard Goal - All
Stages</GoalProcedure>
</ServiceDeskDefinitionResponse>
<Method>GetServiceDesk</Method>
<TransactionID>146</TransactionID>
<ErrorMessage/>
<ErrorLocation/>
</GetServiceDeskResult>
</GetServiceDeskResponse>

```

GetIncidentList Request

```
<GetIncidentList xmlns="vsaServiceDeskWS">
  <req>
    <IncidentListRequest>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName>
      <IncidentCount
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">30</IncidentCount>
    </IncidentListRequest>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetIncidentList>
```

GetIncidentList Response

```
<GetIncidentListResponse xmlns="vsaServiceDeskWS">
  <GetIncidentListResult>
    <IncidentList>
      <Incident xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <ServiceDeskName>Standard</ServiceDeskName>
        <IncidentNumber>STD000001</IncidentNumber>
        <Summary>Getting Started with Service Desk - PLEASE READ!</Summary>
        <Status>Closed</Status>
        <Priority>Low</Priority>
        <Stage>Closed</Stage>
        <CreateDateTime>2010-02-05T17:07:21.55-08:00</CreateDateTime>
        <LastEditDateTime>2010-02-05T22:59:22.64-08:00</LastEditDateTime>
        <Submitter>Kaseya Support</Submitter>
        <SubmitterEmail>noreply@kaseya.com</SubmitterEmail>
      </Incident>
    </IncidentList>
    <Method>GetIncidentList</Method>
    <TransactionID>147</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </GetIncidentListResult>
</GetIncidentListResponse>
```

GetIncident Request

```
<GetIncident xmlns="vsaServiceDeskWS">
  <req>
    <IncidentRequest>
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000001</IncidentNumber>
      <IncludeNotes
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IncludeNotes>
      <IncludeDefinition
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IncludeDefinition>
    </IncidentRequest>
    <SessionID>67223225114316912673490269</SessionID>
  </req>
</GetIncident>
```

GetIncident Response

```
<GetIncidentResponse xmlns="vsaServiceDeskWS">
  <GetIncidentResult>
    <IncidentResponse id="611922114996841">
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000001</IncidentNumber>
      <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Getting Started with
Service Desk - PLEASE READ!</Summary>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        &lt;p&gt;&lt;strong&gt;&lt;span
style='font-size:11.0pt;font-family:"Calibri", "sans-serif";color:blue'&gt;WELCOME TO SERVICE
```

DESK

Your Service Desk module has been pre-configured with a template-driven Standard service desk, and a Knowledge Base desk. Only a few short customization steps are required to use these desks immediately. See <http://help.kaseya.com/WebHelp/EN/KSD/1000000/index.htm?toc.htm?5982.htm>; Getting Started; to quickstart your implementation of Service Desk.

```

    </Description>
    <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard|Closed</Status>
    <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard|Low</Priority>
    <Stage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard|Closed</Stage>
    <Category
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard|Advice&Guidance</Ca
tegory>
    <CreateDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T17:07:21.55-08:00</Cre
ateDateTime>
    <LastEditDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T22:59:22.64-08:00</Las
tEditDateTime>
    <Submitter xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Kaseya
Support</Submitter>
    <SubmitterEmail
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">noreply@kaseya.com</SubmitterEmai
l>
    <SubmitterType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">UNKNOWN</SubmitterType>
    <IsUnread xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>true</IsUnread>
    <IsParticipant
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsParticipant>
    <Owner xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Owner>
    <AssigneeType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">POOL</AssigneeType>
    <Assignee
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Tier1Support</Assignee>
    <ActualCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T22:59:29.28-08:00</Act
ualCompletionDate>
    <ExpectedCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-06T17:07:22.283-08:00</Ex
pectedCompletionDate>
    <IsArchived
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsArchived>
    <IsError xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</IsError>
    <Notify xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">>false</Notify>
    <SourceType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">ServiceDesk</SourceType>
    <CustomFields xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Field fieldName="Source">Text</Field>
    <Field fieldName="Urgency">Low</Field>
    <Field fieldName="KB_Article">No</Field>
    <Field fieldName="Dept">Sales</Field>
    </CustomFields>
    <Notes xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <Note id="213494962391116">
    <Timestamp>2010-02-05T22:59:25.127-08:00</Timestamp>
    <Text>Auto Generated Note:&lt;br/&gt;
Ticket Changed&lt;br/&gt; 'currentStageGoalDateTime' cleared&lt;br/&gt;</Text>
    <Hidden>true</Hidden>
    </Note>
    <Note id="356934215185622">
    <User>garyw</User>
    <Timestamp>2010-02-05T17:07:21.55-08:00</Timestamp>
    <Text>Auto Generated Note:&lt;br/&gt;
Ticket Added&lt;br/&gt;</Text>
    <Hidden>true</Hidden>
    </Note>

```

API Web Services

```
</Notes>
</IncidentResponse>
<Method>GetIncident</Method>
<TransactionID>200</TransactionID>
<ErrorMessage/>
<ErrorLocation/>
</GetIncidentResult>
</GetIncidentResponse>
```

AddIncident Request

```
<AddIncident xmlns="vsaServiceDeskWS">
  <req>
    <AddSDIncident>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName>
      <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Test Ticket From Web
Service</Summary>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">This ticket was
created with the web service.</Description>
      <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||New</Status>
      <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Medium</Priority>
      <Category
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Network</Category>
    </AddSDIncident>
    <SessionID>67223225114316912673490269</SessionID>
  </req>
</AddIncident>
```

AddIncident Response

```
<AddIncidentResponse xmlns="vsaServiceDeskWS">
  <AddIncidentResult>
    <AddSDIncidentResponse>
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000002</IncidentNumber>
      <IncidentID
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">249259141859248</IncidentID>
    </AddSDIncidentResponse>
    <Method>AddIncident</Method>
    <TransactionID>203</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </AddIncidentResult>
</AddIncidentResponse>
```

Chapter 14

Update Incident Request

```
<UpdateIncident xmlns="vsaServiceDeskWS">
  <req>
    <UpdateSDIncident id="89421281980071930157491435">
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Customer_SD_Basic</ServiceDeskName>
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">CSN000380</IncidentNumber>
      <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Test Ticket From Web Service</Summary>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">This ticket was created with the web service.</Description>
      <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||InProgress</Status>
      <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Low</Priority>
      <Stage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Identified</Stage>
      <CreateDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:07:31.923-08:00</CreateDateTime>
      <LastEditDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:07:31.923-08:00</LastEditDateTime>
      <Submitter xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Submitter>
      <SubmitterType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">UNKNOWN</SubmitterType>
      <IsUnread xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IsUnread>
      <IsParticipant
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsParticipant>
      <CurrentStageEscalationDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:22:43.063-08:00</CurrentStageEscalationDateTime>
      <CurrentGoalDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T22:07:43.077-08:00</CurrentGoalDateTime>
      <Owner xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Owner>
      <AssigneeType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">POOL</AssigneeType>
      <Assignee
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Tier1Support</Assignee>
      <ExpectedCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-11T21:07:43.077-08:00</ExpectedCompletionDate>
      <IsArchived
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsArchived>
      <IsError xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsError>
    </UpdateSDIncident>
  </req>
</UpdateIncident>
```

API Web Services

```
<Notify xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</Notify>
<Notes xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
  <Note id="281273717819319">
    <User>garyw</User>
    <Timestamp>2010-03-10T21:07:31.923-08:00</Timestamp>
    <Text>Auto Generated Note:&lt;br/&gt; Ticket Added&lt;br/&gt;</Text>
    <Hidden>true</Hidden>
  </Note>
</Notes>
</UpdateSDIncident>
<SessionID xmlns="">98782788528483188965186776</SessionID>
</req>
</UpdateIncident>
```

UpdateIncident Response

```
<UpdateIncidentResponse xmlns="vsaServiceDeskWS">
  <UpdateIncidentResult>
    <Method>UpdateIncident</Method>
    <TransactionID>205</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </UpdateIncidentResult>
</UpdateIncidentResponse>
```



Glossary

Active Directory

Active Directory is a directory service used to store information about the network resources across a domain. Its main purpose is to provide central authentication and authorization services for Windows based computers. An Active Directory structure is a hierarchical framework of objects. The objects fall into three broad categories: resources (e.g. printers), services (e.g. email) and users (user accounts and groups). The AD provides information on the objects, organizes the objects, controls access and sets security.

The VSA can manage computers, contacts and users by referencing information stored in Active Directory. See Domain Watch in the **Discovery** module for more information.

Agent Menu

The set of options that display when the user right-clicks the **agent** (page 547) icon  in the **system tray** (on page 564) of the managed machine. The agent menu can be **customized** (page 59).

Agent Settings

To provide both flexibility and automation, the VSA enables you to specify different values for the following types of agent settings on a per machine basis:



- **Credential** (page 68)
- **Agent Menu** (page 59)
- **Check-in Control** (page 61)
- **Working Directory** (page 64)
- **Logs** (page 32)
- Machine Profile - Refers to settings in Audit > **Edit Profile** (page 65).
- **View Collections** (page 552)
- **Portal Access** (page 67)
- Remote Control Policy
- **Patch Settings** (page 559)
- Patch File Source
- Patch Policy Memberships
- Fixed Alerts - These all the alert types on the Monitor > **Alerts** (page 248) page except for Event Log alerts and System alerts.
- **Event Log Alerts** (page 248)
- **Monitor Sets** (page 234)
- **Distribute Files** (page 118)
- Protection
- Agent Procedure Schedules

Agent Time Scheduling

With **agent time scheduling**, the system clock used by the agent machine determines when that scheduled task occurs. Scheduling the same task for 10 machines all on Tuesday, at 2:00 PM, will occur whenever 2:00 PM on Tuesday, local time, occurs for each machine, as determined each machine's system clock. A global default to use either server time or agent time scheduling is provided using the new System > Server Management > **Default Settings** (page 384) page.

Agents

The VSA manages machines by installing a software client called an **agent** on a managed machine. The agent is a system service that does not require the user to be logged on for the agent to function and does not require a reboot for the agent to be installed. The agent is configurable and can be totally invisible to the user. The sole purpose of the agent is to carry out the tasks requested by the VSA user. Once installed:

- An agent icon—for example the  agent icon—displays in the system tray of the managed machine. **Agent icons** (page 21) can be custom images or removed altogether.
- Each installed agent is assigned a unique VSA **machine ID / group ID / organization ID** (page 556). Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available agent licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > **Deploy Agents** (page 35) inside the VSA.
- **Multiple agents** (page 44) can be installed on the same machine, each pointing to a different server.
- A **check-in icon** (page 15) displays next to each machine ID in the VSA, displaying the overall status of the managed machine. For example, the  check-in icon indicates an agent is online and the user is currently logged on.
- Clicking a check-in icon displays a single machine interface for the managed machine called **Live Connect** (page 15). **Live Connect** provides instant access to comprehensive data and tools you need to work on that one machine.
- Hovering the cursor over a check-in icon displays an **agent quick view window** (page 16) immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent quick view window.

Agents - Apple

Apple agents support the following functions:

- Audits - selected hardware and software attributes
- Agent procedures
- Remote Control
- FTP
- SSH
- Reset Password
- Task Manager
- Live Connect including Desktop Access.
 - On Apple Leopard (Intel) and above, including Lion and Mountain Lion, you can use Desktop Access in Live Connect to remote control a Windows system using Firefox or Safari.
 - On Windows using any of our supported browsers you can use Desktop Access to remote control a Apple Leopard (Intel) and above, including Lion and Mountain Lion.
- Desktop session recording via Remote Control and Quick View, for Snow Leopard and above, including Lion and Mountain Lion
- LAN Watch via Discovery
- Supported monitoring:
 - SNMP monitoring
 - Process monitoring in monitor sets
 - System Check
 - Log Parser

See **System Requirements** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm>).

Agents - Linux

Linux agents support the following functions:

- Agent procedures
- Latest audits, baselines audits and system audits
- Remote control and FTP with VNC
- SSH
- Reset Password
- LAN Watch and Install Agents - See [Installing Linux Agents](#) (page 46).
- Alerts
- Monitoring of Processes
- Monitoring of SNMP
- Log Parser
- Site Customization - The [Agent Icons](#) tab now includes a set of icons for Linux agents you can customize.
- Only non-plug-in specific items are accessible via a Linux-based Browser or when browsing to Linux agent machine. This is the following:
- Live Connect - Only non-plug-in specific items are accessible via a Linux-based browser or when browsing to a Linux agent machine. Supported menu options include:
 - Home
 - Agent Data
 - Audit Information
 - Ticketing (or Service Desk Ticketing)
 - Chat
 - Video Chat

See [System Requirements](#) (<http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm>).

Alarms - Suspending

The [Suspend Alarms](#) page suppresses [alarms](#) (page 550) for specified time periods, including recurring time periods. This allows upgrade and maintenance activity to take place without generating alarms. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms.*

Alert

Alerts are responses to [alert conditions](#) (page 551). This differs from an [audit](#) (page 551), which simply collects selected data for reference purposes without regard to any criteria.

Alerts have two meanings, generic and specific:

Generic Alerts

Typically there are four types of alert responses to an alert condition:

- Create [Alarm](#)
- Create [Ticket](#)
- Run Procedure
- [Email Recipients](#)

Defining an alert sets the [ATSE response code](#) (page 550) for that machine ID or SNMP device.

Alerts are defined using:

- Monitor > [Alerts](#) (page 248)
- Monitor > [Assign Monitoring](#) (page 286)
- Monitor > [Assign SNMP](#) (page 297)
- Monitor > [System Checks](#) (page 293)

Glossary

- Monitor > [Parser Summary](#) (page 309)
- Monitor > [Assign Parser Sets](#) (page 317)
- Patch Management > Patch Alerts
- Remote Control > Offsite Alerts
- Backup > Backup Alerts
- Security > Apply Alarm Sets
- Discovery > [LAN Watch](#) (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>)

Specific Alerts

The **Alerts** page enables you to quickly define alerts for typical **alert conditions** (page 551) found in an IT environment. For example, low disk space is frequently a problem on managed machines. Selecting the **Low Disk** type of alert displays a single additional field that lets you define the % free space threshold. Once defined, you can apply this alert immediately to any machine ID displayed on the **Alerts** page and specify actions to take in response to the alert.

Alert Actions

Creating an alarm represents only one *type of action* that can be taken when an alert occurs. Two other types of actions are notifications. They include **send an email** or **create a ticket**. A fourth type of action is to **run an agent procedure** to automatically respond to the alert. These four types of actions are called the **ATSE code**. Whether assigned to a machine ID, a group ID, or an SNMP device, the ATSE code indicates which types of actions will be taken for the alert defined.

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

None of the ATSE actions are required to be set when configuring an alert. Both the alert and the ATSE action, including no action, are reported in the Info Center > Monitor - **Monitor Action Log** (page 195) report.

Alert Types

Alerts are one of several **monitor types** (page 558).

- 1 - Admin account disabled
- 2 - Get File change alert
- 3 - New Agent checked in for the first time
- 4 - Application has been installed or deleted
- 5 - Agent Procedure failure detected
- 6 - NT Event Log error detected
- 7 - Kaseya Server stopped
- 8 - Protection violation detected.
- 9 - PCI configuration has been changed
- 10 - Disk drive configuration change
- 11 - RAM size changed.
- 12 - Test email sent by serverInfo.asp
- 13 - Scheduled report completed
- 14 - LAN Watch alert type
- 15 - agent offline
- 16 - low on disk space
- 17 - disabled remote control
- 18 - agent online
- 19 - new patch found
- 20 - patch path missing
- 21 - patch install failed
- 23 - Backup Alert

Alert Types

Types of alerts include:

- Discovery > **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>)
- Backup > Backup Alerts
- Monitor > **Alerts** (page 248) - These are specialized "fixed" alerts that are ready to apply to a machine.
- Monitor > **Assign Monitoring** (page 286)
- Monitor > **SNMP Traps Alert** (page 283)
- Monitor > **Assign SNMP** (page 297)
- Monitor > **System Checks** (page 293)
- Monitor > **Parser Summary** (page 309)
- Monitor > **Assign Parser Sets** (page 317)
- Patch Management > Patch Alerts
- Remote Control > Offsite Alerts
- Security > Apply Alarm Sets

Other add-on modules have alerts not listed here.

Alerts

An alert is created when the performance of a machine or device matches a pre-defined criteria or "alert condition".

Audit

Agents (page 547) can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the Kaseya Server so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per day is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machines's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > **Reporting** (page 142) > Reports are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two **alert** (page 248) types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes**.

Auto Learn Monitor Sets

You can enable **Auto Learn** alarm thresholds for any standard monitor set you assign to selected machine IDs. This automatically fine-tunes alarm thresholds based on actual performance data on a per machine basis.

Each assigned machine collects performance data for a specified time period. During that time period no alarms are triggered. At the end of the auto learn session, the alarm threshold for each assigned machine is adjusted automatically based on the actual performance of the machine. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized monitor sets.

Backup Sets

All files required for a full backup, including all incremental or differential backups, are saved together in a **backup set**.

Glossary

Canonical Name









The primary name for an object in DNS. Each object can also have an unlimited number of aliases.

Chat

Online [chat](#) is a text-based, instant messaging system. It is included with the Kaseya Server primarily to provide immediate technical support. VSA users can chat with machine users and/or chat with other VSA users currently logged on the same Kaseya Server. VSA users can enable or disable the machine user's ability to initiate chat sessions with VSA users. Since Kaseya chats are relayed through the Kaseya Server, all chats are protected by the Kaseya 256 bit rolling encryption protocol.

Check-in Status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the [agent quick view window](#) (page 16).

-  Online but waiting for first audit to complete
-  Agent online
-  Agent online and user currently logged on.
-  Agent online and user currently logged on, but user not active for 10 minutes
-  Agent is currently offline
-  Agent has never checked in
-  Agent is online but remote control has been disabled
-  The agent has been suspended

Check-in: Full vs. Quick

A **full check-in** occurs when an agent completes the processing of any and all outstanding tasks assigned to it by the Kaseya Server. These tasks can include processing an agent procedure, posting cached log data, or refreshing the agent configuration file. A full check-in occurs if 24 hours elapses without a specific task requiring it. A **quick check-in** occurs when an account checks in at the configured check-in interval, indicating to the Kaseya Server that the managed machine is still online. This doesn't require the completion of all outstanding tasks. Some functions require a full check-in before an agent can begin processing a new task. For example, System > [Naming Policy](#) (page 358). You can force a full check-in by right-clicking the agent icon in the system tray of a managed machine and clicking the [Refresh](#) option.

Collection

Collections are a free-form selection of *individual machine IDs within a view*. It doesn't matter which groups the machine IDs belong to, so long as the VSA user is authorized to have access to those groups. This enables the VSA user to view and report on logical collections of related machine IDs, such as laptops, workstations, servers, MS Exchange Servers, etc. Collections are created using the [Only show selected machine IDs](#) checkbox in [View Definitions](#) (page 24). Save a view first before selecting machines IDs using this option. Once the view is saved, a [<N> machines selected](#) link displays to the right of this option. Click this link to display a [Define Collection](#) window, which allows you to create a view using a free-form selection of individual machine IDs.

Note: The [Filter Aggregate Table](#) (page 27) provides an alternate method of selecting machine IDs for a view definition, based on standard and user defined attributes.

Copy Settings and Templates

[Machine ID templates](#) (page 557) are initially used to create an agent install package using the template as the source to copy settings from. But even after agents are installed on managed machines, you'll need to update settings on existing machine ID accounts as your customer requirements change and your knowledge of the VSA grows. In this case use Agent > [Copy Settings](#) to copy these changes to any number of machines IDs you are authorized to access. Be sure to select [Do Not Copy](#) for any settings

you do not want to overwrite. Use **Add** to copy settings without removing existing settings. Kaseya recommends making changes to a selected template first, then using that template as the source machine ID to copy changes from. This ensures that your machine ID templates remain the "master repositories" of all your agent settings and are ready to serve as the source of agent install packages and existing machine ID accounts.

Credentials

A credential is a username and password used to authenticate a user or process's access to a machine or network or some other resource.

Agent Credentials

Specify a *single* credential with administrator privileges for an agent to use, using the Agent > **Set Credentials** (page 68) page.

Managed Credentials

Specify *additional* credentials at three different levels: by organization, by machine group and by individual machine or device. They are managed using three navigation items in the **Audit** module:

- **View Assets** (page 123) - Use this page to create multiple credentials for an *individual* machine or device.
- **Manage Credentials** (page 126) - Use this page to create multiple credentials for *organizations* and *machine groups* within organizations.
- **Credentials Log** (page 127) - This page logs the creation, display and deletion of managed credentials.

Once created, use managed credentials:

- To instantly lookup all the credentials that apply to a machine you're working on. The **Quick View** popup window now includes a **View Credentials** option. Access is controlled by role and by scope. You can add a description for each credential.
- As the source credential for an agent credential in a policy. Check the **Use organization defaults** checkbox in the **Credential** setting of the Policy Management > Policies page to establish the link.

Note: A managed credential can not overwrite the Agent > **Set Credentials** (page 68) directly. The managed credential must be applied to a policy and the policy applied to the machine.

If multiple credentials are defined for a machine, then the most local level defined has precedence: by individual machine, by machine group, or by organization. At any one level, only one managed credential can be designated the source credential for an agent credential.

Current VSA Time

The current time used by the Kaseya Server is displayed in System > **Preferences** (page 353).

Dashboard

The dashboard is a summary display of the status of the entire system. The dashboard's data is filtered by the **machine ID / group ID filter** (page 556). Navigation: Info Center > **View Dashboard** (page 210).

Dashboard List

The dashboard list is a summary display of the alarm statuses of all machines being monitored. The dashboard list's data is filtered by the **machine ID / group ID filter** (page 556). Navigation: Info Center > **Dashboard List** (page 219) or Monitor > Dashboard List.

Distribute File

The **Distribute File** function sends files stored on your VSA server to managed machines. It is ideal for mass distribution of configuration files, such as virus foot prints, or maintaining the latest version of executables on all machines. The VSA checks the integrity of the file every **full check-in** (page 552). If the

Glossary

file is ever deleted, corrupted, or an updated version is available on the VSA, the VSA sends down a new copy prior to any procedure execution. Use it in conjunction with recurring procedures to run batch commands on managed machines.

Event Logs

An **event log service** runs on Windows operating systems (Not available with Win9x). The event log service enables event log messages to be issued by Window based programs and components. These events are stored in event logs located on each machine. The event logs of managed machines can be stored in the Kaseya Server database, serve as the basis of alerts and reports, and be archived.

Depending on the operating system, the **event log types** available include but are not limited to:

- Application log
- Security log
- System log
- Directory service log
- File Replication service log
- DNS server log

Windows events are further classified by the following **event log categories**:

- Error
- Warning
- Information
- Success Audit
- Failure Audit
- Critical - Applies only to Vista, Windows 7 and Windows Server 2008
- Verbose - Applies only to Vista, Windows 7 and Windows Server 2008

Event logs are used or referenced by the following VSA pages:

- Monitor > **Agent Logs** (*page 31*)
- Monitor > **Event Log Alerts** (*page 276*)
- Monitor > Event Log Alerts > **Edit Event Sets** (*page 280*)
- Monitor > **Update Lists by Scan** (*page 232*)
- Agent > **Log History** (*page 32*)
- Agent > **Event Log Settings** (*page 34*)
- Agent > **Agent Logs** (*page 31*)
- Reports > **Logs** (*page 556*)
- **Live Connect** (*page 344*) > Event Viewer
- **Quick View** (*page 16*) > Event Viewer
- System > Database Views > **vNtEventLog** (*page 448*)

Events Sets

Because the number of events in Windows **events logs** (*page 554*) is enormous the VSA uses a record type called an **event set** to filter an alert condition. Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** (*page 554*) entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to. For details on how to configure event sets, see Monitor > Event Log Alerts > **Edit Event Sets** (*page 280*).

Feature Set

A feature set provides advanced, specialized functionality that is typically hidden in the basic module. The basic module must be installed and the feature licensed separately to display feature set options.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. The **FTP server** is the program on the target machine that listens on the network for connection requests from other computers. The **FTP client** is the program on the VSA user's local machine that initiates a connection to the server. The FTP client machine requires user access rights to the FTP server machine. It is included with the Kaseya Server primarily to provide immediate technical support. Once connected, the client can upload files to the server, download files from the server, rename or delete files on the server and so on. Any software company or individual programmer is able to create FTP server or client software because the protocol is an open standard. Virtually every computer platform supports the FTP protocol. Since Kaseya FTP sessions are relayed through the Kaseya Server, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.

Flood Detection

If 1000 events—not counting **black list events** (page 555)—are uploaded to the Kaseya Server by an agent *within one hour*, further collection of events of that log type are stopped for the remainder of that hour. A new event is inserted into the event log to record that collection was suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your Kaseya Server. Alarm detection and processing operates regardless of whether collection is suspended.

Global Event Log Black Lists

Each agent processes all events, however events listed on a "black list" are *not* uploaded to the VSA server. There are two black lists. One is updated periodically by Kaseya and is named `EvLogBlkList.xml`. The second one, named `EvLogBlkListEx.xml`, can be maintained by the service provider and is not updated by Kaseya. Both are located in the `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles` directory. Alarm detection and processing operates regardless of whether entries are on the collection blacklist.

Group Alarms

Alarms for alerts, event log alerts, system check, and log monitoring are automatically assigned to a **group alarm** category. If an alarm is created, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the **Group Alarm Status** (page 223) dashlet of the Monitor > **Dashboard List** page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > **Monitor Lists** (page 231). Group alarm column names are assigned to monitor sets using **Define Monitor Set** (page 235).

Host name

The text equivalent of an IP address. For example, the IP address `89.234.7.197` should resolve to the host name of `www.kaseya.com`.

ISO Image

An **ISO image (.iso)** is a disk image of an ISO 9660 file system. ISO 9660 is an international standard originally devised for storing data on CD-ROM. In addition to the data files that are contained in the ISO image, the ISO image also contains all the filesystem metadata, including *boot code*, structures, and attributes. All of this information is contained in a single file. CD writers typically provide the option of writing an ISO file *as an image* when writing to a CD.

LAN Watch

LAN Watch in the **Discovery** module uses an existing VSA **agent** (page 547) on a managed machine to scan a local area network for any and all new devices connected to that LAN since the last time LAN Watch ran. These new devices can be workstations and servers without agents, **SNMP devices** (page 562) and vPro machines. Optionally, the VSA can send an **alert** (page 549) when a LAN Watch discovers any new device. LAN Watch effectively uses the agent as a proxy to scan a LAN behind a firewall that might not be accessible from a remote server.

Log Monitoring

The VSA is capable of monitoring data collected from many **standard log files** (page 556). **Log Monitoring** extends that capability by extracting data from the output of any text-based log file. Examples include application log files and **syslog** (page 564) files created for Unix, Linux, and Apple operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the Kaseya Server database, **Log Monitoring** uses **parser definitions and parser sets** (page 559) to parse each log file and select only the data you're interested in. Parsed messages are displayed in Log Monitoring, which can be accessed using the Agent Logs tab of **Live Connect** (page 344) > Agent Data or the **Machine Summary** (page 131) page or by generating a report using the Agent > Logs - **Log Monitoring** (page 192) page. Users can optionally trigger alerts when a **Log Monitoring** record is generated, as defined using **Assign Parsing Sets** (page 317) or **Parser Summary** (page 309).

Logs

Logs collect event information about multiple systems, including the Kaseya Server. The different types of logs that can be generated are:

- **Admin Notes** - Lists user notes, sorted by user.
- **Agent Log** - Shows a list of activity associated with the Agent machine Agent. Start and stop times, .ini file changes, and other information is captured. The date and time of each activity is also noted.
- **Agent Procedure Log** - Shows a list of procedures executed on the selected agent machine. The date and time of each procedure execution is also noted, as well as whether it completed successfully or not.
- **Alarm Log** - List out all triggered alarms issued against the selected machine.
- **Configuration Changes** - Shows a log of changes made by a user to a managed machine's agent configuration.
- **Event Logs** - Shows the **event log** (page 554) data collected by Windows. (Not available with Win9x)
- **Log Monitoring** - enables you to monitor the data generated by any text-based log.
- **Monitor Action Log** - The log of **alert conditions** (page 551) that have occurred and the corresponding actions, if any, that have been taken in response to them.
- **Network Statistics** - Shows a list of applications that have accessed the network and the packet size of the information exchanged during the network access session. The time of the exchange is also listed.
- **Remote Control Log** - Lists successful remote controls sessions.

MAC address

The unique **media access control (MAC)** identifier assigned to network adapter cards (NICs).

Machine ID / Group ID / Organization ID

Each **agent** (page 547) installed on a managed machine is assigned a unique **machine ID / group ID / organization ID**. All machine IDs belong to a machine group ID and optionally a subgroup ID. All machine group IDs belong to an organization ID. An organization typically represents a single customer account. If an organization is small, it may have only one machine group containing all the machine IDs in that organization. A larger organization may have many machine groups and subgroups, usually organized by location or network. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.sales.chicago.acme`. In this case `sales` is a subgroup ID within the `chicago` group ID within the organization ID called `acme`. In some places in the VSA, this hierarchy is displayed in reverse order. Each organization ID has a single default machine group ID called `root`. Group IDs and subgroup IDs are created using the System > Orgs/Group/Depts/Staff > Manage > **Machine Groups** (page 374) page.

Machine ID / Group ID filter

The Machine ID / Machine Group filter is available on all tabs and functions. It allows *you*—rather than an administrator—to limit the machines displayed on *all* function pages. The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each

machine—for example, the operating system type. Once filter parameters are specified, click the **Apply** button to apply filter settings to *all* function pages. By default, the Machine ID / Group ID filter displays all machine IDs in <A11 Groups> managed by the currently logged on VSA user.

Note: Even if a VSA user selects <A11 Groups>, only groups the VSA user is granted access to using System > User Security > **Scopes** (page 369) are displayed.

Machine ID Template

A machine ID template is *a machine ID record without an agent*. Since an agent never checks into a machine ID template account, it is not counted against your total license count. You can create as many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are typically copied from a selected machine ID template. Machine ID templates are usually created and configured for certain types of machine. Machine type examples include desktops, Autocad, QuickBooks, small business servers, Exchange servers, SQL Servers, etc. **A corresponding install package can be created based on each machine ID template you define.**

- Create machine ID templates using Agent > **Create** (page 48).
- Import a machine ID template using Agent > **Import/Export** (page 57).
- Base an agent install package on a machine ID template using Agent > **Deploy Agents** (page 35).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > **Copy Settings** (page 55).
- Identify the total number of machine ID template accounts in your VSA using System > **Statistics** (page 389).
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.
- Separate machine ID templates are recommended for Windows, Apple and Linux machines. Alternatively you can create a package that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the **machine ID / group ID / organization ID** (page 556) and the **agent** (page 547). The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

Machine Roles

The **Machine Roles** (page 365) page creates and deletes machine roles. Machine roles determine what *machine users* see when they use **Portal Access** (page 67)—a version of **Live Connect** (page 344)—from a machine with an agent. The **Portal Access** window displays when a *machine user double-clicks the agent icon in the system tray of their managed machine*.

Note: The **User Roles** page determines what *VSA users* see when they use **Live Connect** from within the VSA.

Within the **Machine Roles** page you can select:

- **Members** (page 368) - Assign or remove machines for a machine role.
- **Access Rights** (page 368) - Select the access rights for a machine role. Access rights determine the functions a *machine user* can access.
- **Role Types** (page 368) - Assign or remove role types for a machine role. Currently there is only one machine role type provided and no access rights are restricted.

Managed Machine

A monitored machine with an installed **agent** (page 547) and active **machine ID / group ID** (page 557) account

Glossary

on the Kaseya Server. Each managed machine uses up one **agent license** (page 386).

Master User / Standard User

A master user is a VSA **user** (page 564) that uses a **Master** user role and a **Master** scope. The **Master** user role provides user access to all functions throughout the VSA. The **Master** scope provides access to all scope data objects throughout the VSA. A **Master** user role can be used with a **non-Master** scope, but a **Master** scope cannot be used with a **non-Master** role. Kaseya Server management configuration and other **specialized functions** (page 365) can only be performed by **Master** role users. The term *standard user* is sometimes used to indicate a user that does not use a **Master** user role and a **Master** scope.

Migrating the Kaseya Server

For the latest instructions on migrating an existing Kaseya Server to a new machine see *Moving the Kaseya Server* section in the latest **Kaseya Server installation instructions** (<http://help.kaseya.com/webhelp/EN/VSA/7000000/Install/index.asp#home.htm>).

Monitor Sets

A monitor set is a set of **counter objects**, **counters**, **counter instances**, **services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter** (page 560), service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** (page 231).
2. Create and maintain monitor sets using Monitor > **Monitor Sets** (page 234).
3. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** (page 286).
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.
6. Review monitor set results using:
 - Monitor > **Monitor Log** (page 291)
 - Monitor > **Live Counter** (page 230)
 - Monitor > Dashboard > **Network Status** (page 223)
 - Monitor > Dashboard > **Group Alarm Status** (page 223)
 - Monitor > Dashboard > **Monitoring Set Status** (page 224)
 - Info Center > Reporting > Reports > Monitor > Monitor Set Report
 - Info Center > Reporting > Reports > Monitor > Monitor Action Log

Monitor Types

- 0 - Counter
- 1 - Service
- 2 - Process
- 3 - SNMP
- 4 - Alert - Alerts are further classified using **alert types** (page 550).
- 5 - System Check
- 6 - EPS
- 7 - Log Monitoring

myOrg

myOrg is the **organization** (page 559) of the service provider using the VSA. All other organizations in the

VSA are second party organizations doing business with myOrg. The default name of myOrg, called My Organization, should be renamed to match the service provider's company or organization name. *This name displays at the top of various reports to brand the report.* Agents installed to internally managed machines can be assigned to this organization. *VSA user logons are typically associated with staff records in the myOrg organization.* myOrg cannot be assigned a parent organization.

On Premises

An **on premises** hardware/software installation of the VSA is maintained by a service provider and typically used only by the service provider. See **Software as a Service (SaaS)** (page 564).

Org

The VSA supports three different kinds of business relationships:

- **Organizations** - Supports machine groups and manages machines using agents.
- **Customers** - Supports the billing of customers using **Service Billing**.
- **Vendors** - Supports the procurement of materials using **Service Billing**.

The Org table is a support table shared by *organizations*, *customers* and *vendors*. Each record in the Org table is identified by a unique orgID. The Org table contains basic information you'd generally need to maintain about any kind of business relationship: mailing address, primary phone number, duns number, yearly revenue, etc. Because the Org table is shared, you can easily convert:

- A customer into an organization or vendor.
- A vendor into an organization or customer.
- An organization into a customer or vendor.

Note: myOrg (page 558) is the organization of the service provider using the VSA.

Packager

The **Packager** is a wizard tool used to create a package when a pre-defined install solution cannot be used. **Packager** evaluates the state of a source machine before and after an installation and/or resource change. The **Packager** compiles the differences into a single executable file—the **package**—that can be distributed via agent procedures to any managed machine. Distribute a package any way you choose. You can email it, or store it on a server where a **custom procedure** (page 80) can perform a silent installation on any managed machine.

Parser Definitions and Parser Sets

When configuring **Log Monitoring** (page 555) it's helpful to distinguish between two kinds of configuration records: **parser definitions** and **parser sets**.

A **parser definition** is used to:

- Locate the log file being parsed.
- Select log data based on the log data's *format*, as specified by a template.
- Populate parameters with log data values.
- Optionally format the log entry in **Log Monitoring**.

A **parser set** subsequently *filters* the selected data. Based on the *values* of populated parameters and the criteria you define, a parser set can generate log monitoring entries and optionally trigger alerts. Without the filtering performed by the parser set, the Kaseya Server database would quickly expand. For example a log file parameter called \$FileServerCapacity\$ might be repeatedly updated with the latest percentage of free space on a file server. Until the free space is less than 20% you may not need to make a record of it in **Log Monitoring**, nor trigger an alert based on this threshold. Each parser set applies only to the parser definition it was created to filter. Multiple parser sets can be created for each parser definition. Each parser set can trigger a separate alert on each machine ID it is assigned to.

Patch Policy

Patch policies contain all active patches for the purpose of approving or denying patches. An active

Glossary

patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be members of this patch policy and another patch policy named `workstations` and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- Initial Update and Automatic Update require patches be approved before these patches are installed.
- Approval by Policy approves or denies patch by *policy*.
- Approval by Patch approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- KB Override overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- Patch Update and Machine Update can install denied patches.
- Non-Master role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

Patch Update Order

Service packs and patches are installed in the following order:

1. Windows Installer
2. OS related service packs
3. OS update rollups
4. OS critical updates
5. OS non-critical updates
6. OS security updates
7. Office service packs
8. Office update rollups
9. All remaining Office updates

Note: Reboots are forced after each service pack and at the end of each patch group without warning. This is necessary to permit the re-scan and installation of the subsequent groups of patches.


Performance Objects, Instances and Counters

When setting up counter thresholds in **monitor sets** (page 558), it's helpful to keep in mind exactly how both Windows and the VSA identify the components you can monitor:

- **Performance Object** - A logical collection of counters that is associated with a resource or service that can be monitored. For example: processors, memory, physical disks, servers each have their own sets of predefined counters.
- **Performance Object Instance** - A term used to distinguish between multiple performance objects of the same type on a computer. For example: multiple processors or multiple physical disks. The VSA lets you skip this field if there is only one instance of an object.

- **Performance Counter** - A data item that is associated with a performance object, and if necessary, the instance. Each selected counter presents a value corresponding to a particular aspect of the performance that is defined for the performance object and instance.

Portal Access

Portal Access is a **Live Connect** (page 344) session initiated by the machine user. The machine user displays the **Portal Access** page by clicking the agent icon  on the system tray of a managed machine. **Portal Access** contains machine user options such as changing the user's contact information, creating or tracking trouble tickets, chatting with VSA users or remote controlling their own machine from another machine. **Portal Access** logons are defined using Agent > **Portal Access** (page 67). The function list the user sees during a **Portal Access** session is determined by the System > **Machine Roles** (page 367) page. You can customize **Portal Access** sessions using the System > Customize > **Live Connect** (page 398) page. Both the **Live Connect** and **Portal Access** plug-in installers can be pre-installed using the Agent > **Update Agent** (page 72) page.

Primary Domain Controller

Primary domain controllers have full access to the accounts databases stored on their machines. Only primary domain controllers run **Active Directory** (page 547).

Private Folders


Private Folders

Objects you create—such as reports, procedures, or monitor sets—are initially saved in a folder with your user name underneath a **Private** cabinet. This means only you, the creator of the objects in that folder, can view those objects, edit them, run them, delete them or rename them.

To share a private object with others you first have to drag and drop it into a folder underneath the **Shared** cabinet.

Note: A master role user can check the **Show shared and private folder contents from all users** checkbox in System > Preferences (page 353) to see all shared and private folders. For Private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

Quick Status

A **Quick Status** feature enables you to select *any* monitor set counter, service or process from *any* machine ID and add it to the same single display window. Using **Quick Status**, you can quickly compare the performance of the same counter, service or process on different machines, or display selected counters, services and processes from different monitor sets all within a single view. SNMP sets provide a similar **Quick Status** view for selected SNMP objects. *Any Quick Status view you create exists only for the current session.* The **Quick Status** window is accessed using Monitor > Dashboard > **Monitoring Set Status** (page 224), then clicking the **Quick Status** link or the **Quick Status** icon .

Quick View

Hovering the cursor over a check-in icon displays an agent **Quick View** window immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent **Quick View** window. You can use **agent badges** (page 16) to display **Special Instructions** text in the bottom of the the **Quick View** window.

Record Desktop

Applies to WinVNC only. When enabled a video of the desktop is recorded and the recorded desktop session is left in the working directory of the agent machine. Typically a desktop session video enables a user to see what an administrator did on their box during the recording. This protects the administrator from being accused of making unauthorized changes to the machine. Desktop session videos can be accessed on the working directory of the remote machine. Applies to Windows and Apple machines only. **Record Desktop** sessions can be started and stopped from the following locations:

Glossary

- **Recording every remote control session** - A **Record remote control to a file in the machine working directory** checkbox can be checked on the **User Role Policy** (page 333) and **Machine Policy** (page 334) pages in the **Remote Control** module. Every remote control session that uses these policies are automatically recorded.
- **Recording a single remote control session** - A **Record remote control to a file in the machine working directory** checkbox can be checked on the **Control Machine** (page 326) page prior to launching a single remote control session on a machine.
- **Recording without a remote control session** - A **Record Desktop** button in the **Quick View** (page 16) records the desktop without launching a remote control session.

Silent Install

Silent installs, also called **silent deploys**, do not prompt the user for input. Silent installs may not require user input or else provide a typical configuration that serves the purposes of most users, or else provide command line parameters that enable users to configure the installation at execution. If an install does not support a silent install but still needs to be distributed automatically, users can use **Packager** (page 559) to create a custom installation package. See **Creating Silent Installs** (page 115).

SNMP Community

An SNMP community is a grouping of devices and management stations running SNMP. SNMP information is broadcast to all members of the same community on a network. SNMP default communities are:

- Write = private
- Read = public

SNMP Devices

Certain network devices such as printers, routers, firewalls, servers and UPS devices can't support the installation of an **agent** (page 547). But a VSA agent installed on a managed machine on the same network as the device can read or write to that device using **simple network management protocol (SNMP)**.

SNMP Quick Sets

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>) is performed. You can use the list of discover MIB objects to instantly create a device-specific SNMP set—called a **quick set**—and apply it to the device. Once created, quick sets are the same as any standard set. They display in your private folder in Monitor > **SNMP Sets** and in the drop-down list in Monitor > **Assign SNMP**. A (QS) prefix reminds you how the quick set was created. Like any other standard set, quick sets can be *individualized* for a single device, used with Auto Learn, shared with other users, and applied to similar devices throughout the VSA.

1. Discover SNMP devices using Monitor > **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 297).
3. Click the hyperlink underneath the name of the device, called the **SNMP info** (page 302) link, in the **Assign SNMP** page to display a dialog.
 - Click **Discovered MIB Objects** and select one or more of the MIB objects that were discovered on the SNMP device you just selected.
 - Click **Quick Set Items** and, if necessary, edit the alarm thresholds for selected MIB objects.
 - Enter a name after the (QS) prefix in the header of the dialog.
 - Click the **Apply** button to apply the quickset to the device.
4. Display SNMP monitoring data returned by the quick set using Monitor > **SNMP Log** (page 305), the same as you would for any other standard SNMP set.
5. Optionally maintain your new quick set using Monitor > **SNMP Sets** (page 562).

SNMP Sets

A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** (page 562). The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 562) are the easiest method of implementing SNMP monitoring on a device.
- **SNMP standard sets** - These are usually generic SNMP sets that are maintained and applied to multiple devices. A quick set, once created, can be maintained as a standard set.
- **SNMP individualized sets** - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP auto learn** - This is a standard SNMP set that is applied to an individual device and then adjusted automatically using auto learn.
- **SNMP types** - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** (page 563) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Discovery > **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 297). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 305) or **Dashboard List** (page 219).

The following additional SNMP functions are available and can be used in any order.

- Optionally review the list of all imported SNMP objects using Monitor > **Monitor Lists** (page 231).
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 241).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 246).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** (page 308).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 306).

SNMP Types

Most SNMP devices are classified as a certain type of SNMP device using the MIB object `system.sysServices.0`. For example, some routers identify themselves as routers generically by returning the value 77 for the `system.sysServices.0` MIB object. You can use the value returned by the `system.sysServices.0` MIB object to auto assign SNMP sets to devices, as soon as they are discovered by a LAN Watch.

Note: The entire OID for `system.sysServices.0` is `.1.3.6.1.2.1.1.7.0` or `.iso.org.dod.internet.mgmt.mib-2.system.sysServices.`

You can assign **SNMP sets** (page 562) to **devices** (page 562) *by type automatically* as follows:

1. Add or edit SNMP *types* using the **SNMP Device** tab in Monitor > **Monitor Lists** (page 231).
2. Add or edit the value returned by the MIB object `system.sysServices.0` and associated with each SNMP *type* using the **SNMP Services** tab in Monitor > **Monitor Lists**.
3. Associate a SNMP *type* with a SNMP *set* using the **Automatic Deployment to** drop-down list in Monitor > SNMP Sets > **Define SNMP Set** (page 243).
4. Perform a **LAN Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/7000000/index.asp#1944.htm>). During the LAN Watch SNMP devices are automatically assigned to be monitored by SNMP sets if the SNMP device returns a value for the `system.sysServices.0` MIB object that matches the SNMP type associated with those SNMP sets.

Glossary

You can also assign **SNMP sets** (page 562) to **devices** (page 562) *manually* as follows:

- Assign a SNMP type to an SNMP device using Monitor > **Set SNMP Type** (page 308). Doing so causes SNMP sets using that same type to start monitoring the SNMP device.

Software as a Service (SaaS)

Kaseya provides "software as a service" (SaaS) deployment of **Virtual System Administrator™**. Service providers contract with Kaseya to access a VSA hosted and maintained by Kaseya and can install a specified number of their customer agents. Service providers are allocated a unique *tenant partition* of a shared Kaseya Server and database. Within their assigned partition, service providers can only see their own organizations, machine groups, procedures, reports and tickets. Service providers in a tenant partition have full access to all the functions of the VSA except system maintenance, which is the responsibility of Kaseya. See **On Premises** (page 559).

syslog

Syslog is a standard for forwarding log messages in an IP network to a syslog server. A syslog server collects the messages broadcast by various devices on the network and integrates them into a centralized repository of syslog files. Syslog is commonly used by Unix, Linux and Apple operating systems and hardware devices such as Cisco routers. **Log Monitoring** (page 555) enables you to monitor syslog files.

A typical format for a syslog file entry is:

```
<time> <hostname> <tag>:<message>
```

For example:

```
Oct 15 19:11:12 Georges-Dev-Computer kernel[0]: vmnet: bridge-en1: interface en is going DOWN
```

System Agent Procedures

System agent procedures are basic functions that are exposed by the VSA. You can schedule system agent procedures to run automatically. They cannot be edited nor can they accept parameters. A list of available system agent procedures displays in any Agent Procedure Search popup window. System agent procedures can be run from:

- Within a parent procedure using the **executeProcedure()** or **scheduleProcedure()** commands of an **IF-ELSE-STEP** (page 84) statement.
- Any alerts page using the **Run Agent Procedure** checkbox.
- The **Pending Procedures** tab in **Live Connect** (page 344) or the **Machine Summary** (page 131) page.

Because a system agent procedure can be run using an alert or parent agent procedure associated with a specific machine ID account, the scheduling of a system agent procedure can be copied, typically from a machine ID template to a machine using Agent > **Copy Settings** (page 55).

System Checks

The VSA can monitor machines that *don't have an agent installed on them*. This function is performed entirely within a single page called **System Check**. Machines without an agent are called **external systems**. A machine with an agent is assigned the task of performing the system check on the external system. A system check typically determines whether an external system is available or not. Types of system checks include: web server, DNS server, port connection, ping, and custom.

System Tray

The system tray is located, by default, in the lower right-hand corner of the Windows desktop, in the Taskbar. It contains the system clock, and other system icons.


User Account

See **Machine IDs vs. Agents** (page 557)

Users

VSA users use the VSA application to maintain the Kaseya Server and oversee the monitoring of **managed machines** (page 557) by the Kaseya Server and its **agents** (page 547). VSA users are created using System > **Users** (page 360). Users also refers to machine users, who use the computers managed by the VSA. **Master users** (page 558) have special privileges throughout the VSA.

View Definitions

The **View Definitions** (page 24) window lets you further refine a machine ID / group ID filter based on attributes contained on each machine—for example, the operating system type. Views provide users flexibility for machine management and reporting. View filtering is applied to *all* function pages by selecting a view from the **Select View** drop-down list on the **machine ID / group filter** (page 23) panel and clicking the Apply icon . Any number of views can be created and shared with other users. Views are created by clicking the **Edit** button to the right of the **Views** drop-down list.

Virtual Machine

A virtual machine (VM) is a software implementation of a physical computer (machine) that executes programs like a physical computer. Virtual machines are capable of virtualizing a full set of hardware resources, including a processor (or processors), memory and storage resources and peripheral devices. The **Backup** module can convert a backup image into a VM. See Backup > Image to VM.

Virtual Network Computing (VNC)

Virtual Network Computing (VNC), also called **remote control** or **remote desktop**, is a graphical desktop sharing system which uses the Remote Framebuffer (RFB) protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network. It is included with the Kaseya Server primarily to provide immediate technical support. VNC is platform-independent. A VNC viewer on any operating system can usually connect to a VNC server on any other operating system. The **VNC server** is the program on the remote machine that shares its screen. The **VNC client (or viewer)** is the program on the local machine that watches and interacts with the remote machine. The VNC client machine requires user access rights to the VNC server machine. Since Kaseya VNC sessions are relayed through the Kaseya Server, all VNC sessions are protected by the Kaseya 256 bit rolling encryption protocol.

vPro

Intel® vPro™ Technology provides hardware-based management integration independent of operating system software and network management software. The VSA can discover vPro-enabled machines during a **LAN Watch** (page 555), list the hardware assets of vPro machines, access hardware-based security use the power management and remote booting of ISO images capabilities provided by vPro.

Windows Automatic Update

Windows Automatic Updates is a Microsoft tool that automatically delivers updates to a computer. Windows Automatic Updates is supported in the following operating systems: Windows 2003, Windows XP, Windows 2000 SP3 or later, and all operating systems released after these. Patch Management > Windows Auto Update can enable or disable this feature on managed machines. While Windows Millennium Edition (Me) has an Automatic Updates capability, it cannot be managed as the above operating systems can.

Work Types

Work types determine how time entries are integrated with other functions in the VSA. The work type options displayed in your VSA depend on the modules installed.

- **Admin Tasks** - A recurring operational activity not associated with any project.
- **Work Orders** - Only displays if the **Service Billing** is installed.
- **Service Desk Tickets** - Only displays if **Service Desk** 1.3 or later is installed.

Index

6

64-Bit Commands • 103

A

Access Policy • 410
 Action Buttons • 81
 Active Directory • 547
 Add / Edit Data Set • 168
 Add / Edit Report Template • 153
 Add SNMP Object • 246
 Add/Remove • 137
 AddIncident • 530
 AddIncident Request • 544
 AddIncident Response • 544
 AddMachGroupToScope • 482
 AddOrg • 482
 AddOrgDepartment • 482
 AddOrgDeptStaff • 482
 AddOrgToScope • 483
 AddScope • 483
 AddScopeOrg • 483
 AddScriptAssignment • 517
 AddScriptPrompt • 517
 AddServDeskToScope • 531
 AddTicRequest • 484
 AddUserToRole • 484
 AddUserToScope • 484
 AdminGroupAccess • 484
 Administrator Notes • 12
 Advanced Filtering • 27
 Agent • 19
 Agent Badges • 16
 Agent Icons • 21, 395
 Agent Install Command Line Switches • 42
 Agent Logs • 31
 Agent Menu • 59, 547
 Agent Overview • 20
 Agent Procedure API Web Service • 517
 Agent Procedure API Web Service - Operations • 517
 Agent Procedure Status • 110
 Agent Procedures • 79
 Agent Procedures Overview • 80
 Agent Settings • 547
 Agent Status • 28
 Agent Time • 80, 128, 384, 547
 Agent Time Scheduling • 547
 Agents • 14, 21, 548
 Agents - Apple • 548
 Agents - Linux • 549
 Alarm List • 220
 Alarm Network Status • 220
 Alarm Rotator • 222
 Alarm Summary • 227

Alarm Summary Window • 221
 Alarm Ticker • 223
 Alarms - Suspending • 549
 Alert • 549
 Alert Actions • 550
 Alert Types • 550, 551
 Alerts • 248, 551
 Alerts - Agent Procedure Failure • 262
 Alerts - Agent Status • 250
 Alerts - Application Changes • 253
 Alerts - Backup Alert • 271
 Alerts - Get Files • 255
 Alerts - Hardware Changes • 258
 Alerts - Low Disk • 260
 Alerts - New Agent Installed • 266
 Alerts - Patch Alert • 268
 Alerts - Protection Violation • 264
 Alerts - Summary • 248
 Alerts - System • 275
 Anti-Malware - Anti-Malware Installation Statistics • 179
 Antivirus - Antivirus Installation Statistics • 179
 API • 470
 API Web Services • 469
 Application Blocker • 77
 Application Deploy • 113
 Application Logging • 119, 392
 Approving / Rejecting Reports • 147
 Assign Event Set tab • 279
 Assign LAN Cache • 72
 Assign Monitoring • 286
 Assign Parser Sets • 317
 Assign SNMP • 297
 Assignee Policy • 411
 AssignEventAlertToMachine • 519
 AssignEventLogMachineSettings • 519
 AssignRole • 484
 AssignScope • 485
 Attachment • 525
 Audit • 121, 551
 Audit - Aggregate Table • 179
 Audit - Disk Utilization • 179
 Audit - Inventory • 180
 Audit - Machine Changes • 180
 Audit - Machine Summary • 180
 Audit - Network Statistics • 181
 Audit Overview • 122
 Audit Summary • 129
 Authenticate • 485
 AuthenticateWithAppSessionID • 487
 Auto Learn - Monitor Sets • 290
 Auto Learn - SNMP Sets • 304
 Auto Learn Monitor Sets • 551
 Automating the Installation of the Agent • 38

B

Backup - Backup • 182
 Backup Sets • 551
 Bar Chart • 158
 Bookmarks • 13

Index

C

- Cancel Script • 131
- Canonical Name • 552
- Change Group • 55
- Change Logon • 355
- Change Reporting Configuration • 382
- Changing Passwords Used by External Applications • 363
- Chat • 339, 552
- Check-in
 - Full vs. Quick • 552
- Check-In Control • 61
- Check-in Icons • 15
- Check-in Policy • 356
- Check-in Status • 552
- CloseAlarm • 487
- Collection • 552
- Color Scheme • 14, 393
- Configuration • 1
- Configure • 377
- Configure Column Sets • 131
- Configuring Agent Settings • 40
- Configuring Agent Settings Using Policies • 41
- Configuring Agent Settings Using Templates • 41
- Configuring the Server • 2
- Control Machine • 326
- Copy Settings • 55
- Copy Settings and Templates • 552
- Counter Thresholds • 236
- Cover Page, Header, Footer • 175
- Create • 48
- Create a New Master User • 362
- Create/View • 403
- CreateAdmin • 487
- CreateAgentInstallPackage • 487
- CreateEventSet • 519
- CreateEventSetDefinition • 519
- CreateMachineGroup • 488
- CreateRole • 488
- Creating / Editing Agent Procedures • 83
- Creating an Agent Install Package • 37
- Creating Custom Agent Icons • 396
- Creating Silent Installs • 115
- Credentials • 553
- Credentials Log • 127
- Crystal Reporting Usage • 420
- Current VSA Time • 553
- CustomField • 524
- Customize • 393
 - Live Connect • 398
- Customized New Ticket Link • 349

D

- Dashboard • 553
- Dashboard List • 219, 553
- Dashboard Settings • 227
- Data Backup Summary • 189
- Data Backup Usage Over Time • 189
- Data Filters • 145
- Data Table Column Options • 17
- Database Views • 417

- Database Views and Functions • 419
- Default Settings • 384
- Defaults • 176
- Define Monitor Sets • 235
- Define SNMP Set • 243
- Delete • 52
- Delete/Archive • 405
- DeleteAdmin • 488
- DeleteAgent • 489
- DeleteAgentInstallPackage • 489
- DeleteAllEventAlertsFromMachine • 520
- DeleteAllEventLogMachineSettings • 520
- DeleteEventAlertFromMachine • 520
- DeleteEventLogMachineSettings • 520
- DeleteEventSet • 520
- DeleteEventSetDefinition • 521
- DeleteMachineGroup • 489
- DeleteOrg • 489
- DeleteRole • 490
- DeleteScope • 490
- Deploy Agents • 35
- Deploy Header • 395
- Desktop Management - Power Savings • 182
- Desktop Management - User State • 184
- Device Status • 226
- DisableAdmin • 490
- Distribute File • 118, 553
- Distribution • 109
- Documents • 138
- Domain Logon • 353
- Due Date Policy • 411

E

- Echo • 490, 517
- EchoMt • 490, 518
- Edit Event Sets • 280
- Edit Fields • 412
- Edit Profile • 65
- Email Mapping • 416
- Email Reader • 414
- Enable Matching • 239
- EnableAdmin • 491
- Enabling KSD API Web Service • 523
- Enabling the Agent Procedure API Web Service • 517
- Enabling the Monitoring API Web Service • 518
- Enabling Ticketing for Portal Access Users on Unsupported Browsers • 68
- Enabling VSA API Web Service • 471
- Event Log Alerts • 276
- Event Log Settings • 34
- Event Logs • 554
- Events Sets • 554
- Excel Usage • 419
- Executive - Executive Summary • 184

F

- Feature Set • 554
- File Access • 74
- File Transfer Protocol (FTP) • 555
- Filter Aggregate Table • 27
- Flood Detection • 555

fnMissingPatchCounts_UsePolicy /
 fnMissingPatchCounts_NoPolicy • 425
 fnOSCounts • 426
 Folder Rights • 108
 Folder Tree • 152, 168
 Format Email Alerts for Event Sets • 282
 FTP • 336

G

Get File • 116
 GetAlarm • 491
 GetAlarmList • 492
 GetEventAlertList • 521
 GetEventLogMachineSettingsList • 522
 GetEventSetDefinitionList • 523
 GetEventSetList • 523
 GetGroupLicenseInfo • 493
 GetIncident • 531
 GetIncident Request • 542
 GetIncident Response • 542
 GetIncidentList • 531
 GetIncidentList Request • 542
 GetIncidentList Response • 542
 GetIncidentList2 • 532
 GetLogEntry • 493
 GetMachine • 493
 GetMachineCollectionList • 496
 GetMachineGroupList • 496
 GetMachineList • 497
 GetMachineUptime • 497
 GetNotesList • 498
 GetOrgLocation • 498
 GetOrgs • 499
 GetOrgsByScopeID • 499
 GetOrgTypes • 498
 GetPackageURLs • 500
 GetPartnerUserLocation • 500
 GetPublishedViewColumns • 500
 GetPublishedViewRows • 501
 GetPublishedViews • 503
 GetRoles • 506
 GetScopes • 506
 GetScriptAssignmentID • 518
 GetScriptIDFromScriptName • 518
 GetServiceDesk • 533
 GetServiceDesk Request • 535
 GetServiceDesk Response • 535
 GetServiceDesks • 533
 GetServiceDesks Request • 535
 GetServiceDesks Response • 535
 GetSessionDetails • 506
 GetTicket • 507
 GetTicketList • 508
 GetTicketNotes • 508
 GetTicRequestTicket • 508
 Getting Started • 7
 GetVerboseMachineGroupList • 509
 Global Event Log Black Lists • 555
 Group Alarm Status • 223
 Group Alarms • 555

H

Host name • 555

I

If Your Account Is Disabled • 363
 IF-ELSE-STEP Commands • 84
 Import / Export • 57
 Import Center • 388
 Inbox • 140
 Incident • 528
 Incident Summary • 528
 Indexing the Audit Results Table • 384
 Info Center • 139
 Install Issues and Failures • 44
 Installed Applications • 136
 Installing Linux Agents • 46
 Installing Multiple Agents • 44
 ISO Image • 555

K

Kaseya Remote Control • 342
 KDS - Domain Activity • 189
 KES Status • 226
 KES Threats • 226
 KSD API Web Service • 523
 KSD API Web Service - Operations • 530
 KSD API Web Service Data Types • 524
 K-VNC Toolbar Options • 328

L

LAN Cache • 69
 LAN Watch • 555
 Layout Dashboard • 211
 Learning More • 18
 Legacy Report Definitions • 176
 License Manager • 386
 Limiting Requests by IP Address and User • 481
 Live Connect • 15, 344
 Live Counter • 230
 Local Settings • 397
 LockFunctionAccess • 509
 Log File Parser Definition • 314
 Log File Set Definition • 322
 Log History • 32
 Log Monitoring • 556
 Log Parser • 312
 Logoff • 14
 Logon and Browser Settings • 3
 Logon Hours • 372
 Logon Page • 394
 Logon Policy • 391
 Logs • 556
 Logs - Admin Notes • 190
 Logs - Agent Log • 190
 Logs - Agent Procedure • 190
 Logs - Alarm Log • 191
 Logs - Configuration Changes • 191
 Logs - Event Logs • 191
 Logs - Event Logs Frequency • 192
 Logs - Log Monitoring • 192

Index

Logs - Network Statistics Log • 192
Logs - Remote Control • 193

M

MAC address • 556
Machine ID / Group ID / Organization ID • 556
Machine ID / Group ID filter • 556
Machine ID / Machine Group Filter • 23
Machine ID Template • 557
Machine IDs vs. Agents • 557
Machine Policy • 334
Machine Roles • 367, 557
Machine Status • 225
Machine Summary • 131
Machines Online • 226
Macintosh • 35, 64, 396, 548
Maintaining Agent Install Packages • 39
Manage • 372
Manage - Custom Fields tab • 376
Manage - Departments tab • 374
Manage - General tab • 373
Manage - Machine Groups tab • 374
Manage - Staff tab • 375
Manage - Systems Management tab • 376
Manage Credentials • 126
Manage Files Stored on Server • 108
Managed Machine • 557
Management Dashboard • 209
Managing Scheduled Reports • 146
Manually Installing the Agent • 37
Master User / Standard User • 558
Master User vs. Standard Users • 361
MergeAgent • 509
Migrate • 2, 57, 61, 377, 558
Migrate Tickets • 408
Migrating the Kaseya Server • 558
Minimum System Requirements • 2
Mobile Devices - Device Applications • 193
Mobile Devices - Device Status • 193
Mobile Devices - Device Summary • 194
Mobile Devices - Lost Devices • 194
Monitor • 213
Monitor Icons • 241
Monitor Lists • 231
Monitor Log • 291
Monitor Overview • 214
Monitor Sets • 234, 558
Monitor Status • 226
Monitor Terms and Concepts • 216
Monitor Types • 558
Monitoring - Logs • 194
Monitoring - Monitor 95th Percentile • 195
Monitoring - Monitor Action Log • 195
Monitoring - Monitor Alarm Summary • 196
Monitoring - Monitor Configuration • 196
Monitoring - Monitor Log • 197
Monitoring - Monitor Set • 197
Monitoring - Monitor Trending • 197
Monitoring - Uptime History • 197
Monitoring API Web Service • 518
Monitoring API Web Service - Operations • 519
Monitoring Set Status • 224

MoveMachineToAnotherGroup • 509
myOrg • 558

N

Name Value Instances • 174
Name Value Part • 163
Name Value Parts • 167
Naming Policy • 358
Network Access • 75
Network Health Score • 186
Network Status • 223
Note • 524
Notification Bar • 10
Notify Policy • 408

O

On Premises • 559
Org • 559
Org Custom Field Title • 396
Orgs/Groups/Depts/Staff • 372
Outbound Email • 392

P

Packager • 116, 559
Page Layout • 8
Parser Definitions and Parser Sets • 559
Parser Summary • 309
Partition • 564
Patch - Patch Management • 198
Patch Deploy • 112
Patch Policy • 559
Patch Update Order • 560
Pending Approvals • 111
Performance Objects, Instances and Counters • 560
Pie Chart • 161
Policy Management - Agents Policy Status • 199
Policy Management - Policy Info & Association • 199
Portal Access • 67, 561
Preferences • 353
Preinstall RC • 331
Primary Domain Controller • 561
Primitives • 510, 533
Private Folders • 561
Process Status • 240
Publishing a Report Immediately • 145

Q

QueueAddIncident • 534
Quick Status • 561
Quick View • 16, 561

R

Record Desktop • 561
Refltem • 524
RelatedIncident • 525
Remote Control • 325
Remote Control Overview • 326
RemoveUserFromRole • 511
RemoveUserFromScope • 511
Rename • 53

- RenameMachine • 511
- Report and Report Set User Security • 148
- Report Contexts • 173
- Report Definitions • 143
- Report Folder Trees • 144
- Report Parts • 166
- Report Set Definitions • 149
- Report Set Folder Trees • 149
- Report Sets • 148
- Report Templates • 150
- Reports • 142
- Request Support • 377
- Reset Password • 330
- ResetPassword • 512
- RoleMembership • 512
- Run Audit • 128

S

- SaaS • 564
- Sample API ASP Page • 474
- Sample API C# Application • 472
- Sample Messages • 534
- Schedule • 141
- Schedule / Create • 80
- Scheduling / Rescheduling a Report • 145
- Scheduling Agent Procedures • 82
- Scheduling and Daylight Savings Time • 355
- Scopes • 369
- Script, Cancel • 131
- Security - Configuration • 199
- Security - Historical Threats • 200
- Security - KES Log • 200
- Security - Security • 199
- Send Message • 341
- SendAdminMessage • 512
- Server Management • 377
- Service Billing - Past Billed Invoices • 200
- Service Billing - Sales Order Summary • 200
- Service Billing - Unbilled Revenue by Customer • 201
- Service Billing - Unbilled Revenue by Item Type • 201
- Service Billing - Work Order Summary • 201
- Service Desk - Custom Tickets • 201
- Service Desk - Service Goals • 202
- Service Desk - Service Hours • 203
- Service Desk - Service Times • 203
- Service Desk - Service Volumes • 203
- Service Desk - Tickets • 204
- ServiceDeskDefinition • 525
- Services Check • 239
- Set Alert Actions tab • 279
- Set Credential • 68
- Set SNMP Type • 308
- Set SNMP Values • 306
- SetAdminPassword • 512
- SetGroupLicenseInfo • 513
- SetLicenseByOrg • 513
- SetPartnerUserLocation • 513
- Setting the Report Header Logo • 148
- Set-up Types • 376
- Sharing User-Owned Objects • 370
- Silent Install • 562
- Site Customization • 394

- Site Header • 394
- SNMP Community • 562
- SNMP Devices • 562
- SNMP Icons • 247
- SNMP Log • 305
- SNMP Quick Sets • 302, 562
- SNMP Set Details • 244
- SNMP Sets • 241, 563
- SNMP Traps Alert • 283
- SNMP Types • 563
- Software - Software Applications Changed • 204
- Software - Software Applications Installed • 205
- Software - Software Licenses • 205
- Software - Software Licenses Summary • 205
- Software - Software Operating Systems • 206
- Software as a Service (SaaS) • 564
- Software Deployment - Machine Changes • 207
- Software Deployment - Profile Status by Machine • 206
- Software Deployment - Recent Deployments • 206
- Software Deployment - Software Installed by Machine • 207
- Software Licenses • 137
- Special Fields • 471
- SSH • 338
- Statistics • 389
- Status Monitor • 12
- Supported Apple Functions • 48
- Supported Linux Functions • 47
- Suspend • 58
- Suspend Alarm • 229
- syslog • 564
- System • 351
- System Activity • 185
- System Agent Procedures • 564
- System Check • 293
- System Checks • 564
- System Info • 134
- System Log • 389
- System Overview • 352
- System Preferences • 356
- System Security • 2
- System Tray • 564

T

- Table • 155
- Task Manager • 338
- Tenant Partition • 564
- Ticketing • 399
- Ticketing - Customizable Ticketing • 207
- Ticketing - Ticketing • 208
- Ticketing Overview • 400
- Time Tracking - Timesheet Entries • 209
- Time Tracking - Timesheet Summary • 209
- Toolbox • 11
- Top N - Monitor Alarm Chart • 226

U

- Uninstall RC • 332
- Update Agent • 72
- Update Incident Request • 545
- Update Lists By Scan • 232

Index

UpdateIncident • 534
UpdateIncident Response • 546
UpdateOrg • 513
UpdateTicket • 513
UpdateUser • 515
Updating or Moving the VSA • 2
User Account • 564
User History • 372
User Role Policy • 333
User Roles • 365
User Security • 359
User Settings • 353
Users • 360, 565
Using Variables • 104

V

vAddRemoveList • 427
vAdminNotesLog • 427
vAgentConfiguration • 427
vAgentLabel • 428
vAlertLog • 429
Variable Manager • 107
vBackupLog • 430
vBaseApplicationInfo / vCurrApplicationInfo • 431
vBaseCpuInfo / vCurrCpuInfo • 432
vBaseDiskInfo / vCurrDiskInfo • 432
vBaseDriveManufacturer / vCurrDriveManufacturer • 433
vBasePciInfo / vCurrPciInfo • 433
vBasePrinterInfo / vCurrPrinterInfo • 434
vCollectionMember • 434
vConfigLog • 435
vEventDetail • 435
vEventInstanceDetail • 436
vEventInstanceHistoryDetail • 438
View Assets • 123
View Dashboard • 210
View Definitions • 24, 565
View Summary • 400
Viewing Log Monitoring Entries • 322
Views and Functions Provided • 423
Virtual Machine • 565
Virtual Network Computing (VNC) • 565
vLicenseInfo • 439
vMachine • 440
vMonitorAlarmAlert • 442
vMonitorAlarmCounter • 443
vMonitorAlarmProcess • 444
vMonitorAlarmService • 445
vMonitorAlarmSNMP • 446
vMonitorAlarmSystemCheck • 447
vNetStatsLog • 448
vNtEventLog • 448
vOnBoardDeviceInfo • 449
vPatchApprovalPolicyStatus • 449
vPatchApprovalStatus • 450
vPatchConfiguration • 451
vPatchPieChartCountsNoPolicy • 453
vPatchPieChartCountsUsePolicy • 454
vPatchPolicy • 454
vPatchPolicyMember • 456
vPatchStatus • 456

vPatchStatusByAgent • 458
vPortInfo • 461
vPro • 565
vPro tab • 125
VSA API Web Service • 470
VSA API Web Service - Operations • 482
VSA API Web Service - Overview • 470
VSA API Web Service Security • 477
VSA Logon Policies • 353
VSA Modules • 8
vScriptLog • 461
vScriptStatus • 462
vSystemInfo • 462
vSystemInfoManual • 463
vTicketField • 464
vTicketNote • 464
vTicketSummary • 465
vUptimeHistory • 465
vvProAssetDetails • 466

W

Web Links - Inbound and Outbound • 479
Well Known Parameters • 170
Windows Automatic Update • 565
Work Types • 565
Working Directory • 64