



Kaseya

Our Automation. Your Liberation.™

Virtual System Administrator

User Guide

v5.1.0.0

October 28, 2009

About Kaseya

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

Contents

Configuration	9
<hr/>	
Configuring the Server	10
Agents	10
Agent Icons	11
System Security	12
Minimum System Requirements	13
Updating the VSA	13
Getting Started	15
<hr/>	
Logon and Browser Settings	16
VSA Tabs	17
Machine ID / Group ID Filter	17
View Definitions	18
Filter Aggregate Table	20
Machine Summary	21
Toolbox	23
Status Monitor	24
Administrator Notes	24
Logoff	25
Home	27
<hr/>	
Home Tab	28
View Dashboard	28
Layout Dashboard	29
Audit	31
<hr/>	
Audit Tab	32
Run Audit	33
System Info	35
Installed Apps	36
Add/Remove	37
SW Licenses	37
Name/OS Info	38
IP Info	38
DNS/DHCP	39
Disk Volumes	40
PCI & Disk H/W	41
CPU/RAM	42
Printers	43
Documents	44
Machine Summary	44
File Access	47
Network Access	48
Application Blocker	50

Scripts	53
<hr/>	
Scripts Tab	54
Patch Deploy.....	55
Application Deploy	56
Creating Silent Installs	57
Packager	58
Get File	59
Distribute File	60
Scripts Status.....	61
Distribution	62
Script Browser and Script Toolbar	63
Script Manager.....	64
Script Scheduler.....	65
Script Editor	67
Manage Files Stored on Server	69
Variable Manager.....	70
IF-THEN-ELSE Commands.....	72

Monitor	83
<hr/>	

Monitor Tab.....	84
Alarms.....	86
Dashboard List.....	88
Alarm Summary	90
Alarm Network Status.....	90
Alarm Summary Window.....	90
Alarm Rotator.....	92
Alarm Ticker.....	92
Network Status	92
Group Alarm Status	93
Monitoring Set Status	93
Machine Status.....	95
Device Status	95
Monitor Status.....	95
Machines Online.....	95
Top N - Monitor Alarm Chart	95
KES Status	95
KES Threats	96
Settings	96
Alarm Summary	96
Suspend Alarms.....	98
Live Connect.....	99
Alerts.....	100
Alerts - Summary.....	101
Alerts - Agent Status.....	103
Alerts - Application Changes	106
Alerts - Get Files	108
Alerts - Hardware Changes	110
Alerts - Low Disk.....	113
Alerts - Event Logs	115
Edit Event Sets.....	120
Alerts - LAN Watch	121
Alerts - Script Failure	124
Alerts - Protection Violation	126
Alerts - New Agent Installed	128

Alerts - Patch Alert.....	130
Alerts - Backup Alert.....	133
Alerts - System	136
Monitor Lists.....	138
Update Lists By Scan	140
Monitor Sets.....	140
Define Monitor Sets	142
Counter Thresholds	143
Services Check.....	145
Process Status	146
Monitor Icons	147
Assign Monitoring	147
Auto Learn - Monitor Sets.....	152
Monitor Log.....	153
System Check.....	154
SNMP Sets	158
Define SNMP Set	159
Define SNMP Set Details	161
Add SNMP Object	163
SNMP Icons.....	164
LAN Watch.....	165
Assign SNMP.....	168
SNMP Quick Sets.....	172
Auto Learn - SNMP Sets	174
SNMP Log.....	175
Set SNMP Values	177
SNMP Type.....	178
Parser Summary	179
Log Parser	182
Log File Parser Definition	184
Assign Parser Sets	187
Log File Set Definition	191

Ticketing **193**

Ticketing Tab	194
View Summary.....	194
Create/View	197
Delete/Archive.....	200
Notify Policy	202
Access Policy.....	204
Assignee Policy.....	205
Due Date Policy	205
Edit Fields	207
Email Reader	208
Email Mapping.....	210
Edit Profile / User Profiles.....	210
User Access.....	212

Patch Management **215**

Patch Mgmt Tab.....	216
Methods of Updating Patches	217
Configuring Patch Management.....	217
Patch Processing.....	218

Superseded Patches	218
Update Classification	219
Patch Failure.....	219
Scan Machine	221
Patch Status.....	222
Initial Update	224
Pre/Post Script: Patch Management.....	226
Automatic Update	227
Machine History	228
Machine Update.....	229
Patch Update	231
Rollback	234
Cancel Updates	234
Create/Delete: Patch Policy	235
Membership: Patch Policy	236
Approval by Policy	238
Approval by Patch.....	240
KB Override	242
Windows Auto Update	243
Reboot Action	245
File Source.....	248
Patch Alert	250
Office Source	254
Command Line.....	256
Patch Location	258

Remote Control **261**

Remote Cntl Tab.....	262
Control Machine.....	263
Video Streaming	265
Reset Password.....	267
Power Mgmt.....	268
Select Type	269
Set Parameters	271
Preinstall RC	272
Uninstall RC.....	273
Admin Role Policy.....	274
Machine Policy.....	276
FTP	277
Chat	279
Send Message.....	281
Task Manager	283

Reports **285**

Reports Tab	286
Set Logo.....	287
Schedule Reports	287
Executive Summary.....	289
Network Health Score.....	291
System Activity	293
Aggregate Table	294
Advanced Filtering	295
Machine Summary.....	296

Machine Changes	298
Patch Management.....	299
Inventory	301
Software.....	303
Disk Utilization	305
Network Statistics	306
Uptime History	308
Logs	309
Ticketing.....	311
Backup	312
Monitor	314
Security	316
User State	318
Power Savings.....	319

Agent 323

Agent Tab	324
Agent Status	325
Agent Logs.....	327
Log History.....	328
Event Log Settings.....	329
Deploy Agents.....	331
Agent Install Command Line Switches.....	335
Deploying Macintosh Agents using Apple Remote Desktop	337
Install Issues and Failures	340
Create	341
Delete.....	344
Rename	346
Change Group	347
LAN Watch.....	348
Install Agents	351
View LAN	354
View AD Computers.....	354
View AD Users.....	355
View vPro.....	358
Copy Settings.....	358
Import / Export	360
Suspend.....	360
Agent Menu.....	361
Check-In Control	363
Temp Directory	366
Edit Profile / User Profiles	367
User Access.....	369
Set Credential	371
Update Agent.....	372

System 375

System Tab.....	376
Preferences.....	377
Create / Delete: Machine Groups	379
Rename Group	380
Naming Policy	380
Check-in Policy	382

Create / Delete: Admin Roles	383
Membership: Admin Roles.....	384
Group Access	385
Function Access.....	387
Logon Hours	388
Create / Delete: Admin Accounts.....	388
Enable / Disable.....	390
Set Password.....	391
Reset Master Admin Password	393
Admin History.....	393
Request Support	394
Configure	394
License Manager	399
System Log.....	400
Statistics.....	401
Logon Policy	403
Customize	403
Creating Custom Agent Icons.....	407

Database Views **409**

Database Views	410
Excel Usage	411
Crystal Reporting Usage.....	411
Views Provided	415
fnMissingPatchCounts_UsePolicy / fnMissingPatchCounts_NoPolicy.....	416
fnOSCounts	417
vAdminNotesLog.....	417
vAgentConfiguration	418
vAgentLabel	419
vAlertLog	419
vBackupLog	420
vBaseApplicationInfo / vCurrApplicationInfo.....	421
vBaseCpuInfo / vCurrCpuInfo.....	421
vBaseDiskInfo / vCurrDiskInfo	422
vBaseDriveManufacturer / vCurrDriveManufacturer.....	422
vBasePciInfo / vCurrPciInfo	423
vBasePrinterInfo / vCurrPrinterInfo.....	423
vCollectionMember	424
vConfigLog.....	424
vLicenseInfo.....	425
vMachine.....	425
vMonitorAlarmAlert	427
vMonitorAlarmCounter	428
vMonitorAlarmProcess.....	428
vMonitorAlarmService.....	429
vMonitorAlarmSNMP	430
vMonitorAlarmSystemCheck	430
vNetStatsLog	431
vNtEventLog	431
vOnBoardDeviceInfo.....	432
vPatchApprovalStatus	432
vPatchPolicy	433
vPatchPolicyMember	434
vPatchStatus.....	434
vPortInfo.....	436

vScriptLog	436
vScriptStatus	436
vSystemInfo	437
vTicketField	438
vTicketNote	438
vTicketSummary	438

VSA API Web Service 441

Overview	443
Enabling VSA API Web Service	444
Special Fields	444
VSA API Web Service Sample Client - C# GUI application	445
VSA API Web Service Sample Client - ASP Page	446
VSA API Web Service Security	449
Web Links - Inbound and Outbound	451
Operations	453
Admin Group Access	453
Authenticate	453
CloseAlarm	453
CreateAdmin	454
CreateAgentInstallPackage	454
CreateMachineGroup	454
CreateRole	454
DeleteAdmin	455
DeleteAgent	455
DeleteMachineGroup	455
DeleteRole	455
DisableAdmin	455
Echo	456
EnableAdmin	456
GetAlarm	456
GetAlarmList	457
GetGroupLicenseInfo	458
GetLogEntry	458
GetMachine	459
GetMachineCollectionList	462
GetMachineGroupList	462
GetNotesList	462
GetMachineList	462
GetPackageURLs	463
GetTicket	463
GetTicketList	464
GetTicketNotes	464
LockFunctionAccess	465
Primitives	465
RoleMembership	465
SendAdminMessage	466
SetAdminPassword	466
SetGroupLicenseInfo	466
UpdateTicket	466

Glossary of Terms 469

Index 487

Chapter 1

Configuration

In This Chapter

Configuring the Server	10
Agents	10
Agent Icons	11
System Security	12
Minimum System Requirements	13
Updating the VSA	13

Configuring the Server

The server is the heart of the system. Administrators 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 administrators and agents.

Administrators and agents need to be able to connect back to the server from anywhere on the internet. Verify your server meets the following requirements:

1. **Public server name/IP address** - Define a public IP address for your server. If your server is behind a gateway on a private network, your VSA may be using the private IP address. Long term it is better to use a name instead of an IP address. Using a name lets you change the IP address without having to re-configure any agents. Set the name/IP address of the VSA using [System > Configure](#) (page 394).
2. **Open required ports at the firewall** - Administrators access the VSA through the web interface (typically port 80). Agents connect to the server on a separate port (default port 5721). Both these port must be opened at your firewall for TCP/IP traffic. The agent port (5721) must be open for both inbound and outbound.
3. **Verify localhost access for the web server** - Several VSA services depend on localhost access. Typically localhost access can be enabled by:
 - a. Opening the [IIS Enterprise Manager](#).
 - b. Right clicking the [Default Web Site](#) and selecting [Properties](#).
 - c. Clicking the [Web Site](#) tab.
 - d. Verifying the [IP Address](#) field is set to (All Unassigned).
4. **Specify the alert email sender address** - The VSA sends alerts via email. Emails are sent from your server using the built-in SMTP service. You can set the address these emails come from to any valid email address using [System > Configure](#). The default email address is vsa@kaseya.com.

Note: For the latest instructions on migrating an existing KServer to a new machine see the article [How do I move my Kaseya Server to a new computer? \(270436\)](#) in the Kaseya Support Knowledge Base Portal.

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 in for it to function and it does not require a reboot for it 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 IT administrator. Once installed:

- A K icon  displays in the icon tray of the remote machine. This can be a custom image or removed altogether.
- Each installed agent is assigned a unique VSA [machine ID / group ID](#) (page 476). 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 licenses purchased by the service provider.

Agents are typically installed using packages created using [Agent > Deploy Agents](#) (page 331) inside the VSA.

Agent Icons

Once installed on a machine, the agent displays an icon in the computer's system tray. This icon is the user's interface to the agent. The icon may be disabled at the discretion of the administrator using the Agent > [Agent Menu](#) (page 361) page.

Note: You can fully customize agents icon using System > Customize. See [Creating Custom Agent Icons](#) (page 407). This includes unique icons for Macintosh 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 [User Access Welcome Page](#) (page 484).

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 363) settings are correct.
4. Manually set the VSA address in the agent by right clicking the agent menu, selecting [Set Account...](#), and filling in the form with the correct address.

Set Agent Account Information

Please enter the Machine.Group ID for this Agent and the address of your management server. The Agent automatically connects to the server's IP Address or hostname to manage your system.

Machine.Group

Server Address

OK Cancel

Agent Icon Background is Red

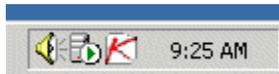
The agent icon turns [red](#) when a user manually disables remote control. Users prevent anyone from remote controlling their machine by selecting [Disable Remote Control](#) when they right click the agent menu.



Configuration

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 Cntl > Send Message \(page 281\)](#) 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 user.



Note: See [Agent > Agent Menu \(page 361\)](#) for a description of how to turn these options on or off.

Disabling the Agent Menu

Administrators may completely **disable the agent menu** ([page 361](#)) and remove the icon from the machine's desktop.



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 256-bit RC4 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.

Administrators 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 administrator 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-1. 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.

The web site itself is protected by running the Hotfix Checker tool on the VSA server every day. The VSA sends alerts to the master administrator when new IIS patches are available. This helps you keep the VSA web server up to the latest patch level with a minimum of effort. Finally, for maximum web security, the VSA web pages fully support operating as an SSL web site.

Minimum System Requirements

Up to date minimum system requirements are always available on our web site at

<http://www.kaseya.com/support/system-requirements.aspx>

Updating the VSA

The most recent update information is always available at

<http://vsaupdate.kaseya.net/vsaupdate/Detailed-Update-Instr.pdf>

Chapter 2

Getting Started

In This Chapter

Logon and Browser Settings	16
VSA Tabs	17
Machine ID / Group ID Filter	17
Machine Summary	21
Toolbox	23
Status Monitor	24
Administrator Notes	24
Logoff	25

Logon and Browser Settings

To logon to Kaseya® Virtual System Administrator™

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

Note: For initial logon, use the master administrator 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: See [System > Preferences \(page 377\)](#) for a description of how to set up a domain logon.

4. Click the logon icon .

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

Enabling Browser Cookies and JavaScript

Internet Explorer 5.0 or greater must have cookies and JavaScript enabled in order to proceed.

To Enable Cookies in Internet Explorer 5

Cookies are enabled by default in Internet Explorer. However, if cookies are turned off, you may need to enable them.

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 [Cookies](#) section.
7. In [Allow cookies that are stored on your computer](#), select the [Enable](#) radio button.
8. In [Allow per-session cookies](#), select the [Enable](#) radio button.
9. Press [OK](#).

To Enable Cookies in Internet Explorer 6

1. Click on the [Tools](#) menu.
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. Press [OK](#).

To Enable JavaScript in Internet Explorer

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](#), enable the [Custom](#), [High safety](#), [Low safety](#), or [Medium safety](#) radio button, depending on the security requirements of the machine running the script.
8. Press [OK](#).

VSA Tabs

[Home](#) | [Audit](#) | [Scripts](#) | [Monitor](#) | [Ticketing](#) | [Patch Mgmt](#) | [Remote Cntl](#) | [Backup](#) | [Security](#) | [User State](#) | [Reports](#) | [Agent](#) | [System](#)

All VSA functions can be accessed through tabs located at the top of the console window. Within each tab are the core functions that allow administrators to perform a variety of tasks on remote managed machines and the server.

Machine ID / Group ID Filter

Machine ID / Group ID Filter

Each [agent](#) ([page 470](#)) installed on a managed machine is assigned a unique machine ID/group ID name. All machine IDs are associated with a group ID and optionally a subgroup ID. Typically a group ID represents a single customer account. Subgroup IDs typically represent a location or network within a group ID. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.acme.chicago`. In this case `chicago` is a subgroup ID defined within the group ID called `acme`. Only a master administrator, or administrators authorized by a [master administrator](#) ([page 469](#)), can create group IDs. Any administrator can create subgroup IDs. Group IDs and subgroup IDs are created using the [System > Machine Groups > Create/Delete](#) ([page 379](#)) page.

Filtering Views



The Machine ID / Group ID filter is available on all tabs and functions. It allows you to limit the machines displayed on *all* function pages. The [View Definitions](#) window lets you further refine a Machine ID / Group ID filter based on attributes contained on each machine—for example, the

operating system type. Once filter parameters are specified, click the green arrow icon  to apply filter settings to *all* function pages. By default, the Machine ID / Group ID filter displays all machine IDs in `<All Groups>` managed by the currently logged in administrator.

Note: Even if an administrator selects `<All Groups>`, only groups the administrator is granted access to using [System > Group Access](#) ([page 385](#)) 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`.

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.

Getting Started

Rows

Select the number of machines IDs displayed on each page.

Select Machine Group

Limits the display of data on all function pages by group ID.

Select View

Change views by selecting a different view definition. The [View Definitions](#) window lets you further refine a Machine ID / Group ID filter based on attributes contained on each machine—for example, the operating system type.

Edit...

Click the [Edit...](#) button to display the [View Definitions](#) (*page 18*) 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 / Group ID 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 [Select View](#) drop down list on the [Machine ID / Group ID Filter](#) (*page 17*) panel and clicking the green arrow  icon.

Share...

You can share a view with selected administrators and administrator roles or make the view public for all administrators and administrator roles.

To Create or Edit a New View

1. Click the [Edit...](#) button to the right of the [Select View](#) drop down list to open the View Definitions editor.
2. Enter a name for the view in the [Edit Title](#) area.
3. Enter the desired filter specifications.
4. Click the [Save](#) or [Save As](#) button.

View by Machine ID

- [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 of machine IDs.

View by Network Status and Address

- [Show machines that have / have not / never been online in the last N Days](#) - Check this box to only list machines whose agents have checked into server, or not, within the specified period of time. Use the [never](#) option to filter [machine ID template](#) (page 477) accounts, because these accounts never check in.
- [Connection gateway filter](#) - Check to only list machines that have a [connection gateway](#) (page 38) 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`.

View by Operating System

- [OS Type](#) - Check to only list machines that match the selected operating system as reported using the Audit > [Name/OS Info](#) (page 38).
- [OS Version](#) - Check to only list machines that match the OS version string as reported using Audit > [Name/OS Info](#) (page 38). Use this filter to identify machines by [service pack](#).

View Machines Based on Script History/Status

- [With script scheduled/not scheduled](#) - Check to only list machines that have the specified script either scheduled to run or not.

Note: Click the select script link to specify the script by name.

- [Last execution status success/failed](#) - Check to only list machines that have already executed the selected script. Select the appropriate radio button to list machines that successfully executed the script or failed to execute the script.
- [Script has/has not executed in the last N days](#) - Check to only list machines that have or have not executed the script in the specified period of time.

View Machines by Application

- [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.

View Machines by Patch Update

- [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 478).
- [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.

Getting Started

- [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](#) (page 227) configuration.
- [Machines with Patch Reboot Action configuration](#) - Check to only list machines with the selected [Reboot Action](#) (page 245) configuration.
- [Machines with Patch File Source configuration](#) - Check to only list machines with the selected patch [File Source](#) (page 248) configuration.
- [Machines missing a specific patch \(identified by the patch's 6 digit KB Article ID\)](#) - Check to only list machines missing a specific patch.

View Machines by Agent Data

- [Advanced Agent Data Filter](#) - Check and click the [Define Filter...](#) button to further refine the view using the [Filter Aggregate Table](#) (page 20).

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](#) (page 18).

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 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. 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`

NOT

Search for a string not containing the match data.

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

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.

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

Returns all data whose value is numerically less than, if a number. If this is alphabetic data then it returns all strings appearing earlier in the alphabet.

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

For example: `< 3` returns all values numerically less than "3".

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)

Returns all data whose value is numerically greater than, if a number. If this is alphabetic data then it returns all strings appearing after it in the alphabet.

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

For example: `> 3` returns all values numerically greater than "3".

Machine Summary

Audit > Machine Summary

- Similar information is provided using [Reports > Machine Summary \(page 296\)](#).

The [Machine Summary](#) page for any machine ID can be displayed immediately by clicking the check-in status icon next to any machine ID.

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  Agent has been disabled
-  Agent has been suspended

Alternatively, you can navigate to the [Audit > Machine Summary](#) page, which lists all machine IDs currently matching the [Machine ID / Group ID filter \(page 17\)](#), and click any machine ID to display the [Machine Summary](#) page.

Displaying the Machine Summary Page Using a URL

The following URL displays the [Machine Summary \(page 21\)](#) web page for a specific machine ID:

Getting Started

`http://...?machName=<MachineID>`

For example:

<http://demo.kaseya.com?machName=jconners.acme>

Machine Summary

The **Machine Summary** page allows administrators to perform tasks and functions solely for one managed machine. A tabbed property sheet provides access to various categories of information about the managed machine. The administrator can customize the layout of the **Installed Applications** and **System Info** tabs.

Note: Administrator access to the tabs of the Machine Summary page is determined using System > Function Access (page 387).

The following elements are displayed in the **Machine Summary**:

- **Machine Info** - Current User, Domain/Workgroup, IP Address, Computer Name, Subnet Mask, OS, Version and Build, Default Gateway, Connection Gateway, RAM, MAC Address, CPU, DHCP Server, DNS Server, and Primary and Secondary WINS Servers, Last Checkin, Last Reboot, First Time Checkin.
- **Installed Applications** - Lists all the applications installed on the managed machine. Provides the same functionality as Audit > **Installed Apps** (page 36). Clicking the **Filter...** button enables you to filter the applications displayed by application attribute.
- **System Info** - Lists system hardware attributes and related information.
 - Click the **Show More** button to add or subtract system information attributes from the default list provided.
 - Click the automatic assignment icon  next to an system information attribute to manually edit the value. Click the manual edit icon  to display the **Edit Manual Input Value Only** dialog box. Use this dialog box to manually change the value of the attribute for this machine or for all machines using the current machine ID / group ID filter.
 - Click the **System Serial Number** link to display a machine manufacturer's support site, for the following manufacturers: Dell, IBM, Lenovo, HP, Compaq, Gateway, and Sony.
- **Disk Volumes** - Drive letter, Type, Format, Free Space, Used Space, Total Size, and Label.
- **PCI & Disk Hardware** - Type, Vendor, and Product name. Provides the same functionality as Audit > **PCI & Disk H/W** (page 41).
- **Printers** - Lists the printers and ports a machine can direct print jobs to.
- **Documents** - Lists documents uploaded to the KServer for a machine. You can upload additional documents. Provides the same functionality as Audit > **Documents** (page 44).
- **Pending Scripts** - Displays and schedules pending scripts for a machine and the script history for that machine. Includes the execution date/time and administrator who scheduled the script.
 - To add a script to the pending script schedule, click the **Click to schedule new script** link to display the **Search for Script** window and select a script. The name of the selected script displays at the top of the **Pending Scripts** window. Enter scheduling parameters, then click the **Schedule** button.
 - You can cancel any scheduled script by clicking the checkbox next to the pending script and clicking the **Cancel** button.
- **Agent Logs** - Displays the event logs available for a machine: Agent Log, Configuration Log, Network Statistics, Event Log, Script Log, Remote Control Log, Log Monitoring.
- **Alerts** - Defines alerts for a machine: Agent Status, Application Status, Get File Changes, Hardware Changes, Low Disk Space, Event Log, LAN Watch, Script Execution Failure, Protection Violations, Patch Alert, Backup Alert.
- **Patch Status** - Displays **Missing** and **Pending** Microsoft patches and schedules missing patches. If a machine belongs to a **patch policy** (page 478), missing patches may be further

identified as `Denied (Pending Approval)`. The user can manually override the denied patch policy by scheduling the patch.

- To schedule a missing patch, check the box next to the patch, enter scheduling parameters and click the [Schedule](#) button.
- To cancel a pending patch, check the box next to the patch and click the [Cancel](#) button.
- To display the history of patches installed on a machine, click the [Show History](#) link.
- **Remote Control** - Displays and configures remote control settings for a machine.
- **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 Mgmt > [Membership: Patch Policy](#) (page 236)
 - **View Definition Collections** - Defined using the [Only show selected machine IDs](#) option in [View Definitions](#) (page 18).
 - **Temp Directory** - Can also be defined using Agent > [Temp Directory](#) (page 366).
 - **Check-In Control** - Can also be defined using Agent > [Check-In Control](#) (page 363).
 - **Edit Profile** - Can also be defined using Agent > [Edit Profile](#) (page 210) and Ticketing > [User Profiles](#) (page 210).
 - **Agent Logs and Profiles** - Can also be defined using Agent > [Log History](#) (page 328).
- **New Ticket** - Click this link to create a new ticket assigned to this machine ID using the [Ticket > View Ticket](#) (page 197) page.

Customizing the New Ticket Link

To customize the [New Ticket](#) link on the [Machine Summary](#) 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 KServer.

```
<?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>
```

Toolbox



The [Toolbox](#) provides the administrator with a common area to access frequently used commands and functions. The [Toolbox](#) is accessible from any tab, giving administrators convenient access to frequently used features of the VSA.

Getting Started

Notes

Click the [Notes](#) icon  to display the [Administrator Notes](#) (page 24) window. [Administrator Notes](#) provides a place to record and retrieve what previous administrator actions were performed on each machine.

Status

Click the [Status](#) icon to  display the [Status Monitor](#) (page 24) 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 administrators can also display the list of logged on administrators.

Turn off sound

A unique audible tone sounds each time a machine goes online, machine goes offline, an administrator logs in, or an administrator 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 [Kaseya® Virtual System Administrator™](#). To get an immediate update, click the [Refresh](#) link.

List logged on administrators

Uncheck this box to hide the list of administrators.

Note: This option is available to master administrators 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 administrators have done on that machine. The system time-stamps each administrator note and associates the note with an administrator name.

Open the notes editor by clicking the Notes icon  in the [Toolbox](#) (page 23).

Note: You can print Administrator Notes using [Reports > Logs](#) (page 309) and selecting Admin Notes in the Choose a log to display field.

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385). 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 administrator that entered the note. If a different administrator edits the note, this field is updated with the new administrator'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 administrator 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 administrator and has the same time-stamp, the system asks if you want to modify all occurrences of the note.

Note

Displays the administrator entered note for the selected machine.

Notes per Page

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

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 administrators log off and terminate all browser sessions when not administering the server.

Chapter 3

Home



In This Chapter

Home Tab	28
View Dashboard	28
Layout Dashboard	29

Home Tab

Home

The [Home](#) tab contains a summary display of the entire system called the [dashboard](#) and a summary display of the alarm status of all machines being monitored call the [console](#). The results displayed by the dashboard and console depend on the [Machine ID / Group ID filter](#) ([page 476](#)).

- The [Home](#) tab provides a quick start guide to the main features of the VSA.
- You can view VSA demos at <http://www.kaseya.com/get-started/demo.aspx>.
- You can view VSA training videos at <https://training.kaseya.com> <https://training.kaseya.com>.
- You can completely customize the menu options displayed on the [Home](#) tab using System > [Customize](#) ([page 403](#)).

Functions	Description
View Dashboard (page 28)	Displays system summary information at a glance.
Layout Dashboard (page 29)	Specify which items appear in the dashboard and the order the items appear.
Dashboard List (page 88)	Multiple monitoring views display a summary of monitoring status.
Settings (page 96)	Use this page to customize the Dashboard List page.

View Dashboard

Home > 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 476](#)). You can manage [tasks](#) and send [messages](#) to other administrators using the dashboard. Customize the dashboard display using Home > [Layout Dashboard](#) ([page 29](#)).

Alerts

Displays all alerts relating to all machine IDs matching the current [machine ID / group ID filter](#) ([page 17](#)). The display lists the most recent alerts first. By default, alerts generated within the **last 24 hours** are **highlighted in red**. Alerts generated within the **last week** are **highlighted in yellow**. The color coding lets you quickly distinguish alerts you may not have examined yet.

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 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 478](#)) 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 shows 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.

Tasks

Use this section to create, edit, and monitor tasks you or other administrators 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 377) page.

Messages

Use this section to send messages to other administrators. Messages you have received are listed in the lower part of this pane.

Note: Send messages to users using [Remote Cntl > Send Message](#) (page 281).

Layout Dashboard

[Home](#) > [Layout](#)

The [Layout Dashboard](#) page displays/hides each item and sets the order they appear, from top to bottom. Each [dashboard](#) (page 28) pane appears as a vertical section. To display an item, simply 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 alerts, 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 4

Audit

In This Chapter

Audit Tab	32
Run Audit	33
System Info	35
Installed Apps	36
Add/Remove	37
SW Licenses	37
Name/OS Info	38
IP Info	38
DNS/DHCP	39
Disk Volumes	40
PCI & Disk H/W	41
CPU/RAM	42
Printers	43
Documents	44
Machine Summary	44
File Access	47
Network Access	48
Application Blocker	50

Audit Tab

Audit

Agents (page 470) 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 KServer 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 **Reports** (page 286) are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two **alert** (page 100) 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** (page 41), 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.

Note: You can view Audit demos at <http://www.kaseya.com/get-started/demo.aspx>.

Functions	Description
Run Audit (page 33)	The Run Audit function used in conjunction with the Reports tab can be used to generate reports about usage trends and managed machine configurations, which can be helpful in isolating faults and other software or hardware-related problems.
System Info (page 35)	Shows DMI / SMBIOS data collected.
Installed Apps (page 36)	Shows a list of executable (.exe) files on selected managed machines.
Add/Remove (page 37)	Shows the Add or Remove Programs list from a managed machine.
SW Licenses (page 37)	Shows a list of vendor license codes found on selected managed machines.
Name/OS Info (page 38)	Shows the Windows Networking computer name, operating system, and operating system version in use on the managed machines.
IP Info (page 38)	Shows the Machine.Group ID, IP address, subnet mask, default gateway, and connection gateway in use on the managed machines.
DNS/DHCP (page 39)	Shows the Machine.Group ID, DNS Server, DHCP

	server, and primary and secondary WINS servers in use on the managed machine(s).
Disk Volumes (page 40)	Shows the Machine.Group ID, types of drives with corresponding drive letters, and free space, used space and total space on physical and logical drives in use on the managed machines.
PCI & Disk H/W (page 41)	Shows information about PCI, disk drives, and disk controller cards installed on managed machines.
CPU/RAM (page 42)	Shows the Machine.Group ID, CPU, quantity and speed of CPUs, and RAM as reported in use on the managed machines.
Printers (page 43)	Lists all printers available to a managed machine.
Documents (page 44)	Stores files associated with a managed machine.
Machine Summary (page 21)	Displays detailed information about a single managed machine.
File Access (page 47)	Prevents unauthorized access to files on managed machines by rogue applications or users.
Network Access (page 48)	Lets you approve or deny network access on a per application basis.
Application Blocker (page 50)	Application blocker prevents any application from running on a managed machine.

Run Audit

Audit > Run Audit

[Agents](#) (page 470) 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 KServer 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 [Reports](#) (page 286) are based on the latest audit. The [Machine Changes](#) report compares a machine ID's latest audit to a baseline audit. Two [alert](#) (page 100) types specifically address changes between a baseline audit and the latest audit: [Application Changes](#) and [Hardware Changes](#).

Latest Audit

Runs the [Latest Audit](#) of all selected machine IDs when [Schedule](#) is clicked. Captures the state of machines on a frequent basis, such as daily.

Baseline Audit

Runs a [Baseline Audit](#) of all selected machine IDs when [Schedule](#) is clicked. Run a baseline audit to capture the state of machines in a known working state.

Audit

System Info

Collects [System Info](#) of all selected machines IDs when [Schedule](#) is clicked. [System Info](#) (page 35) displays all DMI / SMBIOS data collected for each managed machine. This data virtually never changes and typically only needs to be run once.

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.

Run Now

Click [Run Now](#) to run this task on selected machine IDs immediately.

Cancel

Click [Cancel](#) to cancel execution of this task on selected managed machines.

Run recurring every <N> <periods>

Check the box to make this task a recurring task. Enter the number of times to run this task each time period.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task 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, ...

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.

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](#).

PCI & Disk Audit

Enables/disables the hardware audit driver for an agent. Only disable the driver if you suspect a driver conflict on the managed machine. The agent can not audit PCI hardware cards if this driver is disabled.

Check-in status

These icons indicate the agent check-in status of each managed machine:



Agent has checked in



Agent has checked in and user is logged on. Tool tip lists the logon name.



Agent has not recently checked in



Agent has never checked in



Online but waiting for first audit to complete



The agent is online but remote control is disabled



The agent has been suspended

Machine.Group ID/System Info

The top line shows the machine ID. The bottom line displays the last time a System Info audit was performed. If a System Info audit is pending, the time displays **as red text with yellow highlight**.

Latest Audit/Baseline Audit

The top line displays when the Latest Audit data was performed. The bottom line displays the last time a Baseline Audit was performed. If the baseline audit is pending, the time displays **as red text with yellow highlight**.

Next Audit/Recurring Interval

Displays the time of the next scheduled Latest Audit. The bottom line displays the recurring interval for latest audits. If the latest audit is pending, the time displays **as red text with yellow highlight**.

System Info

Audit > System Info

- Similar information is provided using Reports > Inventory (page 301).

The [System Info](#) page displays all DMI / SMBIOS data collected by the system info [audit](#) (page 472) for a selected machine ID. Data items displayed can include:

- System Information
 - 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 - maximum 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
- On Board Devices - table of motherboard based devices (like video or ethernet)
- Port Connectors - table of all the connections available on the chassis

Audit

- Memory Devices - table of memory modules installed on the motherboard
- System Slots - table indicating status of each available card slot

Show More...

Click the [Show More](#) button to display the [Select System Information to Display](#) popup window. This window enables you to add or subtract DMI / SMBIOS data items to display in the [System Info](#) page.

You can also manually add new data items by clicking [New...*](#) button. If you enter `http://` or `https://` at the start of a manually added data item using the [New...*](#) button, then a URL link is automatically created.

Automatic Collection

The automatic collection icon  indicates the data item is automatically collected and updated each time collection runs. [Click this icon to toggle to Manual Collection mode.](#)

Manual Collection

The manual collection icon  indicates the data item is manually input by the administrator. These items are *not* updated each time collection runs. [Click this icon to toggle to Automatic Collection mode.](#)

Edit Value

Edit any [System Info](#) data item by clicking the edit value icon . The edit value icon displays for data items set to [Manual Collection](#).

Installed Apps

Audit > Installed Apps

- Similar information is provided using [Reports > Software](#) ([page 303](#)).

The [Installed Apps](#) page lists all applications found during the [latest audit](#) ([page 472](#)) for a selected machine ID. The list of machine IDs you can select depends on the [Machine ID / Group ID filter](#) ([page 17](#)). The following information is displayed by default:

- [Application](#) - The filename of the application.
- [Version](#) - The version number of the application.
- [Product Name](#) - The product name of the application.
- [Description](#) - A brief description of the application as reported in the Properties dialog box of the executable file.
- [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.

You can adjust the display of data using the following controls:

Rows/page

Select the number of rows displayed per page. Selecting `All` may take a long time to display.

Show page starting with...

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

Filter...

Click the [Filter...](#) button to display the [Filter List of Displayed Applications](#) popup window. This window enables you to select and order the columns of information displayed. You can also narrow your search by entering filter criteria. Include an asterisk (*) wildcard with the text you enter to match multiple records. By default, the (*) wildcard is used, which lists all files. For example, enter the letter A* in the [Application](#) field, then click [Save](#) to display all application names beginning with the letter A. Use [Advanced Filtering](#) (page 295) options to specify additional criteria.

Full column width

Column data is limited to to the width allotted for each column. Hovering over shortened data displays the full data as a tool tip. To display data in full width columns check this box.

Add/Remove

Audit > Add/Remove

- Similar information is provided using [Reports > Software](#) (page 303).
- Alerts can be defined using [Monitor > Alerts > Application Changes](#) (page 106).

Click a machine ID on the [Add/Remove](#) page to show the [Add or Remove Programs](#) list from a managed machine. Information shown on this page is collected when a [Latest Audit](#) (page 33) is performed. The list of machine IDs you can select depends on the [Machine ID / Group ID filter](#) (page 17).

SW Licenses

Audit > SW Licenses

- Similar information is provided using [Reports > Software](#) (page 303).

The [SW Licences](#) 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 17) and machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Information shown on this page is collected when a [Latest Audit](#) (page 33) 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.

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.

Audit

Version

The version of the application.

Date

The version release date.

Name/OS Info

Audit > Name/OS Info

- Similar information is provided using [Reports > Software](#) (page 303).

Name/OS Info displays the Microsoft Windows Networking computer name, operating system, and version information for all machine IDs currently matching the Machine ID / Group ID filter. Information shown in this function is collected when a [Latest Audit](#) (page 33) is performed.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Computer Name

Lists the name of the computer as reported and used by Windows Networking.

Operating System

Lists the operating system name used by the managed machine.

Version

Lists the version number of the operating system in use by the managed machine.

IP Info

Audit > IP Info

IP Info displays IP address, subnet mask, default gateway (internal) and connection gateway (external) information for machine IDs matching the current [Machine ID / Group ID filter](#) (page 17). Information shown in this function is collected when a [Latest Audit](#) (page 33) is performed.

Note: The connection gateway is the public IP address the outside world sees when a machine connects from a private LAN behind a NAT gateway. Typically that IP address is the address on the WAN side of the NAT gateway.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

IP Address

Lists the IP address assigned to the managed machine.

Subnet Mask

Lists the subnet mask that the IP address belongs to.

Default Gateway/Connection Gateway

Lists the default and connection gateway in use by the managed machine.

Country

The country associated with the [Default Gateway/Connection Gateway](#).

MAC Address

Lists the Media Access Control (MAC) address of the machine listed, which uniquely identifies each node on a network.

DNS/DHCP

Audit > DNS/DHCP

DNS/DHCP displays DNS servers, DHCP server, Primary and Secondary WINS server information for all machine IDs currently matching the Machine ID / Group ID filter. Information shown in this function is collected when a [Latest Audit](#) (page 33) is performed. If a function is not used on a managed machine, not available is shown. For example, Secondary WINS servers are often not used.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in

Audit

-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

DNS Server

Displays the DNS servers in use by the managed machine.

DHCP Server

Displays the DHCP servers in use by the managed machine.

Primary/Secondary WINS

Displays the primary and, if used, the secondary WINS servers in use by the managed machine.

Disk Volumes

Audit > Disk Volumes

- Similar information is provided using Reports > [Disk Utilization](#) (page 305).

The [Disk Volumes](#) page displays drive letter, label, drive type (fixed, removable, CD-ROM or network), format, free space, used space and total size of drive information for all machine IDs currently matching the Machine ID / Group ID filter. Information shown in this function is collected when a [Latest Audit](#) (page 33) is performed.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Drive

Lists the drive letter in use by the managed machine for the selected drive.

Label

Lists the name given to the volume. In Windows, this value can be set and viewed by right-clicking the volume in any Explorer window and selecting [Properties](#).

Type

Lists the type of drive in use by the managed machine. The different types are:

- [Removable](#) - Examples include a ZIP drive, tape drive, optical drive, etc.
- [Fixed](#) - Standard non-removable hard drives.
- [CD-ROM](#) - CD-ROM, CD- RW and DVD-ROM drives, all reported as CD-ROM drives.
- [Network](#) - Mapped network drives accessible from the managed machine.

Format

Lists the formatting applied to the volume. Formats that can be read by the system are: NTFS, FAT32, FAT, and CDFS.

Free Space

Lists the available free space, in megabytes, as reported from removable and network drives.

User Space

Lists the used space, in megabytes, as reported from removable and network drives.

Total Size

Lists the total storage capacity, in megabytes, of the removable or network drive.

PCI & Disk H/W

Audit > PCI & Disk H/W

- Similar information is provided using [Reports > Inventory \(page 301\)](#).

The [PCI & Disk H/W](#) page displays information about network cards, controller cards, multimedia cards, hard disk controllers and other devices installed for all machine IDs currently matching the Machine ID / Group ID filter. Information shown in this function is collected when a [Latest Audit \(page 33\)](#) is performed.

The different types of devices reported by the system are:

- Network cards
- Graphics cards
- Multimedia (sound) cards
- Hard disk controller cards
- CD-ROM and hard disk vendor information

Disabling PCI & Disk H/W Audit

The agent uses a driver to query the PCI bus during an audit. Only disable this driver if you suspect a driver conflict on the managed machine. The agent can not audit PCI hardware cards if this driver is disabled.

Check-in status

These icons indicate the agent check-in status of each managed machine:



Agent has checked in

Audit

-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Type

Lists the type of device installed on the managed machine. This can include network interface cards, graphics cards, sounds cards, hard disks, and CD-ROM drives.

Vendor

Lists the manufacturer of the device installed on the managed machine.

Product

Lists the device installed in the managed machine.

Notes

Click the Notes icon  to maintain notes about this record.

CPU/RAM

Audit > CPU/RAM

The [CPU/RAM](#) page displays the CPU type, number of CPUs, CPU speed, and total physical RAM for all machine IDs currently matching the Machine ID / Group ID filter. Information shown in this function is collected when a [Latest Audit](#) (page 33) is performed. The amount of RAM reported may be slightly different than the actual physical RAM in the machine. This is the RAM information as reported by the operating system and is normal.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

CPU

Lists the manufacturer and model of the CPU as reported by the managed machine. If a managed machine has more than one CPU, the manufacturer and model is displayed for each one.

Quantity (Qty.)

Lists the number of CPUs used in the managed machine.

Speed

Lists the clock speed, in megahertz, of the managed machine. If a managed machine has more than one CPU, the speed is displayed for each one.

Note: Due to rounding, the listed speed of the processor may not match the speed specified by its manufacturer.

RAM

Lists the amount of physical random access memory available, in megabytes, as reported by the managed machine. The amount of RAM reported may be slightly different than the actual physical RAM in the machine. This is the RAM information as reported by the operating system and is normal.

Printers

Audit > Printers

The [Printers](#) page lists all printers mounted for the currently logged on user at the time the last audit ran, for all machine IDs currently matching the Machine ID / Group ID filter. Information shown in this function is collected when a [Latest Audit](#) (page 33) is performed.

Full column width

Column data is limited to to the width allotted for each column. Hovering over shortened data displays the full data as a tool tip. To display data in full width columns check this box.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Audit

Printers

Lists the name of each printer found during the latest audit.

Note: Printers are mounted on a per user basis. Therefore, the printers listed are those of the user who is logged on at the time of the audit. If no user is logged on, the printers of the Administrator account are reported.

Port

Name of the port this printer is connected to.

Model

Lists the model name reported by the manufacturer of each printer found.

Documents

Audit > Documents

- This function can also be accessed using the Documents tab of [Machine Summary \(page 21\)](#).

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.

To Store a Document

1. Click a machine ID.group ID link. The list of machine IDs you can select depends on the [Machine ID / Group ID filter \(page 17\)](#). Documents previously stored on the KServer for this machine ID display.
2. Click [Browse](#) to locate a file on your local computer or LAN.
3. Click [Upload](#) to upload the file to the Kserver.
The added [Filename](#) displays, along with its file [Size](#) and the date/time of the [Last Upload](#).

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 from the KServer.

Machine Summary

Audit > Machine Summary

- Similar information is provided using [Reports > Machine Summary \(page 296\)](#).

The [Machine Summary](#) page for any machine ID can be displayed immediately by clicking the check-in status icon next to any machine ID.

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in

 Online but waiting for first audit to complete

 Agent has been disabled

 Agent has been suspended

Alternatively, you can navigate to the Audit > [Machine Summary](#) page, which lists all machine IDs currently matching the [Machine ID / Group ID filter](#) (page 17), and click any machine ID to display the [Machine Summary](#) page.

Displaying the Machine Summary Page Using a URL

The following URL displays the [Machine Summary](#) (page 21) web page for a specific machine ID:

`http://...?machName=<MachineID>`

For example:

<http://demo.kaseya.com?machName=jconners.acme>

Machine Summary

The [Machine Summary](#) page allows administrators to perform tasks and functions solely for one managed machine. A tabbed property sheet provides access to various categories of information about the managed machine. The administrator can customize the layout of the [Installed Applications](#) and [System Info](#) tabs.

Note: Administrator access to the tabs of the Machine Summary page is determined using [System > Function Access](#) (page 387).

The following elements are displayed in the [Machine Summary](#):

- [Machine Info](#) - Current User, Domain/Workgroup, IP Address, Computer Name, Subnet Mask, OS, Version and Build, Default Gateway, Connection Gateway, RAM, MAC Address, CPU, DHCP Server, DNS Server, and Primary and Secondary WINS Servers, Last Checkin, Last Reboot, First Time Checkin.
- [Installed Applications](#) - Lists all the applications installed on the managed machine. Provides the same functionality as Audit > [Installed Apps](#) (page 36). Clicking the [Filter...](#) button enables you to filter the applications displayed by application attribute.
- [System Info](#) - Lists system hardware attributes and related information.
 - Click the [Show More](#) button to add or subtract system information attributes from the default list provided.
 - Click the automatic assignment icon  next to an system information attribute to manually edit the value. Click the manual edit icon  to display the [Edit Manual Input Value Only](#) dialog box. Use this dialog box to manually change the value of the attribute for this machine or for all machines using the current machine ID / group ID filter.
 - Click the [System Serial Number](#) link to display a machine manufacturer's support site, for the following manufacturers: Dell, IBM, Lenovo, HP, Compaq, Gateway, and Sony.
- [Disk Volumes](#) - Drive letter, Type, Format, Free Space, Used Space, Total Size, and Label.
- [PCI & Disk Hardware](#) - Type, Vendor, and Product name. Provides the same functionality as Audit > [PCI & Disk H/W](#) (page 41).
- [Printers](#) - Lists the printers and ports a machine can direct print jobs to.
- [Documents](#) - Lists documents uploaded to the KServer for a machine. You can upload additional documents. Provides the same functionality as Audit > [Documents](#) (page 44).
- [Pending Scripts](#) - Displays and schedules pending scripts for a machine and the script history for that machine. Includes the execution date/time and administrator who scheduled the script.
 - To add a script to the pending script schedule, click the [Click to schedule new script](#) link to display the [Search for Script](#) window and select a script. The name of the selected script

Audit

displays at the top of the [Pending Scripts](#) window. Enter scheduling parameters, then click the [Schedule](#) button.

- You can cancel any scheduled script by clicking the checkbox next to the pending script and clicking the [Cancel](#) button.
- [Agent Logs](#) - Displays the event logs available for a machine: Agent Log, Configuration Log, Network Statistics, Event Log, Script Log, Remote Control Log, Log Monitoring.
- [Alerts](#) - Defines alerts for a machine: Agent Status, Application Status, Get File Changes, Hardware Changes, Low Disk Space, Event Log, LAN Watch, Script Execution Failure, Protection Violations, Patch Alert, Backup Alert.
- [Patch Status](#) - Displays [Missing](#) and [Pending](#) Microsoft patches and schedules missing patches. If a machine belongs to a [patch policy](#) (page 478), missing patches may be further identified as [Denied](#) ([Pending Approval](#)). The user can manually override the denied patch policy by scheduling the patch.
 - To schedule a missing patch, check the box next to the patch, enter scheduling parameters and click the [Schedule](#) button.
 - To cancel a pending patch, check the box next to the patch and click the [Cancel](#) button.
 - To display the history of patches installed on a machine, click the [Show History](#) link.
- [Remote Control](#) - Displays and configures remote control settings for a machine.
- [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 Mgmt > [Membership: Patch Policy](#) (page 236)
 - [View Definition Collections](#) - Defined using the [Only show selected machine IDs](#) option in [View Definitions](#) (page 18).
 - [Temp Directory](#) - Can also be defined using Agent > [Temp Directory](#) (page 366).
 - [Check-In Control](#) - Can also be defined using Agent > [Check-In Control](#) (page 363).
 - [Edit Profile](#) - Can also be defined using Agent > [Edit Profile](#) (page 210) and Ticketing > [User Profiles](#) (page 210).
 - [Agent Logs and Profiles](#) - Can also be defined using Agent > [Log History](#) (page 328).
- [New Ticket](#) - Click this link to create a new ticket assigned to this machine ID using the [Ticket > View Ticket](#) (page 197) page.

Customizing the New Ticket Link

To customize the [New Ticket](#) link on the [Machine Summary](#) 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 KServer.

```
<?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>
```

File Access

Audit > 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.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled

Audit

 The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

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

Audit > 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.

Note: To determine which applications should be approved or denied network access, use the [Network Statistics](#) (page 306) report to view network bandwidth utilization versus time. Drill down and identify peak bandwidth consumers by clicking on 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.

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.
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.
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.

Notify user when app blocked

Click [Enable](#) to 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 user has four responses that they can enter for the given application:

- [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.](#)

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in

Audit

-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

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.

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

- 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`.

Application Blocker

Audit > 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.

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 17) 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (*page 476*) displayed is based on the [Machine ID / Group ID filter](#) (*page 17*) and the machine groups the administrator is authorized to see using [System > Group Access](#) (*page 385*).

Application

Filename of the application being blocked.

Chapter 5

Scripts



In This Chapter

Scripts Tab	54
Patch Deploy	55
Application Deploy	56
Creating Silent Installs	57
Packager	58
Get File	59
Distribute File	60
Scripts Status	61
Distribution	62
Script Browser and Script Toolbar	63
Script Manager	64
Script Scheduler	65
Script Editor	67
Manage Files Stored on Server	69
Variable Manager	70
IF-THEN-ELSE Commands	72

Scripts Tab

Scripts

Use the [Scripts Tab](#) to create and schedule automated tasks on managed machines.

Note: You can view Script demos at <http://www.kaseya.com/get-started/demo.aspx>.

Installations

You can schedule the installation of Microsoft and non-Microsoft applications and patches using [Patch Deploy](#) (page 55) and [Application Deploy](#) (page 56).

Note: See [Patch Management](#) (page 216) to install Microsoft patches on managed machines.

When a pre-defined install solution cannot be used, use [Packager](#) (page 58) to create a self-extracting file ready for automated distribution. Transfer files to and from managed machines using [Get File](#) (page 59) and [Distribute File](#) (page 60).

Script Analysis

You can view the status of all scripts run on a managed machine using [Scripts Status](#) (page 61). You can also spread out the impact scripts have on network traffic and server loading using [Distribute](#) (page 62).

Customized Scripts

You can also create user-defined scripts to modify files and/or the registry on managed machines.

- See [Script Browser and Script Toolbar](#) (page 63) for an introduction to managing scripts.
- See [Script Editor](#) (page 67) for an introduction to creating and editing scripts.
- See [IF-THEN-ELSE](#) (page 72) for a list of script commands available to you.

Windows vs. Macintosh

Customized scripts include the ability of specifying what type of operating system they should be run on, including managed machines running the Macintosh OS.

Functions	Description
Patch Deploy (page 55)	Use this wizard tool to create scripts to deploy patches to managed machines.
Application Deploy (page 56)	Use this wizard tool to create scripts to deploy third party install packages (setup.exe) to managed machines.
Packager (page 58)	An external application that allows administrators to create customized installation packages deployable on administered managed machines.
Get File (page 59)	View and manage files uploaded to the KServer from managed machines by a Get File script command.
Distribute File (page 60)	Write files to all selected managed machines and maintain them.
Scripts Status (page 61)	Shows the status of scripts executed on managed machines: machine.group ID, time of the last executed script, results of the executed script, and the number of times the script has been executed.

Distribution (page 62)	Minimize network traffic and server loading by executing scripts evenly throughout the day
--	--

Patch Deploy

Scripts > Patch Deploy

The [Patch Deploy](#) wizard is a tool that creates a script to distribute and apply Microsoft patches. The wizard walks you through a step by step process resulting in a script you can schedule to deploy a patch to any managed machine. See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

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 script for these hot fixes, via this wizard, that can be used to schedule the installation on any desired machine.

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 script, it restricts execution of the script 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 VSA server 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 VSA server 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 VSA server. Click the Back button and upload the file to the VSA 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 script. 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 which 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 480). 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 script.

The new script appears under the Install Tab. Master administrators can specify a shared script or private script. Standard Administrators can only create private scripts.

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.

Application Deploy

Scripts > Application Deploy

The [Application Deploy](#) page is a wizard tool that creates a script to distribute vendor installation packages, typically `setup.exe`. The wizard walks you through a step by step process resulting in a script 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 script 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 identifies the installer type.

Step 1: How do you want to deploy the application?

The wizard generated script 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 script. 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 here link to start FTP.](#)

Step 3: What kind of installer is this?

The wizard needs 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 script.

The new script appears under the Install Tab. Master administrators can specify a shared script or private script. Standard Administrators can only create private scripts.

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.

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 480*).

Silent Installs with InstallShield

InstallShield has a record mode that captures answers to all dialog boxes in the installation script. InstallShield requires the recorded response `iis` file to be on the managed machine during the installation. To deploy, the script must use `WriteFile` commands to send both the `setup.exe` and `record.iis` files from VSA server to the managed machine and then use `ExecuteFile` 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:

Scripts

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 /flc:\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 /flc:\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 `Write File` script 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 `Execute File` script command.
 - a. **If the install package is a single file** - Run `setup.exe /s /a /s /flc:\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 /flc:\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 script to perform the following:

1. Use the `Write File` script 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 `Execute File` script function.

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 script to perform the following:

1. Use the `Write File` script 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 `Execute File` script function.

Packager

Scripts > 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 scripts to any managed machine. Distribute a package any way you choose. You can email it, or store it on a server where a [custom script](#) (*page 63*) 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 script.

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

Scripts > Get File

The **Get File** page accesses files previously uploaded from a managed machine. Files can be uploaded to the KServer using the **Get File** or **Get File In Directory Path** commands. The KServer stores uploaded files in a unique directory for each machine ID. Clicking the machine ID displays *all* uploaded files for that machine ID.

Note: This set of files is machine-specific. Use **Manage Files Stored on Server** (*page 69*) to access files stored on the KServer 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 Cntl > FTP** (*page 277*) is the simplest way.

Use **Get File** in conjunction with a script 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 script to do the following:

Scripts

1. Send the utility to the managed machine using either the [Write File](#) script command or the [Distribute File](#) page.
2. Execute the utility using either the script command [Execute DOS Command](#) or [Execute File](#) command and pipe the output to a text file, such as `results.txt`.
3. Upload the file to the KServer using the [Get File](#) command.

Example 2: Comparing Versions of a File

As an option in the [Get File](#) script 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-THEN-ELSE Script Editor to create a simple [Get File](#) script. The complete script displays in text format as follows when you click the [Export Script...](#) link on the [script editor](#) (page 67) page:

```
Get File
Parameter 1 : c:\temp\info.txt
Parameter 2 : news\info.txt
Parameter 3 : 2
OS Type : 0
```

Parameter 3 : 2 causes the following to occur if the file changes: save existing version, get file, and send alert. The first time the above script statement executes on a managed machine the agent sends `c:\temp\info.txt` to the KServer and the KServer stores it. The second time the above statement executes, the KServer 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 [Get File](#) 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 script on a recurring schedule and activate a [Get File Changes](#) alert using Monitor > [Alerts](#) (page 100). 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 `KBxxxxxxx.log` and the `WindowsUpdate.log` are uploaded to the KServer. These logs can be reviewed using Scripts > [Get File](#) (page 59) for a specific machine and can help you troubleshoot patch installation failures. The Reports > [Logs](#) (page 309) > Script Log contains entries indicating these log files have been uploaded to the KServer for each machine.

Distribute File

Scripts > 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 473). 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 script execution. Use it in conjunction with recurring scripts to run batch commands on managed machines.

Note: The script command `Write File` performs the same action as `Distribute File`. Each time a script executes the `Write File` command, the agent checks to see if the file is already there or not. If not, the file is written. `Write File` is better than `Distribute File` for sending executable files you plan to run on managed machines using scripts.

Select server file

Select a file to distribute to managed machines. These are same set of files managed by clicking the [Managed Files...](#) link.

Note: The only files listed are your own private managed files or shared managed files. If another administrator 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 67*) link to open the [Manage Files Stored on Server](#) popup window. Use this window to add, update, or remove files stored on the KServer. This same window displays when you select [Managed Files...](#) using the [Script Editor](#) (*page 67*). Private files are listed with `(Priv)` in front of the filename. Master administrators see all file distributions. Instead of the `(Priv)` prefix, `(admin name)` is listed.

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 KServer. 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.

Agent File Location

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 for that machine ID.

Scripts Status

Scripts > Scripts Status

- Similar information is displayed in using the [Pending Scripts](#) tab of [Audit > Machine Summary](#) (*page 21*).

The [Scripts Status](#) function page allows administrators to display the status of scripts for a selected machine ID. The list of machine IDs you can select is based on the [Machine ID / Group ID filter](#) (*page 17*). Administrators can, at a glance, find out what time a script was executed and whether it was

Scripts

successfully executed. See [Using Scripts](#) (page 63) for more information about scripts.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Time

Displays the date and time the script was last executed.

Status

Displays the results of the executed script. Pending or recurring scripts are displayed **as red text with yellow highlight**.

Admin

Displays the administrator who scheduled the script.

Distribution

Scripts > Distribution

The [Distribution](#) page spreads network traffic and server loading by executing scripts evenly throughout the day or a specific block of time in a day. Applies to scripts currently scheduled to run on a [recurring basis](#) only. See [Scheduling Scripts](#) (page 63) for more information.

Note: Recurring scripts listed here include function-specific scripts that are not visible in your Script Browser (page 63), such as scripts created using a Patch Management wizard.

Scripts can cause excessive network loading by pushing large files between the KServer and agent. Performing these operations with hundreds of agents simultaneously may cause unacceptable network loading levels.

Script Histograms

The system plots a histogram for each script currently scheduled to run on a recurring basis. Setting the histogram period to match the recurring interval of the script counts how many machines execute the script in a specific time interval. Peaks in the histogram visually highlight areas where a lot of machines are trying to execute the script 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 script such that the network loading is spread evenly over time. **Only machine IDs currently matching Machine ID / Group ID filter are counted in the histogram.**

Reschedule selected script evenly through the histogram period

Pick this radio control to reschedule selected scripts running on all machines IDs currently matching the [Machine ID / Group ID filter](#) (page 17). Script execution start times are staggered evenly across the entire histogram period.

Reschedule selected script evenly between <start time> and <end time>

Pick this radio control to reschedule selected scripts running on all machines IDs currently matching the Machine ID / Group ID filter. Script 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 this box to only allow the script to run at the scheduled time of day, within a 15 minute window. If the machine is offline at the scheduled time, then the script does not execute at all. If recurring is set, then the script is rescheduled to run at the next appointed time.

Distribute

Click the [Distribute](#) button to schedule selected scripts, using the schedule parameters you've defined.

Note: The script recurring interval is replaced with the histogram period.

Select Histogram Period

Selects the schedule time period for the histograms.

Histogram Plots

Each recurring script displays a histogram of all the machine IDs that are scheduled to run that script within the selected histogram period. Only machine IDs currently matching Machine ID / Group ID filter are counted in the histogram.

Above the histogram is a:

- [Script name](#) - name of the script. Check the box next to the script name to select this script for distribution.
- [Peak](#) - the greatest number of machines executing the script at the same time.
- [Total](#) - total number of machines executing the script.

Script Browser and Script Toolbar

Scripts > Script Browser

All *user-defined* scripts are displayed and selected using the [Script Browser](#). Sample scripts can be loaded using the System > [Configure](#) (page 394) page. Within the script browser:

- Clicking a folder displays the [Script Manager](#) (page 64).
- Clicking a script displays the [Script Scheduler](#) (page 65).

Scripts that can be used by all administrators are listed under [Public Scripts](#). New scripts are created initially as private scripts and listed under [My Scripts](#). Private scripts can be shared with individual administrators or with administrator roles or made public using the [Script Editor](#).

Scripts

Note: Function specific scripts, such as the scripts defined using the Patch Deploy (page 55) wizard, are not displayed in the Script Browser and cannot be changed using the Script Editor (page 67).

System Scripts

Certain scripts are provided as **system scripts**. They display as an option when you use the search tool to locate a script. System scripts cannot be edited nor can they be run as top level scripts. System scripts can only be run from within another script using the **Execute Script** or **Schedule Script** commands.

Script Toolbar

The Script Toolbar displays at the top of the Script Browser and provides the following:

-  Open/expand all folders
-  Close/collapse all folders
-  Search tool used to locate a script.

Note: You cannot select, edit or run a system script (page 477) directly from within the script browser.

-  Import a new script
-  Create a new script and open the **Script Editor** (page 67).

Note: New scripts are always created initially as private scripts. Private scripts can be shared or made public using the Script Editor.

-  Displays the **Manage Files Stored on Server** (page 69) popup window.

Script Manager

Scripts > Script Browser > *script folder*

Click any script *folder* in the **Script Browser** (page 63) to open the **Script Manager**. With **Script Manager** you can:

- Take ownership of any public script or public folder.
- Rename, delete or edit any script you have ownership of.
- Re-order, or move any script or folder contained in the selected script folder.
- Create new folders.
- Import and export folders.

In addition Script Manager includes a set of toolbar buttons:

-  Open/expand all folders
-  Close/collapse all folders
-  Sort all scripts and folders in the current folder alphabetically
-  Search tool used to locate a script

Note: You cannot select, edit or run a system script (page 477) directly from within the script browser.

-  Create a new script and open the **Script Editor** (page 67).

Note: New scripts are always created initially as private scripts. Private scripts can be shared or made public using the Script Editor.

Sort

Click the up/down arrows  to move a script or folder up or down in the list.

Edit

Click the [Edit](#) button to edit a script.

Note: You can't edit a public script you don't own. Use [Script Editor](#) to save the script under a different name or accept ownership to edit the original script.

Take Ownership...

This link displays if you don't own a public script. Click the [Take Ownership](#) link to display the [Rename...](#) and [Delete...](#) buttons.

Rename...

Click the [Rename...](#) button to a script or folder. The new name must be less than 64 characters in length.

Delete...

Click the [Delete...](#) button to delete a script or folder.

New Public... / New Folder...

Click the [New Public...](#) button to create a new public folder or the [New Folder...](#) button to create a new private folder.

Move

Select a new destination folder from the `<Select New Folder>` drop down list to move a script or folder.

Note: *Public* scripts and folders cannot be moved into *private* folders. *Private* scripts and folders cannot be moved into *public* folders.

Import and Export Folders

Script folders can be imported or exported as XML formatted files. Click the [Export Folder](#) link to export any folder. Click [Public Scripts](#) or [My Scripts](#) to access the [Import Folder](#) link.

Note: *Scripts* are imported and exported using the [Script Editor](#) ([page 67](#)) or by using the [Import Script](#)  toolbar button at the top of the [Script Browser](#).

Script Scheduler

Scripts > Script Browser

- Click a script in the [Script Browser](#) ([page 63](#)) or from a [Script Manager](#) ([page 64](#)) page to display the [Script Scheduler](#) page.

The [Script Scheduler](#) page schedules or immediately runs an existing script. If necessary, click the [Edit](#)

Scripts

(page 67) button to edit the script.

1. Set scheduling options for the script.
2. Select machine IDs. The list of machine IDs you can select depends on the [Machine ID / Group ID filter](#) (page 17) and machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).
3. Press either the [Schedule](#) or [Run Now](#) button.

Edit

Click [Edit](#) to edit the script using [Script Editor](#) (page 67).

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

Click [Cancel](#) to cancel execution of this task on selected managed machines.

Run Now

Click [Run Now](#) to run this task on selected machine IDs immediately.

Run recurring every <N> <period>

Check the box to make this task a recurring task. Enter the number of times to run this task each time period.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task 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, ...

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.

Last Execution Time/Last Execution Status

If a previous script was performed, the date of the last script and its status is displayed.

Next Scheduled Run/Recurring Interval

Shows the time of the next scheduled script and its execution frequency.

Auto Refresh

Selecting this checkbox automatically updates the paging area every five seconds.

Script Editor

Scripts > Script Browser >  toolbar button

Scripts > Script Manager > Edit

Scripts > Script Scheduler > Edit

The [Script Editor](#) creates and maintains customizable scripts that perform specialized tasks on managed machines. A number of pre-defined scripts are distributed with the VSA. Additional pre-defined scripts can be downloaded from the Kaseya user forum. These scripts can be used as is or customized by administrators. Scripts can be maintained using the [Script Editor](#) or imported and exported as text files and edited in any text editor.

Scripts are organized by three main statements:

1. Each script begins with an **IF** statement.
2. If the statement is true, the **THEN** statement is executed.
3. If the statement is false, the **ELSE** statement is executed.

Drop down lists provide the set of [IF-THEN-ELSE parameters](#) (page 72) appropriate for each statement.

Operating System Detect

When writing a [THEN-ELSE](#) statement, you can select the operating system the script will execute on. This parameter is useful when you want to write one script that can be executed on different operating systems. For example, directory paths in Windows and Macintosh can require different directory path syntax in order to work correctly. Creating two separate script steps within the same script for All Windows Operating Systems and a Mac OS X operating system, avoids having to create an extra script for a separate operating system.

Guidelines

Use the following guidelines when constructing a script:

- Multiple steps can be defined under either the **THEN** statement or **ELSE** statement.
- If no conditional statement is required, set the **IF** statement to `True` and define one or more steps underneath the **THEN** statement and *no* steps underneath the **ELSE** statement.
- Each script can have only one **IF** statement. Nest **IF** statements by adding a step underneath the **THEN** or **ELSE** statement and use the [Execute Script](#) command. There is no limit to the number of nested scripts allowed.
- When nesting scripts, only the top level script has to be scheduled to run.
- Launch scripts written in other scripting languages by using the [Execute File](#) or [Execute Shell Command](#).

Using Variables

Use variables to store values that can be referenced in multiple script steps. Variables are passed automatically to nested scripts.

- **Two Methods for Creating Variables:**
 - [Script Variables](#) - Use the [Get Variable](#) command within a script to create a new variable name without any special characters. Example: `VariableName`. In subsequent steps, including steps in nested scripts, reference the variable by bracketing the variable name with the `#` character. Example: `#VariableName#`. Scripts variables cannot be referenced outside of the script or nested scripts that use them.
 - [Managed Variables](#) - Use the [Variable Manager](#) (page 70) to define variables that can be used repeatedly in different scripts. 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 script. Within a script, reference a managed variable by bracketing the variable name with the `<` and `>` character. Example: `<VariableName>`.

Scripts

- **Where Used** - Once variables are created you can include them, in their bracketed format, *in any text entry field* displayed by an IF-THEN-ELSE 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 script runtime as `c:\dir > filelist.txt`.
 - **Types of Variable Values Possible** - The following are the types of variable values typically obtained by using the **Get Variable** parameter.
 - **Registry Value** - Data from the specified registry value on the managed machine.
 - **File Content** - Data from a specified file on the managed machine.
 - **Constant Value** - Specified constant as typed in the script editor.
 - **Expression Value** - Specify an expression that consists of script variables and six mathematical operators +, -, *, /, (, and) that are evaluated and assigned to a new script variable. For example, $((\#variable1\# + \#variable2\#) + 17.4) / (\#variable3\# * 4)$. The script variables must contain numeric values.
 - **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 Temp Directory Path** - Temporary directory on the managed machine as specified on the **Temp Directory** function on the agent tab.
 - **User Temp Directory Path** - The temporary directory for the user currently logged in on the managed machine. This path is the expansion of the `%TEMP%` environment variable for the currently logged in user. If no user is logged in, it is the default Windows temporary directory.
 - **Machine.Group ID** - Machine ID of the agent executing the script.
 - **File Version Number** - Version number from the property of the specified file on the managed machine.
 - **File Size** - Size in bytes of the specified file on the managed machine.
 - **File Last Modified Date** - Date of the specified file on the managed machine in the format of `yyyy/mm/dd hh:mm:ss`.
 - **SQL View Data** - Use the **GetVariable** command with the **SQL View Data** option to create a new script 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 script is retrieved. If `ColumnName` contains a space, surround it with square brackets. Example: `vSystemInfo/[Product Name]`. See **System > Database Views** (page 410) for a list of the SQL views and columns that are available.
- Note: - Automatic SQL View Data Variables - SQL view parameters are available as automatically declared script variables. Automatic variables enable you to skip using the **GetVariable** command with the **SQL View Data** option. Use the format `#SqlViewName.ColumnName#` in a script to return the value of a `dbo.SqlView.Column` for the agent executing the script.
- **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`.

Import Script...

Click the [Import Script...](#) link to display the [Import Script](#) popup window. Click [Browse...](#) to select the text file to be imported. Click [Import](#) to load the script into the Script Editor.

Note: Importing new scripts are always imported as private scripts. They can be shared or made public afterwards.

Export Script...

Click the [Export Script...](#) link to display the script in text format in the [Export Script](#) popup window. You can copy it to the clipboard or download it to a text file.

Manage Files...

Click the [Manage Files...](#) link to display the [Manage Files Stored on Server](#) (page 69) popup window.

Manage Variables...

Click the [Manage Variables...](#) link to display the [Variable Manager](#) (page 70) popup window.

Take Ownership...

You can't edit a public script you don't own. Click the [Take Ownership](#) link to display the [Save](#), [Rename...](#) and [Delete...](#) buttons. Otherwise you can make a copy of the current script using the [Save As...](#) button.

Share...

You can share scripts you own with other [individual administrators](#) (page 388), [administrator roles](#) (page 383), or make the script public to all administrators.

Note: A master administrator can take ownership of a script and change share rights.

Save As...

Select [Save As...](#) to save a script under a different name. The script name must be less than 64 characters in length.

Save

Select [Save](#) to save changes to a script.

Rename

Select [Rename](#) to rename a script.

Delete

Select [Delete](#) to delete a script.

Script Notes

Enter any notes about the script.

Manage Files Stored on Server

Scripts > Script Browser >  Toolbar Button
 ... Script Editor > Manage Files

Only files stored on the KServer can be distributed to managed machines. Scripts distribute files

Scripts

stored on the KServer to managed machines using the [Write File](#) or [Write File in Directory Path](#) commands.

Note: This set of files is not machine specific. Use [Get File \(page 59\)](#) to access machine-specific files stored on the server.

Use the [Manage Files Stored on Server](#) popup window to upload a file and store it on the KServer. You can also list, display and delete files already stored on the KServer.

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 administrators.
- Click [Browse...](#) to locate files to upload. Then click [Upload](#) to upload the file to the KServer.

To delete a file stored on the KServer:

- 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 KServer.

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 administrator. Put shared files into the `VSASharedFiles` directory. Any files located in this directory will automatically update what is available in the scripting user interface at the next administrator logon.

Variable Manager

Use the [Variable Manager](#) to define variables that can be used repeatedly in different scripts. 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 script. Within a script, reference a managed variable by bracketing the variable name with the < and > character. Example:

```
<VariableName>.
```

Using managed variables, managed machines can run scripts that access *locally available resources* based on the group ID or subgroup ID.

Note: Using [System > Naming Policy \(page 380\)](#), this benefit can be applied automatically by IP address even to a highly mobile workforce that travels routinely between different enterprise locations.

Using Variables

Use variables to store values that can be referenced in multiple script steps. Variables are passed automatically to nested scripts.

- **Two Methods for Creating Variables:**
 - **Script Variables** - Use the [Get Variable](#) command within a script to create a new variable name without any special characters. Example: `VariableName`. In subsequent steps, including steps in nested scripts, reference the variable by bracketing the variable name with the # character. Example: `#VariableName#`. Script variables cannot be referenced outside of the script or nested scripts that use them.
 - **Managed Variables** - Use the [Variable Manager \(page 70\)](#) to define variables that can be used repeatedly in different scripts. 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 script. Within a script, reference a managed variable by bracketing the variable name with the < and > character. Example: `<VariableName>.`

- **Where Used** - Once variables are created you can include them, in their bracketed format, *in any text entry field* displayed by an IF-THEN-ELSE 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 script runtime as `c:\dir > filelist.txt`.
 - **Types of Variable Values Possible** - The following are the types of variable values typically obtained by using the **Get Variable** parameter.
 - **Registry Value** - Data from the specified registry value on the managed machine.
 - **File Content** - Data from a specified file on the managed machine.
 - **Constant Value** - Specified constant as typed in the script editor.
 - **Expression Value** - Specify an expression that consists of script variables and six mathematical operators +, -, *, /, (, and) that are evaluated and assigned to a new script variable. For example, $((\#variable1\# + \#variable2\#) + 17.4) / (\#variable3\# * 4)$. The script variables must contain numeric values.
 - **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 Temp Directory Path** - Temporary directory on the managed machine as specified on the **Temp Directory** function on the agent tab.
 - **User Temp Directory Path** - The temporary directory for the user currently logged in on the managed machine. This path is the expansion of the `%TEMP%` environment variable for the currently logged in user. If no user is logged in, it is the default Windows temporary directory.
 - **Machine.Group ID** - Machine ID of the agent executing the script.
 - **File Version Number** - Version number from the property of the specified file on the managed machine.
 - **File Size** - Size in bytes of the specified file on the managed machine.
 - **File Last Modified Date** - Date of the specified file on the managed machine in the format of `yyyy/mm/dd hh:mm:ss`.
 - **SQL View Data** - Use the **GetVariable** command with the **SQL View Data** option to create a new script 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 script is retrieved. If `ColumnName` contains a space, surround it with square brackets. Example: `vSystemInfo/[Product Name]`. See **System > Database Views** (page 410) for a list of the SQL views and columns that are available.
- Note: - Automatic SQL View Data Variables - SQL view parameters are available as automatically declared script variables. Automatic variables enable you to skip using the **GetVariable** command with the **SQL View Data** option. Use the format `#SqlViewName.ColumnName#` in a script to return the value of a `dbo.SqlView.Column` for the agent executing the script.
- **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`.

Scripts

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](#).

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 administrators. However, only master administrators can create and edit shared variables.

Private

Selecting the [Private](#) radio button allows the variable to be used only by the administrator 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.

IF-THEN-ELSE Commands

The following is a summary of IF-THEN-ELSE parameters used in VSA scripts.

IF Definitions

Application is Running	Test to see if the specified application is running.
Check Registry Value	Evaluate the given registry value.
Check Variable	Evaluate the given agent variable.
Evaluate Expression	Compares a variable with a supplied value.
Service is Running	Determines if a service is running on the managed machine.
Test File	Test for the existence of a file.

Test File in Directory Path	Test for the existence of a file in the current directory path.
Test Registry Key	Test for the existence of the given registry key.
True	Always returns <code>True</code> , executing THEN branch.
User Is Logged In	Tests whether a specific user, or any user, is logged in or not.
User Response is Yes	Presents a Yes/No dialog box to the user.

THEN/ELSE Definitions

Close Application	Close a running application.
Delete File	Delete a file from the managed machine.
Delete File in Directory Path	Delete file in directory returned by Get Directory Path From Registry .
Delete Registry Key	Delete the key from the registry.
Delete Registry Value	Delete the value from the registry.
Execute File	Execute any file as if it was run from the Run item in the Windows Start menu.
Execute File in Directory Path	Same as execute file. File location is relative to the directory returned by Get Directory Path From Registry .
Execute Script	Start another VSA script.
Execute Shell Command	Run any command from a command shell.
Get Directory Path From Registry	Returns the directory path stored in the registry at the specified location.
Get File	Get a file from the managed machine and save it to the KServer.
Get File in Directory Path	Get a file from the managed machine located relative to the directory returned by Get Directory Path From Registry and save it to the KServer.
Get Variable	Get a value from the agent on the managed machine and assign it to a variable
Impersonate User	Use the specified user account to execute a file or shell when Execute as user is specified.
Pause Script	Pause the script for N seconds.
Reboot	Reboot the managed machine.
Rename Locked File	Renames a file that is currently in use.
Rename Locked File in Directory Path	Renames a file in directory returned by Get Directory Path From Registry that is currently in use.
Schedule Script	Schedules a script to be run.
Send Email	Sends an email to one or more recipients.
Send Message	Displays a message in a dialog box on the managed machine.
Send URL	Open a browser to the specified URL on the managed machine.
Set Registry Value	Set the registry value to a specific value.
Use Credential	Use the user logon credentials set for the machine ID in Set Credential to execute a file or

	shell when Execute as user is specified.
Write Directory	Writes a directory from the server to the managed machine.
Write File	Write a file stored on the KServer to the managed machine.
Write File in Directory Path	Write a file stored on the KServer to the managed machine using the directory returned by Get Directory Path From Registry .
Write Script Log Entry	Write a string to the Script Log.

Using Variables

Use variables to store values that can be referenced in multiple script steps. Variables are passed automatically to nested scripts.

- **Two Methods for Creating Variables:**
 - **Script Variables** - Use the [Get Variable](#) command within a script to create a new variable name without any special characters. Example: `VariableName`. In subsequent steps, including steps in nested scripts, reference the variable by bracketing the variable name with the # character. Example: `#VariableName#`. Scripts variables cannot be referenced outside of the script or nested scripts that use them.
 - **Managed Variables** - Use the [Variable Manager](#) (*page 70*) to define variables that can be used repeatedly in different scripts. 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 script. Within a script, reference a managed variable by bracketing the variable name with the < and > character. Example: `<VariableName>`.
- **Where Used** - Once variables are created you can include them, in their bracketed format, *in any text entry field* displayed by an IF-THEN-ELSE 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 script runtime as `c:\dir > filelist.txt`.
- **Types of Variable Values Possible** - The following are the types of variable values typically obtained by using the [Get Variable](#) parameter.
 - **Registry Value** - Data from the specified registry value on the managed machine.
 - **File Content** - Data from a specified file on the managed machine.
 - **Constant Value** - Specified constant as typed in the script editor.
 - **Expression Value** - Specify an expression that consists of script variables and six mathematical operators +, -, *, /, (, and) that are evaluated and assigned to a new script variable. For example, `((#variable1# + #variable2#) + 17.4) / (#variable3# * 4)`. The script variables must contain numeric values.
 - **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 Temp Directory Path** - Temporary directory on the managed machine as specified on the [Temp Directory](#) function on the agent tab.
 - **User Temp Directory Path** - The temporary directory for the user currently logged in on the managed machine. This path is the expansion of the `%TEMP%` environment variable for the

currently logged in user. If no user is logged in, it is the default Windows temporary directory.

- **Machine.Group ID** - Machine ID of the agent executing the script.
- **File Version Number** - Version number from the property of the specified file on the managed machine.
- **File Size** - Size in bytes of the specified file on the managed machine.
- **File Last Modified Date** - Date of the specified file on the managed machine in the format of `YYYY/mm/dd hh:mm:ss`.
- **SQL View Data** - Use the `GetVariable` command with the `SQL View Data` option to create a new script 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 script is retrieved. If `ColumnName` contains a space, surround it with square brackets. Example: `vSystemInfo/[Product Name]`. See `System > Database Views` (page 410) for a list of the SQL views and columns that are available.

Note: - Automatic SQL View Data Variables - SQL view parameters are available as automatically declared script variables. Automatic variables enable you to skip using the `GetVariable` command with the `SQL View Data` option. Use the format `#SqlViewName.ColumnName#` in a script to return the value of a `dbo.SqlView.Column` for the agent executing the script.

- **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`.

IF Parameters

Application is Running

Checks to see if a specified application is currently running on the managed machine. If the application is running, the **THEN** statement is executed; otherwise, the **ELSE** statement is executed. When this option is selected from the drop-down list, the **Enter the application name** field appears.

Check Registry Value

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.

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 available tests are:

- **Exists** : true if the registry key exists in the hive.
- **Absent** : 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).

Scripts

- `>=` : 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).

Check Variable

Enter a variable name, in the form `#var_name#`, in the space provided. **Check Variable** evaluates the current 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, **THEN** steps are executed. If the check is false, **ELSE** steps are executed. The available tests are:

- `Exists` : true if the variable exists.
- `Absent` : 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 (variable must be a string).
- `Not Contains` : true if the test value is *not* a sub string of the variable (variable must be a string).

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`. 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 script 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 script is executed.

Evaluate Expression

Enter an expression containing one or more variable names, in the form `#var_name#`, in the space provided. **Evaluate Expression** 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, **THEN** 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`, `Absent`, `Contains`, or `Not Contains` operators.

Service is Running

Determines if a service is running on the managed machine.

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

Test File

Determines if a file exists on a managed machine. Enter the full path and filename. For example, entering `c:\windows\notepad.exe` returns `True` if `Notepad.exe` exists, `False` if it does not.

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

Test File in Directory Path

Enter the name of a file to see if it exists on the managed machine. Because a `THEN` or `ELSE` step must be executed prior to this `IF` test, `Test File in Directory Path` is only useful for scripts called by the `THEN` or `ELSE` step of a parent script.

Test Registry Key

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

True

Selecting `True` directs the `THEN` steps 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 `Test File`.

User Is Logged In

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

User Response is Yes

Displays a dialog box on the managed machine with `Yes` and `No` buttons. Also carries out the `ELSE` statement if an administrator-configured specified amount of time has timed out. If `Yes` is selected by the user, the `THEN` statement is executed. If the selection times out or the user selects `No`, the `ELSE` statement is executed. This function requests the user's permission to proceed with the script. This query is useful for scripts that require a reboot of the managed machine before completion.

Script variables, for example `#varName#`, may be used inside `User Response is Yes` fields to dynamically generate messages based on script data.

THEN-ELSE Parameters

Operating System Detect

When writing a `THEN-ELSE` statement, you can select the operating system the script will execute on. This parameter is useful when you want to write one script that can be executed on different operating systems. For example, directory paths in Windows and Macintosh can require different directory path syntax in order to work correctly. Creating two separate script steps within the same script for `All Windows Operating Systems` and a `Mac OS X` operating system, avoids having to create an extra script for a separate operating system.

Scripts

Close Application

If the specified application is running on the managed machine, then that application is closed down.

Delete File

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`.

Delete File in Directory Path

Deletes the specified file located at the path returned using the [Get Directory Path From Registry](#) parameter.

Delete Registry Key

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

Delete Registry Value

Delete the value stored at the specified registry key.

Execute File

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
- Flag indicating whether the script should wait until the `.exe` completes or not. (1 to wait, 0 to have the script continue without waiting).

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`.

Execute File in Directory Path

Same as [Execute File](#) except the location of the `.exe` file is located at the path returned from a [Get Directory Path From Registry](#) parameter.

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`.

Execute Script

Causes another named script to execute. Use this capability to string multiple **IF-THEN-ELSE** clauses together. If the script no longer exists on the KServer, an error message displays next to the script drop-down list. You can use this command to run a [system script](#) (*page 483*).

Execute Shell Command

Allows the script 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 prompt](#) 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: Execute Shell Command opens a command prompt window on the managed machine to execute in. If you do not want a window opening on the managed machine, because it might confuse users, put all the commands into a batch file. Send that file to the managed machine using the Write File command. Then run the batch file with the Execute File command. Execute File does not open a window on the managed machine.

Get Directory Path From Registry

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.

Get File

Upload the file at the specified path from the managed machine. Be sure to enter a full path filename that you want to upload. The file is stored on the KServer in a private directory for each managed machine. Access the uploaded file using Scripts > [Get File](#) (page 59).

- 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 send an email alert if the uploaded file *differs* from the file that was uploaded previously.
- Optionally send an email alert if the uploaded file is the *same* as the file that was uploaded previously.

Get File in Directory Path

Just like the [Get File](#) command but it adds the path returned from the [Get Directory Path From Registry](#) command to the beginning of the remote file path. Access the uploaded file using Scripts > [Get File](#) (page 59) function.

Get URL

Returns the URL of a website page and stores it in a file.

Get Variable

Defines a new agent variable. When the script 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](#) at the top of this topic for the types of variable values supported by the [Get Variable](#) parameter.

Impersonate User

Enter a username, password, and domain for the agent to log in with, when [Execute as user...](#) is specified using [Execute File](#), [Execute File in Directory Path](#) or [Execute Shell Command](#). Leave the domain blank to log into an account on the local machine.

Pause Script

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

Scripts

Reboot

Unconditionally reboots the managed machine. To warn the user first, preface this command with a [User Response is Yes](#) message. A [User Response is Yes](#) message prompts the user before rebooting their machine.

Rename Locked File

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. [Rename locked file](#) can also be used to delete a file that is currently in use if the destination is empty. The file is deleted when the system is rebooted.

Rename Locked File in Directory Path

Renames a file that is currently in use. The file is renamed the next time the system is rebooted. The specified file name is appended to the directory path. [Rename locked file in directory path](#) can also be used to delete a file that is currently in use if the destination is empty. The file is deleted when the system is rebooted.

Schedule Script

Schedules a script to be run. Optionally specifies the time to wait after executing this step before running the script and the specific machine ID to run the script on. You can use this command to run a [system script](#) (page 483).

Send Email

Sends an email to one or more recipients. Specifies the subject and body text of the email.

Send Message

Sends the entered message to a managed machine. Selecting [Immediately](#) displays a message dialog box immediately. Selecting [After user clicks the flashing system tray icon](#) flashes the agent system tray icon when a message is received. The message is displayed when the user clicks the icon.

Send URL

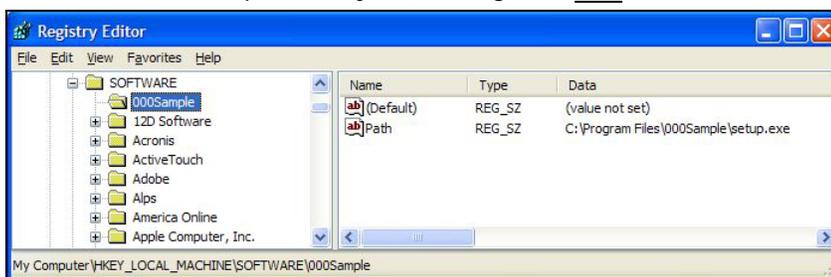
Sends the entered URL to a managed machine. Selecting [Immediately](#) launches the default web browser and the specified URL is displayed. Selecting [After user clicks the flashing system tray icon](#) flashes the agent system tray icon when a message is received. The URL is displayed in the default web browser when the user clicks the icon.

Set Registry Value

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 Name column in image below.
Example of setting the (Default) value: HKEY_LOCAL_MACHINE\SOFTWARE\000Sample\
 - [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.



Use Credential

Use the credentials set for the machine ID in [Set Credential](#) (page 371) to execute a file or shell when [Execute as user...](#) is specified using [Execute File](#), [Execute File in Directory Path](#) or [Execute Shell Command](#). The `Use Credential` script command behaves the same as the `Impersonate User` command except a unique credential can be used to access each machine instead of using a fixed credential in a script.

Note: A script execution error is logged if a `Set Credential` script command encounters an empty username.

Write Directory

Writes a selected directory, including subdirectories and files, from [Manage Files Stored on Server](#) (page 69) to the full path directory name specified on the managed machine.

Write File

Writes a file selected from a drop down list from [Manage Files Stored on Server](#) (page 69) 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 script executes the `Write File` 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 script moves to the next step. You can repeatedly run a script with `Write File` 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`.

Write File in Directory Path

Writes the specified filename to the path returned from a [Get Directory Path From Registry](#) command.

Write Script Log Entry

Writes the supplied string to the script log for the agent executing this script.

Chapter 6

Monitor

In This Chapter

Monitor Tab	84
Alarms	86
Dashboard List	88
Settings	96
Alarm Summary	96
Suspend Alarms	98
Live Connect	99
Alerts	100
Monitor Lists	138
Update Lists By Scan	140
Monitor Sets	140
Assign Monitoring	147
Monitor Log	153
System Check	154
SNMP Sets	158
LAN Watch	165
Assign SNMP	168
SNMP Log	175
Set SNMP Values	177
SNMP Type	178
Parser Summary	179
Log Parser	182
Assign Parser Sets	187

Monitor Tab

Monitor

The **Monitoring** tab in **Kaseya® Virtual System Administrator™** provides five methods of monitoring machines and log files:

- **Alerts** - Monitors events on *agent-installed* machines.
- **Monitor Sets** - Monitors the performance state on *agent-installed* machines.
- **SNMP Sets** - Monitors the performance state on *non-agent-installed devices*.
- **System Check** - Monitors events on *non-agent-installed* 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, scripts and job ticketing, for such problems and state changes as:

- When any critical server or desktop computer goes off-line.
- When a 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 script 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 327*) page, as well as the **Logs** (*page 309*) reports.

Note: You can view Monitor demos at <http://www.kaseya.com/get-started/demo.aspx>.

Note: You can download a Monitoring Configuration **MonitoringGuide51.pdf** PDF from the first topic of online help.

Note: You can download a **Configuring Log Parsers Step-by-Step** PDF from the first topic of online help.

Note: Kaseya's IT Monitor Assist service 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.

Function	Description
Dashboard List (<i>page 88</i>)	Provides multiple monitoring views.
Settings (<i>page 96</i>)	Administrators can customize the Dashboard List page.
Alarm Summary (<i>page 96</i>)	List of alarms for monitored machines.
Suspend Alarms (<i>page</i>)	Suspend alarm notifications for specific machine IDs.

98)	
Live Connect (page 99)	Real time view of monitor counter objects.
Monitor Lists (page 138)	Configure the monitor list objects for monitoring.
Update Lists By Scan (page 140)	Scan machines for monitor counters and services.
Monitor Sets (page 140)	Configure monitor sets.
SNMP Sets (page 158)	Configure SNMP monitor sets.
Add SNMP Object (page 163)	Manage SNMP MIB objects.
Alerts (page 100)	Configure monitor alerts for machines.
Assign Monitoring (page 147)	Assign, remove and manage alarms of monitor sets on machines.
Monitor Log (page 153)	View monitor log data in chart and table format.
System Check (page 154)	Assign, remove and manage alarms for system checks on machines.
LAN Watch (page 165)	Scan network range for specific SNMP enabled devices.
Assign SNMP (page 168)	Assign, remove and manage alarms of SNMP monitor sets on devices.
SNMP Log (page 175)	View SNMP log data in chart and table format.
Set SNMP Values (page 177)	Set SNMP values on the specified device.
SNMP Type (page 178)	Assign SNMP types to SNMP devices.
Parser Summary (page 179)	Define alerts for parser sets and copy parser set assignments to multiple machine IDs.
Log Parser (page 182)	Define log parsers and assign them to machine IDs.
Assign Parser Sets (page 187)	Create and assign parsers sets to machine IDs and create alerts on parser set assignments.

Alarms

The same alarm management concepts and guidelines apply to all methods of monitoring.

Alarm Conditions

An alarm condition exists when a machine's performance succeeds or fails to meet a pre-defined criteria.

Alarms

In graphical displays throughout the VSA, when an [alarm condition](#) (page 471) exists, the VSA displays, by default, a red traffic light  icon. If no alarm condition exists, a green traffic light icon  displays. These icons can be customized.

Alarms, and [other types of responses](#) (page 472), are enabled using the following pages:

- Monitor > [Alerts](#) (page 100)
- Monitor > [Assign Monitoring](#) (page 147)
- Monitor > [Assign SNMP](#) (page 168)
- Monitor > [System Checks](#) (page 154)
- Monitor > [Parser Summary](#) (page 179)
- Monitor > [Assign Parser Sets](#) (page 187)
- Patch Mgmt > [Patch Alerts](#) (page 250)
- Remote Cntl > Offsite Alerts
- Backup > Backup Alerts
- Security > Apply Alarm Sets
- Agent > [LAN Watch](#) (page 348)

Five Methods of Monitoring

Each of the five methods of monitoring in [Kaseya® Virtual System Administrator™](#) is either event-based or state-based.

- Event-based
 - [Alerts](#) - monitors events on *agent-installed* machines
 - [System Check](#) - monitors events on *non-agent-installed* machines
 - [Log Monitoring](#) - monitors events in *log files*
- State-based
 - [Monitor Sets](#) - monitors the performance state on *agent-installed* machines
 - [SNMP Sets](#) - monitors the performance state on *non-agent-installed devices*

Event-Based Alarms

[Alerts](#) (page 100), [System Check](#) (page 154) and [Log Monitoring](#) (page 182) represent [event-based alarms](#) that occur perhaps once. For example a backup may fail. There is no transition out of the condition, it just happens. Since there is no state, the red alarm in a dashlet never transitions back to green until you close the alarm in the alarm log. Typically event-based alarms are easier to configure, since the possibilities are reduced to whether one or more of the events happened or did not happen with a specified time period.

State-Based Alarms

[Monitor set](#) (page 140) counters, services, and processes and [SNMP set](#) (page 158) objects are either currently within their expected state range or outside of it and display as red or green alarm icons *dynamically*. These are known as [state-based alarms](#).

- *If an alarm state currently exists, monitor dashlets* (page 88) *show red alarms*.

- *If an alarm state does not currently exist, monitor dashlets show green alarms.*

For monitor sets and SNMP sets, the criteria for an alarm condition can be tailored using [Auto Learn](#) (page 152) and [Individualized](#) (page 147) sets. Alarms for monitor sets and SNMP sets can be *dismissed* using the [Network Status](#) (page 92) dashlet. 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.

Reviewing Created Alarms

All alarm 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 state* 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. Alarms can also be deleted from the alarm log. Note that a state-based alarm, like a monitor set or SNMP set, can trigger an alarm state that changes to red and then changes back to green. This same state-based alarm, if the [Create Alarm](#) checkbox is checked, can also generate an alarm *record* that remains `Open` until you close it.

Created alarms can be, reviewed, `Closed` or [Deleted...](#) using:

- Monitor > [Alarm Summary](#) (page 96)

Monitor > Dashboard List > any [Alarm Summary Window](#) (page 90) within a dashlet Created alarms can also be reviewed using:

- Monitor > Dashboard List > [Alarm Summary](#) (page 90) dashlet
- Monitor > Dashboard List > [Alarm Network Status](#) (page 90)
- Monitor > Dashboard List > [Alarm Rotator](#) (page 92)
- Monitor > Dashboard List > [Alarm Ticker](#) (page 92)
- Monitor > Dashboard List > [Group Alarm Status](#) (page 92)
- Monitor > Dashboard List > [Monitor Set Status](#) (page 93)
- Monitor > Dashboard List > [Monitor Status](#) (page 95)
- Monitor > Dashboard List > [Top N - Monitor Alarm Count](#) (page 95)
- Monitor > Dashboard List > [KES Status](#) (page 95)
- Monitor > Dashboard List > [KES Threats](#) (page 96)
- Reports > [Logs](#) (page 309) > Alarm Log
- Reports > [Monitor](#) (page 314) > Monitor Action Log

Reviewing Alarm Conditions without Creating Alarms

A user can assign monitor sets, SNMP sets, alerts, system checks or log monitoring to machine IDs *without checking the Create Alarm checkbox* and an [Monitor Action Log](#) entry will still be created.

These logs enable a user to review alarm conditions that have occurred without being specifically notified by the creation of an alarm, email or ticket. You can generate a report using Reports > [Monitor](#) (page 314) > Monitor Action Log.

Reviewing Performance with or without Creating Alarms

You can review monitor sets and SNMP set performance results, *with or without creating alarms*, using:

- Monitor > [Live Connect](#) (page 99)
- Monitor > [Monitor Log](#) (page 153)
- Monitor > [SNMP Log](#) (page 175)
- Monitor > Dashboard > [Network Status](#) (page 92)
- Monitor > Dashboard > [Group Alarm Status](#) (page 93)
- Monitor > Dashboard > [Monitoring Set Status](#) (page 93)
- Reports > [Monitor](#) (page 314) > Monitor Set Report

Reviewing Performance Data using Quick Sets

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 93), then clicking the [Quick Status](#) link or the Quick Status icon .

Reviewing Performance Data using Machine Status or Device Status

A [Machine Status](#) feature enables you to select any monitor set counter, service or process *for a single machine ID* and add it to the same single display window. Unlike the Quick Status window, a Machine Status view persists from one session to the next. SNMP sets display a similar window called the [Device Status](#) window for selected SNMP objects. The Machine Status window and Device Status window are accessed using Monitor > Dashboard > [Monitoring Set Status](#) (page 93), then clicking the machine/device status icon .

Suspending Alarms

The triggering of alarms can be suspended. The [Suspend Alarms](#) page suppresses [alarms](#) (page 470) 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

Alert, system check, and log monitoring alarms are automatically assigned to a [group alarm](#) category. If an alert alarm is triggered, 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 93) dashlet of the Monitor > [Dashboard List](#) page. You can create new groups using the Group Alarm Column Names tab in Monitor > [Monitor Lists](#) (page 138).

Dashboard List

[Home](#) > [Dashboard List](#)

[Monitor](#) > [Dashboard List](#)

- Similar information is provided using [Monitor](#) > [Alarm Summary](#) (page 96) and [Reports](#) > [Monitor](#) (page 314).

The [Dashboard List](#) page is the VSA's primary method of visually displaying monitoring data, including triggered alarm conditions. The [Dashboard List](#) page maintains configurable monitoring windows called [Dashboard Views](#). Each dashboard contains one or more panes of monitoring data called [Dashlets](#). Each administrator 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 Summary](#) (page 90)
 - [Alarm Network Status](#) (page 90)
 - [Alarm Rotator](#) (page 92)
 - [Alarm Ticker](#) (page 92)

- [Network Status](#) (page 92)
 - [Group Alarm Status](#) (page 93)
 - [Monitoring Set Status](#) (page 93)
 - [Monitor Status](#) (page 95)
 - [Machines Online](#) (page 95)
 - [Top N - Monitor Alarm Chart](#) (page 95)
 - [KES Status](#) (page 95)
 - [KES Threats](#) (page 96)
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 administrators, administrator roles or to make it public for all administrators 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.
- [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/group ID filter at the top of VSA web 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 dashboard you created are checked.

View

Displays the view icons available for each dashboard.

-  - Click to view this dashboard.

Monitor

-  - Click to configure this dashboard.
-  - Click to delete this dashboard.

Owner

The administrator who last modified the dashboard.

Note: You must take ownership of a dashboard before you can modify it.

Title

The name of the dashboard.

Description

The description of the dashboard.

Load on Startup

If checked, this dashboard displays when the administrator logs in. Choices apply only to the currently logged in administrator.

Alarm Summary

Dashboard List > Alarm Summary

The [Alarm Summary](#) dashlet displays all alarms for all machine IDs matching the dashlet's machine/group ID filter. The display lists the most recent alarms first. By default, alarms generated within the **last 24 hours** are **highlighted in red**. Alarms generated within the **last week** are **highlighted in yellow**. The color coding lets you quickly distinguish alarms you may not have examined yet. The color coding is customizable using [Settings](#) (page 96).

Each alarm contains a link to create or display a [Ticket](#) associated with the alarm.

Note: The Alarm Summary dashlet should be distinguished from the Alarm Summary Window (page 90) and Alarm Summary (page 96) page.

Alarm Network Status

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 90) of `Open` alarms for that machine.

Alarm Summary Window

Dashboard List > Alarm Network Status

Dashboard List > Group Alarm Status

Dashboard List > Monitor Set Status

The [Alarm Summary](#) window displays a filtered list of alarm log records. The filtering depending on how you accessed the window. An alarm listed in the alarm log does not represent the *current state* 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 96) 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.
- [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  buttons to display the previous and next page. The drop down list alphabetically lists the first record of each page of data.

Alarm ID

Lists a system-generated and unique ID for each alarm. The expand icon  can be clicked to display specific alarm information.

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385). Each dashlet displays all machine groups and machine IDs matching the *dashlet's* individual machine/group ID filter.

Monitor

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 197) 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 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 machine/group ID filter.

Alarm Ticker

[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 machine/group ID filter.

Network Status

[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* individual machine/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 90). Alarm log entries can remain `Open` indefinitely, long after the alarm state has returned to "no alarm".

Group Alarm Status

Dashboard List > Group Alarm Status

The **Group Alarm Status** dashlet summarizes the alarm status of all group IDs matching the dashlet's machine/group ID filter.

- Click the **Group ID** link to display the alarm status of all machine IDs and SNMP device IDs included in that group ID.
- Click the **Machine ID/SNMP Device ID** link to display a **Monitor Set Status** (page 93) window for the machine ID and any SNMP devices linked to it.
- Click any red icon  in the table to display the **Alarm Summary Window** (page 90) for that group or machine ID.
- **Alarm count for last <N periods>** - Alarm status is based on alarms activated within this time period.

Note: User defined group alarm column names are maintained using the Monitor Lists (page 138) page. Group alarm column names are assigned to monitor sets using Define Monitor Set (page 142).

Monitoring Set Status

Dashboard List > Monitoring Set Status

- You can also display a **Monitoring Set Status** dashlet using the **Group Alarm Status** dashlet of the **Dashboard List** page, by clicking a **group ID** link, then a **machine ID.group ID** link.

The **Monitoring Set Status** dashlet displays all alarms assigned to a machine ID, whether created by a **monitor set** (page 477), **alert** (page 471), **system check** (page 483), **SNMP set** (page 158), or **Log Monitoring** (page 476). Applies to all machine IDs matching the dashlet's machine/group ID filter.

Alarm count for last <N periods>

Alarm status is based on alarms activated within this time period.

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 473) icon - Click to display the **Machine Summary** (page 21) popup window.
- The machine status icon  - Click to display the **Machine Status** (page 95) 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 476).

Monitor

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 window provides a quick chart of the monitor set object you click. Clicking a *different* quick chart icon within the same monitor set adds that monitor set object to the [Quick Status Monitor](#) window. Quick chart selections are not permanently saved between sessions. Use the [Machine Status](#) (page 95) icon  to permanently save chart display selections.
- The monitoring log icon  - Click to display the [monitoring log](#) (page 153) for this single alarm counter in a popup window.
- The [Live Connect](#) (page 99) 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 90). 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 90). 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 90). 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 95) 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 [monitoring log](#) (page 153) 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 90). The [Alarm Summary Window](#) is restricted to just Open alarms for the selected SNMP set object and SNMP device.

Machine Status

Dashboard List > Monitor Set Status > Machine Status icon 

The [Machine Status](#) popup window selects and displays charts or tables for [monitor set](#) (page 477) 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 List > Monitor Set Status > Machine Status icon 

The [Device Status](#) popup window selects and displays charts or tables for [SNMP devices](#) (page 481). 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 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 machine/group ID filter. This dashlet can be customized using Monitor > [Settings](#) (page 96).

Machines Online

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 machine/group ID filter. This dashlet can be customized using Monitor > [Settings](#) (page 96).

Top N - Monitor Alarm Chart

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 machine/group ID filter. The chart shows up to 10 machines. This dashlet can be customized using Monitor > [Settings](#) (page 96).

KES Status

Dashboard List > KES Status

The [KES Status](#) dashlet displays different views of the security status of machine IDs using Kaseya Endpoint Security protection. Applies to all machine IDs matching the dashlet's machine/group ID filter. The three views of security status are:

Monitor

- [Machine Configuration](#)
- [Scan Details](#)
- [Profile Chart](#)

Note: This dashlet does not display unless the Kaseya Endpoint Security add-on module is enabled for the VSA.

KES Threats

[Dashboard List](#) > [KES Threats](#)

The [KES Threats](#) dashlet displays different views of the security threats reported for machine IDs using Kaseya Endpoint Security protection. Applies to all machine IDs matching the dashlet's machine/group ID filter. The three views of security threats are:

- [Most Recent](#)
- [Most Common](#)
- [Profile Chart](#)

Note: This dashlet does not display unless the Kaseya Endpoint Security add-on module is enabled for the VSA.

Settings

[Home](#) > [Settings](#)

[Monitor](#) > [Settings](#)

The [Settings](#) page enables you to customize controls for dashlets.

- Alarm sounds can be turned on for [Monitor Set Status](#) and [Alarm Summary](#).
- The [Chart Total Monitor Alarms](#) and [Chart Top N Monitor Alarms](#) background and title 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 alarm condition.
 - The additional percentage of machines online, below which represents a warning condition.
- [Custom Dashboard Skin](#) - Select the border and titlebar style you want dashlets to display.

Alarm Summary

[Monitor](#) > [Alarm Summary](#)

- Similar information is provided using [Monitor](#) > [Dashboard Lists](#) ([page 88](#)) and [Reports](#) > [Monitor](#) ([page 314](#)).

The [Alarm Summary](#) page displays [alarms](#) ([page 470](#)) for all machine IDs that match the current [machine ID / group ID filter](#) ([page 17](#)). 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.
- **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  buttons to display the previous and next page. The drop down list alphabetically lists the first record of each page of data.

Alarm ID

Lists a system-generated and unique ID for each alarm. The expand icon  can be clicked to display specific alarm information.

Machine.Group ID

The list of **Machine ID.Group IDs** (*page 476*) displayed is based on the **Machine ID / Group ID filter** (*page 17*) and the machine groups the administrator is authorized to see using **System > Group Access** (*page 385*). Each dashlet displays all machine groups and machine IDs matching the *dashlet's* individual machine/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.

Monitor

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 197) 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 Alarms

Monitor > Suspend Alarms

The [Suspend Alarms](#) page suppresses [alarms](#) (page 470) 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 17).

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 times to run this task each time period.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

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 for the scheduled task to recur.

Live Connect

Monitor > Live Connect

The [Live Connect](#) page displays live performance counter data for a selected machine ID. Only machines IDs assigned one or more monitor sets using [Assign Monitoring](#) (page 147) are listed on this page. The list of machine IDs you can select depends on the [Machine ID / Group ID filter](#) (page 17).

Each specific live connect 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled

Monitor

 The agent has been suspended

Machine ID.Group ID

Lists the [Machine.Group IDs](#) (page 476) currently matching the [Machine ID / Group ID filter](#) (page 17) 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 connect uses to gather data.

Select Counter

Lists the counters included in a selected monitor set. Click a counter link to display a live connect window for that counter.

Alerts

Monitor > Alerts

The [Alerts](#) page enables you to quickly define alerts for typical [alarm conditions](#) (page 471) found in an IT environment. For example, low disk space is frequently a problem on managed machines. Selecting the [Low Disk](#) type of alarm displays a single additional field that lets you define the % free space threshold. Once defined, you can apply this alarm immediately to any machine ID displayed on the [Alerts](#) page and specify the response to the alarm.

Note: [Monitor Sets](#) (page 477) represent a more complex method for monitoring alarm conditions. Typical alarm 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 101)
- [Agent Status](#) (page 103)
- [Application Changes](#) (page 106)
- [Get Files](#) (page 108)
- [Hardware Changes](#) (page 110)
- [Low Disk](#) (page 113)
- [Event Logs](#) (page 115)
- [LAN Watch](#) (page 121)
- [Script Failure](#) (page 124)
- [Protection Violation](#) (page 126)
- [New Agent Installed](#) (page 128)
- [Patch Alert](#) (page 130)
- [Backup Alert](#) (page 133)
- [System](#) (page 136)

Group Alarms

Alert, system check, and log monitoring alarms are automatically assigned to a [group alarm](#) category. If an alert alarm is triggered, 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 93) dashlet of the Monitor > [Dashboard List](#) page. You can create new groups using the Group Alarm Column Names tab in Monitor > [Monitor Lists](#) (page 138).

Machine Summary Alerts Tab

The [Machine Summary](#) page provides, in summary fashion, all the information available for a single machine. Typically you display this page by clicking the check-in status icon—for example, the  icon—next to any machine ID. One of the tabs provided is the [Alerts](#) tab. You can use this tab to quickly review, enable, or disable all the alerts applied to a single machine.

To Create An Alert

The same general procedure applies to all alert types.

1. Select an alert function from the [Select Alert Function](#) drop down list.
2. Check any of these checkboxes to perform their corresponding actions when a an alarm condition is encountered:
 - Create [Alarm](#)
 - Create [Ticket](#)
 - Run [Script](#)
 - [Email Recipients](#)
3. Set additional email parameters.
4. Set additional alert-specific parameters. These differ based on the alert function selected.
5. Check the paging rows to apply the alert to.
6. Click the [Apply](#) button.

To Cancel an Alert

1. Select one or more paging rows.
2. Click the [Clear](#) button.

The alert information listed next to the paging row is removed.

Alerts - Summary

[Monitor](#) > [Alerts](#) (page 100)

- [Select summary from the Select Alert Function drop-down list](#)

The [Alerts - Summary](#) 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](#) 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 or scripts using this page, script assignments are displayed in the paging area.

Apply

Click [Apply](#) to apply alert parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Monitor

Clear

Click [Clear](#) to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in this field. It defaults from System > [Preferences](#) (page 377).
- 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 to selected machine IDs 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 to machine IDs.
- If [Removed](#) is clicked, all email addresses are removed from selected machine IDs **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Alert Type

Lists all alert types you can assign to a machine ID using the [Monitor > Alerts](#) (page 100) page. Displays any script assignments assigned to this machine ID.

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- 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 > Alerts](#) (page 100)

- [Select Agent Status from the Select Alert Function drop-down list](#)

The [Alerts - Agent Status](#) page triggers an alert if an agent is offline, first goes online, or someone has disabled remote control on the selected machine.

Note: When ever the KServer service stops, the system suspends all agent online/offline alerts. If the KServer stops for more than 30 seconds, then agent online/offline alerts are suspended for one hour after the KServer starts up again. Rather than continuously try to connect to the KServer when the KServer 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 KServer starts back up.

Passing Alert Information to Emails and Scripts

The following types of monitoring alert emails can be sent and formatted:

- Alert when single agent goes off-line
- Alert when multiple agents in the same group go off-line
- Alert when agent first goes online
- Alert when users disable remote control

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) from the database. For example, to include the computer name of the machine generating the alert in an email, use

Monitor

		<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#	last check-in time
	#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 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (*page 476*) displayed is based on the [Machine ID / Group ID filter](#) (*page 17*) and the machine groups the administrator is authorized to see using [System > Group Access](#) (*page 385*).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (*page 481*):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Email Address

A comma separated list of email addresses where notifications are sent.

Time Offline

Displays the number of days if an alert is sent when a machine ID is off-line for the specified number of days.

Monitor

Agent Goes Online

Displays a checkmark  if an alert is sent when an agent does online.

RC Disabled

Displays a checkmark  if an alert is sent when the user disables remote control.

Alerts - Application Changes

Monitor > [Alerts](#) (page 100)

- [Select Application Changes from the Select Alert Function drop-down list.](#)
- [Similar information is provided using Audit > Add/Remove \(page 37\) and Reports > Software \(page 303\).](#)

The [Application Changes](#) page triggers an alert when a new application is installed or removed on selected machines. This alert is based on the [latest audit](#) (page 472).

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.

Passing Alert Information to Emails and Scripts

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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
	#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 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script after alert

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

Alert when audit detects New application installed

If checked, an alert is triggered when a new application is installed.

Alert when audit detects Existing application deleted

If checked, an alert is triggered 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:

 Agent has checked in

Monitor

-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email 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](#) > [Alerts](#) (page 100)

- [Select Get Files](#) from the [Select Alert Function](#) drop-down list

The [Alerts - Get File](#) page triggers an alert when a script's [Get File](#) or [Get File in Directory Path](#) command executes, uploads the file, and the file is now different from the copy previously stored on the server. If there was not a previous copy on the server, the alert is also triggered.

Note: The VSA issues the alert only if the send alert if file changed option has been selected in the script.

Passing Alert Information to Emails and Scripts

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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#	script name the 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 alert 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script after alert

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.

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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Hardware Changes

[Monitor](#) > [Alerts](#) (page 100)

- [Select Hardware Changes from the Select Alert Function drop-down list](#)

The [Alerts - Hardware Changes](#) page triggers an alert 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 472).

Passing Alert Information to Emails and Scripts

The following type of monitoring alert emails can be sent and formatted:

- Alert when disk or PCI card is added or removed
- 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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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
<m>	#m#	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 alert 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script to run on a specified range of machine IDs

Monitor

by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Low Disk

Monitor > Alerts (page 100)

- Select **Low Disk** from the **Select Alert Function** drop-down list

The **Low Disk** page triggers an alert 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 472).

Passing Alert Information to Emails and Scripts

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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 alert 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** (page 88), Monitor > **Alarm Summary** (page 96) and Reports > **Logs** (page 309) > Alarm Log.

Monitor

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:



Agent has checked in



Agent has checked in and user is logged on. Tool tip lists the logon name.



Agent has not recently checked in



Agent has never checked in



Online but waiting for first audit to complete



The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Event Logs

[Monitor](#) > [Alerts](#) (page 100)

- [Select Event Logs from the Select Alert Function drop-down list](#)

The [Alerts - Event Logs](#) page triggers an alert when an event log entry for a selected machine matches a specified criteria. After selecting the [event log type](#), you can filter the alerts triggered by [event set](#) and by [event category](#).

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.

Prerequisite

Event logging must be enabled for a particular machine using [Agent > Event Log Settings](#) (page 329).

Windows 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 KServer database, serve as the basis of alerts and reports, and be archived.

Depending on the operating system, the [event logs types](#) available include but are not limited to:

- Application log
- Security log
- System log
- Directory service log
- File Replication service log
- DNS server log

The list of event types available to select can be updated using [Monitoring > Update Lists by Scan](#) (page 140).

Windows events are further classified by the following [event log categories](#):

- Error
- Warning
- Information
- Success Audit

Monitor

- Failure Audit
- Critical - Applies only to Vista.
- Verbose - Applies only to Vista.

Event logs are used or referenced by the following VSA pages:

- Monitor > [Agent Logs](#) (page 327)
- Monitor > Alerts > [Event Logs](#) (page 115)
- Monitor > Alerts > [Edit Event Sets](#) (page 120)
- Monitor > [Update Lists by Scan](#) (page 140)
- Agent > [Log History](#) (page 328)
- Agent > [Event Log Settings](#) (page 329)
- Agent > [Agent Logs](#) (page 327)
- Reports > [Logs](#) (page 476)

System > Database Views > [vNtEventLog](#) (page 431)

Event Sets

Because the number of events in Windows based events logs is enormous the VSA uses a record type called an [event set](#) to filter the triggering of alerts.

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 474) 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 triggers an alert on any machine that event set is applied to.

For details on how to configure event sets, see Monitor > Alerts > Event Logs > [Edit Event Sets](#) (page 120).

Sample Event Sets

The VSA provides a growing list of sample event sets. The names of sample event sets begin with ZC. They can be updated using System > [Configure](#) (page 394). 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. An Excel document called `Standard Monitoring Library.xls` provides a description of each sample event set. It can be downloaded from the Kaseya Support Forum.

Creating an Event Log Alert

1. On the Monitor > [Alerts](#) page select the [event log type](#) using the drop-down list.
2. Select the [Event Set](#) (page 120) filter used to filter the events that trigger alerts. By default `<All Events>` is selected.
3. Check the box next to any of the following [event category](#):
 - Error
 - Warning
 - Information
 - Success Audit
 - Failure Audit
 - Critical - Applies only to Vista.
 - Verbose - Applies only to Vista.

Note: Red letters indicate logging disabled. Event logs may be disabled by the VSA for a particular machine, based on settings defined using Agent > Event Log Settings (page 329). A particular event category may be not be available for certain machines, such as the Critical and Verbose event categories for non-Vista machines.

4. Specify the *frequency* of the alarm 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.

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 475)—are uploaded to the KServer 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 log to record that collection has been suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your KServer. Alarm detection and processing operates regardless of whether collection is suspended.

Passing Alert Information to Emails and Scripts

The following types of monitoring alert emails can be sent and formatted:

- Single event log alert. Same template applied to all event log types.
- Multiple event log alerts. Same template applied to all event log types.
- 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 alert emails.

The following variables can be included in your formatted email alerts and in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<cg>	#cg#	Event category
<cn>	#cn#	computer name
<db-view.column>	not available	Include a view.column (page 415) 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
<esn>	#esn#	event source name
<et>	#et#	event time

Monitor

<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

Note: Only the following variables can be included in multiple event log alerts: <at> <ed> <ev> <gr> <id> <lt>.

Apply

Click [Apply](#) to apply alert 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).

- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

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 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- 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.

Monitor

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>](#).

Edit Event Sets

Monitor > [Alerts](#) (page 100)

- On the [Alerts](#) page, select `Event Logs` from the [Select Alert Function](#) drop down list.
- 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 474) 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 triggers an alert on 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. On the [Alerts](#) page, select [Events Logs](#) from the [Select Alert Function](#) drop down list.
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 an event set data as text.
 - Importing event set data from a file.
1. If you enter a new name and click [New](#), the [Edit Event Set](#) window displays the five properties used to filter events.

2. Click [Add](#) to add a new event to the event set.
3. Click [Ignore](#) to specify an event that should *not* trigger an alarm.
4. 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. On the [Alerts](#) page, select [Event Logs](#) from the [Select Alert Function](#) drop down list.
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>
```

Alerts - LAN Watch

[Monitor](#) > [Alerts](#) (page 100)

- [Select LAN Watch](#) from the [Select Alert Function](#) drop-down list

The [Alerts - LAN Watch](#) page works in conjunction with the [LAN Watch](#) (page 165) page. [LAN Watch](#) scans a machine ID's local LAN and detects new machines and devices connected to the machine's LAN. Both [LAN Watch](#) and the [Alerts - LAN Watch](#) page can subsequently trigger an alarm, email recipients and run a script when a new machine or device is discovered on a LAN. Only the [Alerts - LAN Watch](#)

Monitor

page can create a ticket when a new machine or device is discovered on a LAN.

Passing Alert Information to Emails and Scripts

The following type of monitoring alert emails can be sent and formatted:

- Alert when new device discovered by LAN Watch

Note: Changing this email alarm format changes the format for all LAN Watch alert emails.

The following variables can be included in your formatted email alerts and in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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
<nd>	#nd#	new device data
	#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 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Email Address

- A comma separated list of email addresses where notifications are sent.

Alerts - Script Failure

Monitor > Alerts (page 100)

Select `Script Failure` from the `Select Alert Function` drop-down list. The `Script Failure` page triggers an alert when a script fails to execute on a managed machine.

Passing Alert Information to Emails and Scripts

The following type of alert emails can be sent and formatted:

- Format email message generated by Script Exec Failure alerts

Note: Changing this email alarm format changes the format for all `Script Failure` alert emails.

The following variables can be included in your formatted email alerts and in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a <code>view.column</code> (page 415) from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
	#em#	script error message
<en>	#en#	script name the 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 alert 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Monitor

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - Protection Violation

Monitor > Alerts (page 100)

- Select Protection Violation from the Select Alert Function drop-down list

The Alerts - Protection Violation page triggers an alert 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

- Scripts > Distribute File (page 60)
- Audit > File Access (page 47)
- Audit > Network Access (page 48)

Passing Alert Information to Emails and Scripts

- The following type of alert emails can be sent and formatted:
- Alert when Protection Violation detected

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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 alert 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

Distributed file changed on agent and was updated

If checked, an alert is triggered when a file distributed using Script > [Distributed File](#) (page 60) is changed on the managed machine. The agent verifies the distributed file at every [full check-in](#) (page 473).

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 47).

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 48).

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:

 Agent has checked in

Monitor

-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Email Address

A comma separated list of email addresses where notifications are sent.

Alerts - New Agent Installed

[Monitor](#) > [Alerts](#) (page 100)

- [Select New Agent Installed from the Select Alert Function drop-down list](#)

The [New Agent Installed](#) page triggers an alert when a new agent is installed on a managed machine in selected *groups*.

Passing Alert Information to Emails and Scripts

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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 alert 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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

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 Mgmt > Patch Alert

Monitor > Alerts (page 100)

Select `Patch Alert` from the [Select Alert Function](#) drop-down list. The [Patch Alert](#) page creates 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.

Passing Alert Information to Emails and Scripts

The following types of monitoring alert emails can be sent and formatted:

- New Patch Available
- Path to Patch Executable Missing - Enabled by selecting the *first* row in the paging area, called [Patch Location Missing](#), and clicking the [Apply](#) button.
- Patch Install Failed
- Patch Approval Policies Updated - Enabled by selecting the *second* row in the paging area, called [Patch Location Missing](#), and clicking the [Apply](#) button.
- Agent Credential Invalid
- Windows Auto Update Configuration Changed

To Create a Patch Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm 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 Scripts

The following types of patch alert emails can be sent and formatted:

- New Patch Available
- Path to Patch Executable Missing

- Patch Install Failed
- Patch Approval Policies Updated
- Agent Credential Invalid
- 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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<au>	#au#	auto update change
<bi>	#bi#	bulletin ID
<bl>	#bl#	new bulletin list
<db-view.column>	not available	Include a view.column (page 415) 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.

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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

Apply

Click [Apply](#) to apply alert 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 triggers an alarm whenever the system discovers one of three different patch alert conditions for a selected machine ID:

- [New patch is available](#)
- [Patch install fails](#)
- [Agent credential is invalid or missing](#)
- [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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Patch Location Missing

Displays as the first row of data. If selected and the [Apply](#) button clicked, an alert is generated if the system discovers the [Patch Location](#) (page 258) path for a patch is missing. This is a system alert and not associated with any machines.

Approval Policy Updated

Displays as the second row of data. If selected and the [Apply](#) button clicked, an alert is generated when a new patch is added to all patch policies. See [Patch Approval Policy](#) (page 478). This is a system alert and not associated with any machines.

ATSE

The ATSE response code assigned to machine IDs:

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- 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 Mgmt > [Windows Auto Update](#) (page 243).

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](#) > [Alerts](#) (page 100)

Select [Backup Alert](#) from the [Select Alert Function](#) drop-down list The [Backup Alert](#) page creates alerts for backup events on managed machines. The list of machine IDs you can select depends on the [Machine ID / Group ID filter](#) (page 17). 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 a an alarm condition is encountered:
 - [Create Alarm](#)
 - [Create Ticket](#)
 - [Run Script](#)
 - [Email Recipients](#)
2. Set additional email parameters.
3. Set additional backup alert specific parameters.

Monitor

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 Scripts

The following types of backup alert emails can be sent and formatted:

- Backup failed
- Verify backup failed
- Recurring backup skipped if machine offline
- Backup Completed Successfully
- Full Backup Completed Successfully
- Image Location free space below

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 in scripts.

Within an Email	Within a Script	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 415) 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

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the **Email Recipients** field. It defaults from System > **Preferences** (page 377).
- 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 alarm condition is encountered.
- 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 **Removed** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the **From Address** using System > **Configure** (page 394).

Apply

Click **Apply** to apply alert 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 backup process completes successfully.
- **Full Backup Completed** - Alerts when a full backup process completes successfully.
- **Backup Fails** - Alerts when a backup process 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.
- **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 administrator.

Monitor

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email 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](#) > [Alerts](#) (page 100)

- [Select system](#) from the [Select Alert Function](#) drop-down list

The [Alerts - System](#) page triggers an alert when selected events occur on the *KServer*. Selecting the [Alerts - System](#) page does not display a managed machine list. The events listed only apply to the *KServer*. This option only displays for [master administrators](#) (page 469).

Passing Alert Information to Emails and Scripts

The following types of monitoring alert emails can be sent and formatted:

- Administrator account disabled manually by a master administrator
- Administrator account disabled because logon failed count exceeded threshold
- KServer has stopped
- Database backup failed
- Email reader failed

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 in scripts.

Within an Email	Within a Script	Description
<an>	#an#	disabled admin name
<at>	#at#	alert time
<bf>	#bf#	database backup error data
<db-view.column>	not available	Include a view.column (page 415) 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
<gr>	#gr#	group ID
<id>	#id#	machine ID
<kn>	#kn#	kserver IP/name
<ms>	#ms#	disabled admin 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.

Clear

Click [Clear](#) to remove all alert parameters from the system.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.

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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

Admin account disabled

If checked, an alert is triggered when an administrator account is disabled, whether manually or automatically.

KServer stopped

If checked, an alert is triggered when the KServer stops.

System database backup failed

If checked, an alert is triggered when the Kserver's database backup fails

Email reader in ticketing failed

If checked, an alert is triggered if the Ticketing > [Email Reader](#) (page 208) fails.

System alerts sent to

Displays the email recipients who are sent system alerts.

Monitor Lists

Monitor > Monitor Lists

The [Monitor Lists](#) page maintains the complete list of all objects, services and processes loaded on the KServer that are used to create [Monitor Sets](#) (page 140) and [SNMP Sets](#) (page 158). The [Monitor List](#) page also maintains user-defined group alarms.

Note: The Counter Objects, Counters, Instances and Services lists can be initially populated by using the [Update Lists by Scan](#) (page 140) page. Additionally these lists, as well as Services and Processes, can be populated with the import of a [Monitor Set](#) (page 140). MIB OIDs can be populated by using the [Add SNMP Object](#) (page 163) page or by the import of a [SNMP Set](#) (page 158).

Counter Objects

This tab lists [counter objects](#) required to create a [Monitor Set](#) (page 140). Monitor Set uses the [PerfMon](#) combination of object/counter/instance 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](#) required to create a [Monitor Set](#) (page 140). Monitor Set uses the [PerfMon](#) combination of object/counter/instance to collect counter information.

Instances

This tab lists [counter instances](#) required to create a [Monitor Set](#) (page 140). 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](#) required by the edit [Monitor Set](#) (page 140) feature to monitor the activity of Windows Services. This list can also be populated with the execution of the [Update Lists By Scan](#) (page 140) page or the import of a [Monitor Set](#) (page 140).

Processes

This tab lists Windows [processes](#) required by the edit [Monitor Set](#) (page 140) feature when monitoring for 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 the [Update Lists by Scan](#) (page 140) feature.

MIB OIDs

This tab lists SNMP [MIB objects](#) required to create [SNMP Sets](#) (page 158). SNMP sets monitor the activity of SNMP devices. This list can be populated with the import of a [SNMP Set](#) (page 158) or the execution of the [Add SNMP Object](#) (page 163) 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 [SNMP Types](#) (page 178). 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 159). During a [LAN Watch](#) (page 165) 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 column names do not display here. Use [Monitor Sets](#) (page 140) and [Define Monitor Sets](#) (page 142) to assign a monitor set to any group alarm column name. Group alarms are displayed using the [Dashboard List](#) (page 88) 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.

Delete Icon

Click the delete icon  to delete a list item.

Monitor

Edit Icon

Click the edit icon  to edit the text of a list item.

Update Lists By Scan

Monitor > Update Lists By Scan

The [Update Lists by Scan](#) page scans one or more machine IDs and returns lists of counter categories, counters, instances and services to select from when creating or editing a monitor set. Also updates the list of event types available for monitoring using [Monitoring > Alerts](#) (page 100). Typically only a handful of machines of each operating system type need to be scanned to provide a set of comprehensive lists.

Scan

Click [Scan](#) to scan selected machine IDs and gather available categories of counter objects, counters, instances and services.

Cancel

Cancels a scan that is pending.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Status

Indicates a pending scan or when a scan was last completed.

Monitor Sets

Monitor > Monitor Sets

The [Monitor Sets](#) page adds, imports or modifies monitor sets. Sample monitor sets can be loaded using the [System > Configure](#) (page 394) page.

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, 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 by source machine ID using Monitor > [Update Lists by Scan](#) (page 140).
2. Optionally update monitor set counter objects, instances and counters manually and review them using [Monitor Lists](#) (page 138).
3. Optionally update predefined *sample* monitor sets using System > [Configure](#) (page 394).
4. Create and maintain monitor sets using Monitor > [Monitor Sets](#) (page 140).
5. Assign monitor sets to machine IDs using Monitor > [Assign Monitoring](#) (page 147).
6. Optionally customize standard monitor sets as *individualized monitor sets*.
7. Optionally customize standard monitor sets using *Auto Learn*.
8. Review monitor set results using:
 - Monitor > [Live Connect](#) (page 99)
 - Monitor > [Monitor Log](#) (page 153)
 - Monitor > Dashboard > [Network Status](#) (page 92)
 - Monitor > Dashboard > [Group Alarm Status](#) (page 93)
 - Monitor > Dashboard > [Monitoring Set Status](#) (page 93)
 - Reports > [Monitor](#) (page 314) > Monitor Set Report
 - Reports > [Monitor](#) (page 314) > Monitor Action Log

Note: Not all monitor sets may be available for editing on the Monitor Set page, since the creator of a monitor set may only have shared the use of the monitor set but not the editing of the set.

Sample Monitor Sets

The VSA provides a growing list of sample monitor sets. The names of sample monitor sets begin with ZC. They can be updated using System > [Configure](#) (page 394). 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. An Excel document called `Standard Monitoring Library.xls` provides a description of each sample monitor set. It can be downloaded from the Kaseya Support Forum.

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.

Add

Click [Add](#) to open a form that asks the user to:

1. [Monitor Set Name](#) - Name the new monitor set.
2. [Monitor Set Description](#) - Optionally describe the new monitor set.
3. [Group Alarm Column](#) - Select a group alarm column. User defined group alarm column names are maintained using the [Monitor Lists](#) (page 138) page. Group alarms display on the [Dashboard List](#) (page 88) page.

Monitor

Import

Click [Import](#) to upload a monitor set XML file to your server. Monitor sets can be exported using [Define Monitor Set](#) (page 142).

Edit

Click [Edit](#) to display the [Define Monitor Set](#) (page 142) window and edit a monitor set.

Define Monitor Sets

[Monitor](#) > [Monitor Sets](#) > [Edit](#)

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 138). Sample monitor sets can be loaded using the [System > Configure](#) (page 394) page.

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, 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 by source machine ID using [Monitor > Update Lists by Scan](#) (page 140).
2. Optionally update monitor set counter objects, instances and counters manually and review them using [Monitor Lists](#) (page 138).
3. Optionally update predefined *sample* monitor sets using [System > Configure](#) (page 394).
4. Create and maintain monitor sets using [Monitor > Monitor Sets](#) (page 140).
5. Assign monitor sets to machine IDs using [Monitor > Assign Monitoring](#) (page 147).
6. Optionally customize standard monitor sets as *individualized monitor sets*.
7. Optionally customize standard monitor sets using *Auto Learn*.
8. Review monitor set results using:
 - [Monitor > Live Connect](#) (page 99)
 - [Monitor > Monitor Log](#) (page 153)
 - [Monitor > Dashboard > Network Status](#) (page 92)
 - [Monitor > Dashboard > Group Alarm Status](#) (page 93)
 - [Monitor > Dashboard > Monitoring Set Status](#) (page 93)
 - [Reports > Monitor](#) (page 314) > Monitor Set Report
 - [Reports > Monitor](#) (page 314) > Monitor Action Log

Click the following tabs to define monitor set details.

- [Counter Thresholds](#) (page 143)
- [Services Check](#) (page 145)
- [Process Status](#) (page 146)
- [Monitor Icons](#) (page 147)

Take Ownership...

You can't edit a public monitor set you don't own. Click the [Take Ownership](#) link to display the [Save](#) and [Delete](#) buttons. Otherwise you can make a copy of the current monitor set using the [Save As...](#) button.

Share...

You can share monitor sets you own with other individual administrators, entire administrator groups, or make the monitor set public for all administrators.

Note: A master administrator can take ownership of a monitor set and change share rights.

Save As...

Select [Save As...](#) to save a monitor set under a different name.

Save

Select [Save](#) to save changes to a monitor set.

Delete

Select [Delete](#) to delete a monitor set.

Export Monitor Set...

Click the [Export Monitor Set...](#) link to display the script in XML format in the [Export Monitor Sets](#) popup window. You can copy it to the clipboard or download it to a text file. Monitor sets can be *imported* using the [Monitor Sets](#) (page 140) page.

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 it belongs to is triggered as well. Group alarms display in the [Group Alarm Status](#) (page 93) pane of the Monitor > [Dashboard List](#) page.

Counter Thresholds

Monitor > Monitor Sets > Edit > Counter Thresholds

The [Counter Thresholds](#) tab defines alarm 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.

Performance Objects, Instances and Counters

When setting up counter thresholds in monitor sets, 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.

Monitor

- **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.

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 138) 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**. You can also update the "master list" of all objects, instances and counters by scanning specific machine IDs using **Update Lists By Scan** (page 140). Once the update is completed, the drop lists should be populated with the options you require.
 - When multiple instances exist, you often have the option of using 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*. The `_Total` can be used as a kind of "wildcard instance". Without the `_Total` instance you would have to specify each instance by its exact name, which makes applying the same monitor set to multiple machines difficult. The true benefit of the `_Total` instance is determining if there *are any performance issues for any instance of this object at all*. Once you know that you can investigate the specific cause.
 - When multiple instances exist, you sometimes have the option of using an instance called `*ALL`. 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**.
3. Select the log data collected. If the returned value is numeric, you can minimize unwanted log data by setting a narrow range of data values over and 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 KServer.
4. Specify when an alarm 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` 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.

- **Duration** - Specify the time the returned values must continuously exceed the alarm threshold to generate the alarm. Many alarm conditions are only alarming if the level is sustained over a long period of time.
 - **Ignore additional alarms for** - Suppress additional alarms for this same issue for this time period. This reduces the confusion of many alarms for the same issue.
5. **Warn when within X% of alarm threshold** - Optionally display a warning alarm when the returned value is within a specified percentage of the **Alarm Threshold**. The default warning icon is a yellow traffic light icon . See [Monitor Icons](#) (page 147).
 6. Optionally activate a **trending alarm**. Trending alarms use historical data to predict when the next alarm 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 alarm is generated. Typically a trending window should be set to the amount of time you need to prepare for an alarm condition, if it occurs. Example: an administrator may want 10 days notice before a hard drive reaches the alarm condition, to accommodate ordering, shipping and installing a larger hard drive.
 - **Ignore additional trending alarms for** - Suppress additional trending alarms for this same issue for this time period.
 - By default, trending alarms display as an orange icon . You can change this icon using the [Monitor Icons](#) (page 147) tab.

Warning status alarms and trending status alarms don't create alarms 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](#) (page 314).

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 Thresholds](#) list.

Save

Save changes made to the wizard pages.

Services Check

[Monitor](#) > [Monitor Sets](#) > [Edit](#) > [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.

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.

Add / Edit

Click [Add](#) or the edit icon  to maintain a [Services Check](#) record.

Monitor

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 138) page. If a service does not display in the drop down list, you can add it manually using [Add Service](#). You can also update the "master list" by scanning specific machine IDs using [Update Lists By Scan](#) (page 140).
 - Select the *ALL selection to monitor all services on a monitored machine.
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 alarms for the specified time period.

Delete

Click the delete icon  to delete a [Services Check](#) record.

Save

Save changes to a [Services Check](#) record.

Cancel

Ignore changes to a [Services Check](#) record and return to the [Services Check](#) list.

Process Status

[Monitor](#) > [Monitor Sets](#) > [Edit](#) > [Process Status](#)

The [Process Status](#) tab defines alarm conditions based on whether a process has started or stopped on a machine ID.

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.

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 138) page. If a process does not display in the drop-down list, you can add it manually using [Add Process](#). You can also update the "master list" by scanning specific machine IDs using [Update Lists By Scan](#) (page 140).
2. **Description** - Describes the process and the reason for monitoring.
3. **Alarm on Transition** - Triggers an alarm when a process (application) is started or stopped.
4. **Ignore additional alarms for** - Suppresses additional alarms for the specified time period.

Delete

Click the delete icon  to delete a [Process Status](#) record.

Save

Save changes to a [Process Status](#) record.

Cancel

Ignore changes to a [Process Status](#) record and return to the [Process Status](#) list.

Monitor Icons

[Monitor](#) > [Monitor Sets](#) > [Edit](#) > [Monitor Icons](#)

The [Monitor Icons](#) tab selects the monitor icons that display in the [Monitor Log](#) (*page 153*) 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

Save changes made to the [Monitor Icons](#) 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.

Assign Monitoring

[Monitor](#) > [Assign Monitoring](#)

The [Assign Monitoring](#) page creates monitor set alerts for managed machines. An alert is a response to an alarm condition. An alarm 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, 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 by source machine ID using [Monitor](#) > [Update Lists by Scan](#) (*page 140*).
2. Optionally update monitor set counter objects, instances and counters manually and review them using [Monitor Lists](#) (*page 138*).
3. Optionally update predefined *sample* monitor sets using [System](#) > [Configure](#) (*page 394*).
4. Create and maintain monitor sets using [Monitor](#) > [Monitor Sets](#) (*page 140*).
5. Assign monitor sets to machine IDs using [Monitor](#) > [Assign Monitoring](#) (*page 147*).
6. Optionally customize standard monitor sets as *individualized monitor sets*.
7. Optionally customize standard monitor sets using *Auto Learn*.
8. Review monitor set results using:
 - [Monitor](#) > [Live Connect](#) (*page 99*)
 - [Monitor](#) > [Monitor Log](#) (*page 153*)

Monitor

- Monitor > Dashboard > [Network Status](#) (page 92)
- Monitor > Dashboard > [Group Alarm Status](#) (page 93)
- Monitor > Dashboard > [Monitoring Set Status](#) (page 93)
- Reports > [Monitor](#) (page 314) > Monitor Set Report
- Reports > [Monitor](#) (page 314) > 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 140). An *individualized monitor set adds an (IND) prefix to the name of the monitor set.*
4. Make changes to your new individualized monitor set. These changes apply only to the single machine it is assigned to.

Note: Changes to a standard monitor set have no affect 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 152) 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.

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 a an alarm 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 Scripts

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 in scripts.

Within an Email	Within a Script	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 415) 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

Monitor

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script to run on a specified range of machine IDs by clicking the [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that triggered the alarm.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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 140).

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.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (*page 476*) displayed is based on the [Machine ID / Group ID filter](#) (*page 17*) and the machine groups the administrator is authorized to see using [System > Group Access](#) (*page 385*).

Monitor Sets

Displays the list 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 152*) 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 140*) 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 481*):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Email Address

A comma separated list of email addresses where notifications are sent.

Auto Learn - Monitor Sets

Monitor > 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

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

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.

Monitor Log

Monitor > Monitor Log

- Clicking the monitoring log icon  next to a single alarm for a specific machine ID in the [Monitoring Set Status \(page 93\)](#) dashlet of the [Dashboard List](#) page displays this same information as a popup window.

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 is limited to machine IDs currently matching the [machine ID / group ID filter \(page 17\)](#). If no machine IDs display use [Monitor > Assign Monitoring \(page 147\)](#) 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:

- 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.
- If there are no values returned, check [Counter Thresholds \(page 143\)](#) 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:

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 140) 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.
- **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 temporary folder are set to full access for `SYSTEM` and `NETWORK SERVICE`. This can happen if the agent temp folder is placed in the `c:\program files\` or `c:\windows` directories. This is not recommended as these folders 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.

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 500 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 159) for more information.

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 > 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.

To Create a System Check Alert

1. Check any of these checkboxes to perform their corresponding actions when a an alarm 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 Scripts

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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 alert 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.

Monitor

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script to run on a specified range of machine IDs by clicking the [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that triggered the alarm.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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.
- **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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

ATSE

The ATSE response code assigned to machine IDs or [SNMP devices](#) (page 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Monitor

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 the triggering of additional system check alarms are suppressed, after the initial problem is *reported*. This prevents reporting multiple alarms for the same problem.

SNMP Sets

Monitor > 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 481). 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 an device-specific SNMP set based on the objects discovered on that device during a LAN Watch. **SNMP quick sets** (page 481) 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 482) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Monitor > **LAN Watch** (page 165).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 168). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 175) or **Dashboard List** (page 88).

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 138).

- Optionally maintain SNMP sets using Monitor > [SNMP Sets](#) (page 158).
- Optionally add an SNMP object using Monitor > [Add SNMP Object](#) (page 163).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > [SNMP Type](#) (page 178).
- Optionally write values to SNMP devices using Monitor > [Set SNMP Values](#) (page 177).

Note: Not all SNMP Sets may be available for editing, since the creator of a SNMP Set may only have shared the use of the set but not the display or editing of the set.

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.

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.

Add

Click [Add](#) to open a form that asks the user to:

1. [Monitor Set Name](#) - Name the new SNMP set.
2. [Monitor Set Description](#) - Optionally describe the new SNMP set.
3. [Automatic deployment to](#) - Select a category of SNMP devices. If a LAN Watch detects this type of SNMP device the system automatically begins monitoring the SNMP device using this SNMP set.
4. [Group Alarm Column](#) - Select a group alarm column. User defined group alarm column names are maintained using the [Monitor Lists](#) (page 138) page. Group alarms display on the [Dashboard List](#) (page 88) page.

Import

Click [Import](#) to upload a SNMP set XML file to your server. SNMP sets can be exported using [Define SNMP Sets](#) (page 159).

Edit

Click [Edit](#) to display [Define SNMP Set](#) (page 159) and edit a monitor set.

Define SNMP Set

[Monitor](#) > [SNMP Sets](#) > [Define SNMP Set](#) > [Edit](#)

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 481). 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 an device-specific SNMP set based on the objects discovered on that device during a LAN Watch. [SNMP quick sets](#) (page 481) 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.

Monitor

- [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 482) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Monitor > [LAN Watch](#) (page 165).
2. Assign SNMP sets to discovered devices using Monitor > [Assign SNMP](#) (page 168). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > [SNMP Log](#) (page 175) or [Dashboard List](#) (page 88).

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 138).
- Optionally maintain SNMP sets using Monitor > [SNMP Sets](#) (page 158).
- Optionally add an SNMP object using Monitor > [Add SNMP Object](#) (page 163).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > [SNMP Type](#) (page 178).
- Optionally write values to SNMP devices using Monitor > [Set SNMP Values](#) (page 177).

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.

Note: Sample SNMP sets can be loaded from the System > Configure (page 394) page.

Click the following tabs to define SNMP set details.

- [SNMP Sets](#) (page 161)
- [SNMP Icons](#) (page 164)

Take Ownership...

You can't edit a public SNMP set you don't own. Click the [Take Ownership](#) link to display the [Save](#) and [Delete](#) buttons. Otherwise you can make a copy of the current SNMP set using the [Save As...](#) button.

Share...

You can share SNMP sets you own with other individual administrators, entire administrator groups, or make the SNMP set public to all administrators.

Note: A master administrator can take ownership of a SNMP set and change share rights.

Save As...

Select [Save As...](#) to save a SNMP set under a different name.

Save

Select [Save](#) to save changes to a SNMP set.

Delete

Select [Delete](#) to delete a SNMP set.

Export SNMP Set...

Click the [Export SNMP Set...](#) link to display the script 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 \(page 158\)](#) page.

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 [SNMP type \(page 178\)](#) when performing a [LAN Watch \(page 165\)](#) 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 \(page 88\)](#) page.

Define SNMP Set Details

Monitor > Define SNMP Set > Edit > 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.

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 \(page 481\)](#). Click [Add Object \(page 163\)](#) to add a MIB object that currently does not exist on the [Monitor Lists \(page 138\)](#) 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. You can also enter ALL. An ALL instance represents all the instances available for an object.

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 168). 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 narrow range of data values over and 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 alarm 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 alarm 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 alarm. Many alarm conditions are only alarming if the level is sustained over a long period of time.
 - **Ignore additional alarms for** - Suppress additional alarms for this same issue for this time period. This reduces the confusion of many alarms for the same issue.
 5. **Warn when within X% of alarm threshold** - Optionally display a warning alarm in the **Dashboard List** (page 88) 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 164).
 6. Optionally activate a **trending alarm**. Trending alarms use historical data to predict when the next alarm 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 alarm is generated. Typically a trending window should be set to the amount of time you need to prepare for an alarm condition, if it occurs.
 - **Ignore additional trending alarms for** - Suppresses additional trending alarms for this same issue during this time period.
 - By default, trending alarms display as an orange icon  in the **Dashboard List** (page 88) page. You can change this icon using the **SNMP Icons** (page 164) tab.
 - Warning status alarms and trending status alarms don't create alarms 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** (page 314).

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 SNMP Sets list.

Save

Save changes made to the wizard pages.

Add SNMP Object

Monitor > Add SNMP Object

Monitor > Define SNMP Set > Edit > 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](#) (page 165) 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 163) 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 481) 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 138). 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

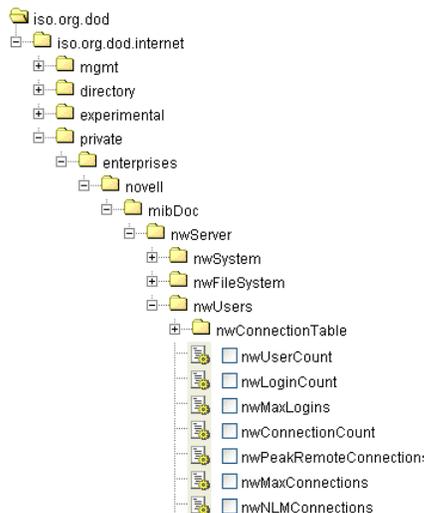
Click [Load MIB...](#) to browse for and upload a MIB file. When a MIB object is added, if the system does not already have the following standard MIB II files—required by most MIBs—it loads them automatically: `snmp-tc`, `snmp-smi`, `snmp-conf`, `rfc1213`, `rfc1759`. Once these files are loaded, the 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.

Monitor

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 159).

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](#) > [Edit](#) > [SNMP Icons](#)

The [SNMP Icons](#) tab selects the SNMP icons that display in the [Dashboard List](#) (page 88) 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 ⚪.

Save

Save changes made to the [SNMP Icons](#) 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.

LAN Watch

Monitor > LAN Watch

Agent > LAN Watch

LAN Watch uses an existing [agent](#) (page 470) on a managed machine to periodically scan the 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 or [SNMP devices](#) (page 481). Optionally, the VSA can send an [alert](#) (page 471) 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.

Using Multiple Machines on the Same LAN

There are only two reasons to do a SNMP LAN Watch on multiple machines within a scan range:

1. There are multiple SNMP Communities within the scan range and therefore there are multiple machines with different SNMP Community Read values.
2. The user wishes to have redundant SNMP monitoring.

Schedule

Click [Schedule](#) to schedule a recurring LAN Watch scan on each selected machine ID. The scan runs every interval that you set. The default is 1 day.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click [Cancel](#) to stop the scheduled scan. Cancel also deletes all records of the devices identified on a LAN from the VSA. If you re-schedule LAN Watch after clicking Cancel, each device on the LAN generates a new alert.

Run recurring every <N> <periods>

Check the box to make this task a recurring task. Enter the number of times to run this task each time period.

Scan IP Range

Set the minimum and maximum IP addresses to scan here. Selecting a machine ID to scan, by checking the box next to that machine's name, automatically fills in the minimum and maximum IP range based on that machine's IP address and subnet mask.

Note: LAN Watch does not scan more than 2048 IP addresses. If the subnet mask of the machine running LAN Watch specifies a larger IP range, LAN Watch truncates it to 2048 addresses. LAN Watch only detects addresses on the local subnet to the machine you run LAN Watch from. For example, with a subnet mask of 255.255.255.0, there can be no more than 253 other devices on the local subnet.

Enable SNMP

If checked, scan for [SNMP devices](#) (page 481) within the specified Scan IP Range.

Monitor

Read Community Name / Confirm

LAN Watch can only identify SNMP devices that share the same **SNMP Community** (page 481) **Read** value as the managed machine performing the LAN Watch. Enter the value in the **Read Community Name** and **Confirm** text boxes.

Note: Community names are *case sensitive*. Typically the default read community name value is `public`, but may be reset by an administrator to `Public`, `PUBLIC`, etc.

Enable vPro

If checked, identify **vPro** (page 486)-enabled machines within the specified **Scan IP Range**. A machine does not need to be a vPro machine to discover vPro machines using LAN Watch. If a vPro machine is used as the LAN Watch discovery machine, it cannot discover itself.

Note: vPro configuration is a prerequisite to using this feature. Refer to the latest Intel documentation for information on how to configure vPro. At the time of this writing, the following link leads to the Intel documentation: <http://communities.intel.com/docs/DOC-1429>.

Username / Password / Confirm

Enter the appropriate vPro credentials to return hardware asset details about vPro machines discovered during the LAN Watch. Typically the same credentials are defined for vPro machines on the same LAN. The results are displayed using Agent > **View vPro** (page 358).

If you don't know the credentials for the vPro machines you want to discover, enter *arbitrary strings* in the **Username**, **Password** and **Confirm** fields. This will allow you to discover the existence of the vPro machines, but not return any other hardware assets details.

Note: vPro-enabled machines with a vPro credential can be powered up, powered-down or rebooted using **Remote Cntl > Power Mgmt** (page 268).

Enable Alerts

If **Enable Alerts** is checked and a new device is discovered by LAN Watch, an alert is sent to all email addresses listed in **Email Recipients**. LAN Watch alerts and email recipients can also be specified using the Monitor > **Alerts** (page 100) page.

Note: Machines that have not connected to the LAN for more than 7 days and then connect are flagged as new devices and will generate an alert.

Email Recipients

If alerts are enabled, enter the email addresses where alert notifications are sent. You can specify a different email address for each managed machine, even if it is for the same event. The **From** email address is specified using System > **Configure** (page 394).

Ignore devices seen in the last <N> days

Enter the number of days to suppress alerts for new devices. This prevents creating alerts for devices that are connected to the network temporarily.

After alert run select script on this machine ID

If checked and an alarm condition is encountered, a script is run. You must click the **select script** link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Skip alert if MAC address matches existing agent

Checking this box suppresses alerts if the scan identifies that the MAC address of a network device belongs to an existing managed machine with an agent on it. Otherwise a managed machine that was offline for several days and comes back online triggers an unnecessary alert during a LAN Watch.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

IP Range Scanned

The IP addresses that are scanned by the selected machine ID when LAN Watch runs.

Last Scan

This timestamp shows when a machine ID was last scanned. When this date changes, new scan data is available to view.

Primary DC

If a primary domain controller icon  displays, this machine ID is a [primary domain controller](#) (page 479). If checked, performing a scan on a primary domain controller running Active Directory enables you "harvest" the users and computers throughout a domain. You can subsequently install VSA agents automatically on computers listed in Active Directory and create VSA administrators and VSA users based on Active Directory user credentials. See [View AD Computers](#) (page 354) and [View AD Users](#) (page 355).

SNMP Active

If the SNMP icon  displays, SNMP devices are included in the scheduled scan.

vPro Active

If the vPro icon  displays, vPro machines are included in the schedule scan.

Alert Active

If checked  LAN Watch alerts are enabled for this scan.

Assign SNMP

Monitor > Assign SNMP

The [Assign SNMP](#) page creates SNMP alerts for SNMP devices discovered using a [LAN Watch](#) (page 165). An [alert](#) (page 471) is a response to an alarm condition.

A SNMP set is a set of MIB objects used to monitor the performance of [SNMP enabled network devices](#) (page 481). 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 an device-specific SNMP set based on the objects discovered on that device during a LAN Watch. [SNMP quick sets](#) (page 481) 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 482) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Monitor > [LAN Watch](#) (page 165).
2. Assign SNMP sets to discovered devices using Monitor > [Assign SNMP](#) (page 168). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > [SNMP Log](#) (page 175) or [Dashboard List](#) (page 88).

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 138).
- Optionally maintain SNMP sets using Monitor > [SNMP Sets](#) (page 158).
- Optionally add an SNMP object using Monitor > [Add SNMP Object](#) (page 163).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > [SNMP Type](#) (page 178).
- Optionally write values to SNMP devices using Monitor > [Set SNMP Values](#) (page 177).

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 158). *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 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.
2. Click [Auto Learn](#) to display the [Auto Learn](#) (page 152) 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.

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.

To apply Auto Learn settings to selected SNMP devices:

1. Select a *standard* SNMP set using the <Select SNMP Set> drop-down list.
2. Click [Auto Learn](#) to display the [Auto Learn](#) (page 152) 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.

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 SNMP objects provided by the specific SNMP device you selected. These objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a [LAN Watch](#) (page 165) is performed. You can subsequently define device-specific SNMP sets called [quick sets](#) and associate alerts with these quick sets. Quick sets can be *individualized* for a single device. The *standard* version of the quick set can be shared with other administrators and applied to similar devices throughout the VSA. The prefix (QS) is used to distinguish quick set names from other kinds of SNMP sets.

1. Discover SNMP devices using Monitor > [LAN Watch](#) (page 165).
2. Assign SNMP sets to discovered devices using Monitor > [Assign SNMP](#) (page 168).
3. Click the [SNMP info](#) (page 172) link in the [Assign SNMP](#) page to display a list SNMP objects that apply to the specific SNMP device you selected.

Display SNMP alarms using Monitor > [SNMP Log](#) (page 175) or [Dashboard List](#) (page 88).

To Create a SNMP Alert

1. Check any of these checkboxes to perform their corresponding actions when a an alarm 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.

Monitor

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 Scripts

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 in scripts.

Within an Email	Within a Script	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 415) 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script to run on a specified range of machine IDs by clicking the [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that triggered the alarm.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

Select Monitor 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 158).

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.

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.

Monitor

Name / Type

The name returned by the ARP protocol when a [LAN Watch](#) (page 165) 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 172) link to display the SNMP objects for this SNMP device.

SNMP Sets

Displays the list of SNMP sets assigned to a SNMP device.



- [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 152) 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 158) 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 481):

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

Email Address

A comma separated list of email addresses where notifications are sent.

SNMP Quick Sets

Monitor > Assign SNMP > SNMP Info link

The [SNMP Info](#) link page displays a list of SNMP objects provided by the specific SNMP device you selected. These objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a [LAN Watch](#) (page 165) is performed. You can subsequently define device-specific SNMP sets called [quick sets](#) and associate alerts with these quick sets. Quick sets can be *individualized* for a single device. The *standard* version of the quick set can be shared with other administrators and applied to similar devices throughout the VSA. The prefix (QS) is used to distinguish quick set names from other kinds of SNMP sets.

1. Discover SNMP devices using Monitor > [LAN Watch](#) (page 165).
2. Assign SNMP sets to discovered devices using Monitor > [Assign SNMP](#) (page 168).
3. Click the [SNMP info](#) (page 172) link in the [Assign SNMP](#) page to display a list SNMP objects that apply to the specific SNMP device you selected.

4. Display SNMP alarms using [Monitor > SNMP Log](#) (page 175) or [Dashboard List](#) (page 88).
Use the following tabs on the [SNMP Info link](#) page to configure an SNMP quick set.

Discovered Objects Sets tab

The [Discovered Object Sets](#) 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".

SNMP Sets tab

The SNMP Sets 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](#) - Select the MIB object. Click [Add Object](#) (page 163) to add a MIB object that currently does not exist on the [Monitor Lists](#) (page 138) page.
- [Current SNMP Value](#) - The value returned by the object/instance combination by the latest SNMP "walk".
- [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.
- [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.
- [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](#).
- SNMP Sets tab

SNMP Icons tab

- Customize the alarm icons for this *specific SNMP quick set*. See [SNMP Icons](#) (page 164) 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.

Monitor

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](#) > [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 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.
2. Click [Auto Learn](#) to display the [Auto Learn](#) (*page 152*) 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.

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.
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 Log

The **SNMP Log** page displays SNMP log data of **MIB objects** (*page 481*) in a **SNMP Set** (*page 158*) 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 17*) 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.

Monitor

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.

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 500 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 159) for more information.

Display Last

Bar charts display log data for the last 500 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.

- 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 > 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 (page 165).

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine ID.Group ID

Lists [Machine ID.Group IDs](#) (page 476) currently matching the [Machine ID / Group ID filter](#) (page 17) and assigned a [SNMP Community](#) (page 481) 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.

Monitor

- [MIBObject](#) - Select the MIB object. Click [Add Object](#) (page 163) to add a MIB object that currently does not exist on the [Monitor Lists](#) (page 138) 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 script 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.

SNMP Type

Monitor > SNMP Type

The [SNMP Type](#) page assigns types to SNMP devices. 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.

You can assign [SNMP sets](#) (page 481) to [devices](#) (page 481) *by type* automatically as follows:

1. Add or edit SNMP types using the [SNMP Device](#) tab in Monitor > [Monitor Lists](#) (page 138).
2. Add or edit the `sysServicesNumber` associated with SNMP types using the [SNMP Services](#) tab in Monitor > Monitor Lists. Broad categories of SNMP devices share the same `sysServiceNumber`.
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 159).
4. Perform a [LAN Watch](#) (page 165). During a LAN Watch 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.
5. Manually assign a SNMP type to an SNMP device using Monitor > [SNMP Type](#) (page 178). 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](#) (page 165).

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](#) > [Parser Summary](#)

The [Parser Summary](#) page displays and optionally define alerts for all parser sets assigned to all machine IDs the administrator has access to. [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.

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 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 a an alarm condition is encountered:

Monitor

- Create [Alarm](#)
 - 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 Scripts

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Delete

Click the delete icon  next to a parser set to delete its assignment to a machine ID.

Monitor

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 [Script](#)
- 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>](#).

Re-Arm

Applies only if [Ignore additional alarms for <N> <periods>](#) is selected.

Log Parser

Monitor > Log Parser

The [Log Parser](#) page defines log parsers and assigns them to selected machine IDs.

Note: The log parsers are only *active* if they are subsequently assigned a log parser set using [Assign Parser Sets \(page 187\)](#).

Log Monitoring

The VSA is capable of monitoring data collected from many [standard log files \(page 476\)](#). [Log Monitoring](#) extends that capability by extracting data from the output of *any* text-based log file. Examples include application log files and [syslog \(page 483\)](#) files created for Unix, Linux, and Macintosh operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the KServer database, Log Monitoring uses a [parser definitions and parser sets \(page 478\)](#) 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 the [Machine Summary \(page 21\)](#) page or by generating a report using the [Agent > Logs \(page 309\)](#) page. Administrators can optionally trigger alerts when a Log Monitoring record is generated, as defined using [Assign Parsing Sets \(page 187\)](#) or [Parser Summary \(page 179\)](#).

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 archives 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 script event itself. Only a new configuration, or reconfiguration, using Log Parser, Assign Parser Sets or Parser Summary generates a script you can see in the Script History or Pending Script 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 184*) to create a new log parser.

Edit...

Select an existing log parser in the [Log File Parser](#) drop-down list and click [Edit...](#) (*page 184*) 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 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 \(page 182\)](#) page. Log parsers are initially [private \(page 480\)](#), but can be shared with other administrators.

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 archives 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 script event itself. Only a new configuration, or reconfiguration, using Log Parser, Assign Parser Sets or Parser Summary generates a script you can see in the Script History or Pending Script 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 [individual administrators \(page 388\)](#), [administrator roles \(page 383\)](#), or make the script public to all administrators.

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\var\log\messages](#) or n:\var\log\messages.

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:

[\\morpheus\var\log\messages.*](#) or n:\var\log\messages.*.

Description

Enter a description for the log parser.

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.
- 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.

Multiline Template

If checked, multiple lines of text and log file parameters are used to parse the log file.

Output Template

Enter a pattern of text and log file parameters to store in [Log Monitoring](#).

Monitor

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

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: If you include a `$Time$` parameter in your template, Log Monitoring uses the time stored in the `$Time$` parameter as the log entry time. Date and time filtering is based on 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.

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 administrator'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 > Assign Parser Sets

The [Assign Parser Sets](#) page creates and edits parser sets and assigns parsers sets to machine IDs. Optionally triggers an alert based on a parser set assignment. A machine ID in the paging area only displays in the paging area of this page if:

- That machine ID has been previously assigned a [log file parser definition](#) (*page 184*) using Monitor > [Log Parser](#) (*page 182*).
- 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.

Parser Definitions and Parser Sets

When configuring [Log Monitoring](#) (*page 476*) 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, and
- Populate parameters with log data values.

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 KServer 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.

Monitor

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 a an alarm 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 Scripts

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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column (page 415) 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

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script to run on a specified range of machine IDs by clicking the [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that triggered the alarm.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

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 182) page.

Define log sets to match

After a log parser is selected, click [Edit](#) (page 191) to define a new parser set or select an existing parser set from the [Define log sets to match](#) (page 191) 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>](#)

Monitor

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (*page 476*) displayed is based on the [Machine ID / Group ID filter](#) (*page 17*) and the machine groups the administrator is authorized to see using [System > Group Access](#) (*page 385*).

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 [Script](#)
- 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>](#).

Re-Arm

Applies only if [Ignore additional alarms for <N> <periods>](#) is selected.

Log File Set Definition

Monitor > 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 476](#)) 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, and
- Populate parameters with log data values.

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 KServer 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 184](#)) 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*.

Monitor

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.

Chapter 7

Ticketing



In This Chapter

Ticketing Tab	194
View Summary	194
Create/View	197
Delete/Archive	200
Notify Policy	202
Access Policy	204
Assignee Policy	205
Due Date Policy	205
Edit Fields	207
Email Reader	208
Email Mapping	210
Edit Profile / User Profiles	210
User Access	212

Ticketing Tab

The **Ticketing Tab** manages service requests from VSA users. These service requests, and your response to them, are documented using **tickets**.

The ticketing system automatically sends email alerts to designated administrators and users for such system events as ticket creation, changes, or resolutions. The system organizes tickets by machine ID or group ID. You may wish to create extra machine ID accounts or group IDs to hold tickets of a global nature, such as general network problems.

Functions	Description
View Summary <i>(page 194)</i>	Define email alerts on a per machine basis.
Create/View <i>(page 197)</i>	Create new tickets, or add or modify notes in existing tickets.
Delete/Archive <i>(page 200)</i>	Permanently delete tickets or move tickets into archival storage.
Notify Policy <i>(page 202)</i>	Determine when email notifications are sent out by the Ticketing module.
Access Policy <i>(page 204)</i>	Determine who can edit and/or display fields in tickets.
Due Date Policy <i>(page 205)</i>	Define default due dates for new tickets based on field values and email subject lines.
Edit Fields <i>(page 207)</i>	Define, modify, or create ticket fields used to classify tickets.
Email Reader <i>(page 208)</i>	Setup automatic polling of a POP3 email server to generate new ticket entries.
Email Mapping <i>(page 210)</i>	Define default field values for new tickets received using the Email Reader. Separate email maps may be defined for email addresses or domains.
User Profiles <i>(page 210)</i>	Edit machine account information.
User Access <i>(page 212)</i>	Set up user accounts to enable users to view or create tickets, chat with administrators and remote control their own machines.

View Summary

Ticketing > View Summary

- Similar information is provided using [Reports > Ticketing](#) *(page 311)*.

The **View Summary** page lists all tickets assigned to machine IDs or group IDs. 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 administrator has viewed all the notes in the ticket. Once viewed, the ticket is marked as read using the  icon. If another administrator 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 displayed depends on the [machine ID / group ID filter](#) (*page 17*) and machine groups the administrator is authorized to see using System > [Group Access](#) (*page 385*).
- 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.
- Users only have access to tickets for their own machine ID.

Assignees

The assignee list presented in [View Summary](#) (*page 194*) and in [Create/View](#) (*page 197*) is created based on the access rights of the currently logged on user. There are three basic sets of rights in the system: master administrator, standard administrator, and user. The assignee list for each is generated as follows.

- **Master Administrators** - Includes all administrators in the VSA.
- **Standard Administrators** - Includes any administrator matching *one* of the following criteria:
 - Any administrator that has access to any machine group that the logged on standard administrator also has access to.
 - All administrators that are members of the same administrator role as the standard administrator.
 - All administrators that have access to all groups.
 - The currently logged in standard administrator.
- **Users** - Includes all administrators that have access to the same machine group the currently logged in user's machine is in.

Tickets for Deleted Machines

The system does not delete tickets when deleting machine IDs. Because no machine data exists for deleted machine IDs, [views](#) (*page 485*) are not applied to this table.

Note: See [Ticketing > Delete/Archive](#) (*page 200*) to delete or archive tickets.

Open Tickets, Past Due, Hold Tickets, Total Tickets

Shows the number of tickets open, past due, on hold, 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](#). Include an asterisk (*) wildcard with the text you enter to match multiple records.

Clicking any of the ticket [Summary](#) links in the paging area displays the details of that ticket using the [View Ticket](#) (*page 197*) page. Words in the ticket notes matching any **Search** word are *highlighted with a green background*.

Ticketing

<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 administrator or 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.
- [Category](#) - Type of problem this ticket discusses.
- [Assignee](#) - Name of the administrator responsible for solving this problem.
- [Status](#) - Open, Hold, Closed
- [Priority](#) - High, Normal, Low
- [Submitter Name](#) - Person who submitted this ticket: administrator, user name, or machine ID.
- [Submitter Email](#) - The submitter email address.
- [Submitter Phone](#) - The submitter phone number.
- [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.

You can also select additional custom fields you have previously created using Ticketing > [Edit Fields](#) (*page 207*).

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 207*).

Mark All Read

Click to mark all tickets as read. Read tickets display a  icon. Any changes or note additions inserted by other administrators 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](#).

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.
- 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 > Create/View

The [Create/View](#) page creates new tickets, or adds or modify notes in existing tickets. Begin by entering a ticket number in the [Ticket ID](#) field. If you don't know the number of the ticket, use [View Summary](#) ([page 194](#)) or [Delete/Archive](#) ([page 200](#)) to locate and select the ticket. The ticket will be displayed using this page.

Editing an Existing Ticket

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.

Ticketing

- 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 is closed.

Note: View, edit and delete privileges for tickets and fields are controlled using [Ticketing > Access Policy \(page 204\)](#). Users and administrators are notified about ticket changes based on [Ticketing > Notify Policy \(page 202\)](#). Change the number automatically assigned to the next new ticket using [Edit Fields \(page 207\)](#).

Creating a New Ticket

Perform the following steps to create a new ticket.

1. All tickets must be assigned to either a machine ID or a group ID.
 - a. Click the [Select machine ID or Group ID](#) link to display a dialog box.
 - b. Select either `machine` or `group` from the [Select <name> ID to assign trouble ticket to](#) drop-down list.
 - c. Select a specific machine or group to assign your new ticket to.
 - d. Once you've selected a machine or group, the dialog box closes and an edit  icon displays next to machine ID or group ID you have selected. You can click this icon to associate a ticket with a different machine ID or group ID.
2. Enter a short description of the problem in the [Summary](#) field.
3. The [Submitter](#) fields are populated as follows:
 - If a machine ID was selected in step 1, the submitter [User Name](#), [User Email](#) and [User Phone](#) fields are populated with contact data maintained for this machine ID using [Ticketing > Edit Profile \(page 210\)](#). This information can be updated if need be.
 - If a group ID was selected in step 1, these submitter fields can be filled in manually, if applicable.
 - If a ticket was created based on a user's or administrator's email using [Ticketing > Email Reader \(page 208\)](#), the [Submitter Email](#) field is populated with the sender's email address.
4. The [Date Created](#) is automatically assigned. This is the date the ticket is created.
5. The [Age / Closed](#) date is automatically assigned. [Age](#) lists the number of hours/days since the creation date for open and hold tickets. If the ticket has been closed then [Age](#) is replaced with [Closed](#) and displays the date and time this ticket was closed.
6. The default due date for a ticket is determined by the [Ticketing > Due Date Policy \(page 205\)](#). It's based on the ticket attributes you enter when a *new* ticket is entered. If the 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 \(page 205\)](#), 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 \(page 194\)](#) page and in [Ticketing \(page 311\)](#) reports. It also displays in **red text** in the header of the [Create/View \(page 197\)](#) page. You can optionally send an email for overdue tickets using [Ticketing > Notify Policy \(page 202\)](#). A ticket is resolved when its status is set to closed and the resolution date is recorded.
7. Classify the ticket using the built-in [Assignee](#), [Category](#), [Status](#), and [Priority](#) fields. You can also classify the ticket using additional `List` type fields that have been created for tickets using [Ticketing > Edit Fields \(page 207\)](#).

Note: All `List` field changes are immediately saved in the ticket.

8. 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.

9. 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.

10. Check the [Suppress email notification](#) checkbox if you won't want email recipients to be notified about the ticket. In most cases you'll want to leave this blank.
11. Complete the creation of the ticket in one of two ways:
- Click [Submit](#) to complete the creation of the ticket and to notify *both* user and administrator email recipients.
 - Click [New Hidden](#) to complete the creation of the ticket to notify *only* administrators email recipients. Use hidden notes to record data or analysis that may be too detailed or confusing to users but useful to other administrators.

Note: Hidden notes are *never* included in email notifications.

Assignees

The assignee list presented in [View Summary](#) (page 194) and in [Create/View](#) (page 197) is created based on the access rights of the currently logged on user. There are three basic sets of rights in the system: master administrator, standard administrator, and user. The assignee list for each is generated as follows.

- [Master Administrators](#) - Includes all administrators in the VSA.
- [Standard Administrators](#) - Includes any administrator matching *one* of the following criteria:
 - Any administrator that has access to any machine group that the logged on standard administrator also has access to.
 - All administrators that are members of the same administrator role as the standard administrator.
 - All administrators that have access to all groups.
 - The currently logged in standard administrator.
- [Users](#) - Includes all administrators that have access to the same machine group the currently logged in user's machine is in.

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 205). 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 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 197) web page for a specific ticket ID

Error! Hyperlink reference not valid.>

Ticketing

For example:

<http://demo.kaseya.com?ticid=1234>Ticket ID

Enter the ticket ID to view/edit an existing ticket. Leave blank to create a new ticket.

Time/Admin

Lists the time a change was made to a ticket and the administrator or user who made the change.

Notes Table

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 [User Access \(page 212\)](#) for details.

Hide

If checked, the note is hidden from users but not other administrators. The default setting is determined by the [as hidden note](#) checkbox in Ticketing > [Access Policy \(page 204\)](#). Access policies are applied by administrator group. If you belong to more than one administrative group, the most restrictive policy has precedence.

Delete/Archive

Ticketing > Delete/Archive

You may reach the point where your system has so many old tickets that they are cluttering up searches with obsolete data. The [Delete/Archive](#) page deletes old tickets, or deletes tickets in a particular category or status.

Note: View, edit and delete privileges for tickets and fields are controlled using [Ticketing > Access Policy \(page 204\)](#).

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 displayed depends on the [machine ID / group ID filter \(page 17\)](#) and machine groups the administrator is authorized to see using System > [Group Access \(page 385\)](#).
- 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.
- Users only have access to tickets for their own machine ID.
- 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, Hold Tickets, Total Tickets

Shows the number of tickets open, past due, on hold, 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](#). Include an asterisk (*) wildcard with the text you enter to match multiple records.

Clicking any of the ticket [Summary](#) links in the paging area displays the details of that ticket using the [View Ticket](#) (*page 197*) 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 administrator or 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.
- [Category](#) - Type of problem this ticket discusses.
- [Assignee](#) - Name of the administrator responsible for solving this problem.
- [Status](#) - Open, Hold, Closed
- [Priority](#) - High, Normal, Low
- [Submitter Name](#) - Person who submitted this ticket: administrator, user name, or machine ID.
- [Submitter Email](#) - The submitter email address.
- [Submitter Phone](#) - The submitter phone number.
- [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.

You can also select additional custom fields you have previously created using Ticketing > [Edit Fields](#) (*page 207*).

Ticketing

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 207).

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.

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.

Notify Policy

[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 group ID, 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 administrators for ticket creations and note additions, but send email to a different list of administrators for overdue tickets. As a default, no email notifications are sent. You must check the checkbox of at least one ticketing event to get an email notification sent.

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 208).

From Address

The `From` address used by ticket notifications is based on the [Email Reader](#) (page 208) address, if one is defined. If an [Email Reader](#) has not yet been defined then the ticket notification `From` address uses the email address defined using `System > Configure` (page 394).

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 any note is added or changed to a ticket.
- [Overdue Ticket](#) - If checked, an email is sent when a ticket passes its due date without being closed.
- [Assignee Change](#) - If checked, an email is sent when a ticket is assigned to a different administrator. 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.
- [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.
- [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 new note is created for a 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 208) and [Email Mapping](#) (page 210). Click [Format](#) to edit the format for this email notification.
- [Format Email...](#) - This option only displays for [master administrators](#) (page 469). Specifies the standard message sent in reply to inbound emails used to create new tickets.

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 > Access Policy

The [Access Policy](#) page determines who can edit and/or display fields in tickets. Independent policies can be set for each administrator role and for all users. Users only see tickets assigned to their machine ID. Standard administrators only see tickets for group IDs they are authorized to access.

Select user or administrator group

Before setting any other policy options, select `<Users>` or an administrator role from the drop-down list.

Access Rights

The following access rights apply to all *users* or to a selected *administrator role*, as specified using [Select user or administrator group](#).

- [Enable ticket delete](#) - If checked, the selected administrator role can delete entire tickets using the [Delete/Archive \(page 200\)](#) page.
- [Enable ticket edit to modify or remove notes or modify summary line \(Adding new notes is always enabled\)](#) - If checked, the selected administrator role can edit existing notes or modify the summary line.

Note: Adding new notes is always enabled for all administrator groups.

- [Enable associate ticket with editing](#) - If checked, enables the selected administrator 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 administrator role can modify the ticket due date.
- [Enable suppress email notifications when editing trouble tickets](#) - If checked, the selected administrator role can suppress email notifications when modifying an existing ticket.
- [View hidden notes](#) - If checked, the selected administrator role can view hidden notes.

Note: Hidden notes can *never* be viewed by users.

- [Change hidden notes status checkbox](#) - If checked for the selected administrator 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 administrator role, notes are automatically inserted whenever any ticket field changes.
 - [As hidden note](#) - If checked for the selected administrator 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](#) -
- [Define access to each ticket field](#) - Defines access to each field for the selected administrator role. Fields are created using [Edit Fields \(page 207\)](#). 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](#) > [Assignee Policy](#)

The [Assignee Policy](#) page automatically assigns an administrator 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 207).

Overriding Assignee Policy

[Assignee Policy](#) can be overridden for a specific ticket using the [Create/View](#) (page 197) page, by the toggling the  icon next to the [Assignee](#) field to display a  icon, then assigning an administrator 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 administrator 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](#) > [Due Date Policy](#)

The [Due Date Policy](#) page sets the due date for each *new ticket* based on field values. Any combination of list fields may be defined to set a due date. This allows you to set a ticket due date based on the urgency of the ticket and a guaranteed level of service. For example, define a new field named [Service Level](#) with the following list items: 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.

Ticketing

Overdue Tickets

When a ticket is overdue, the due date displays in bolded **dark red text**, both in the [View Summary](#) (page 194) page and in [Ticketing](#) (page 311) reports. It also displays in **red text** in the header of the [Create/View](#) (page 197) page. You can optionally send an email for overdue tickets using Ticketing > [Notify Policy](#) (page 202). 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 this 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 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 207).

Edit Fields

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 194), [View Ticket](#) (page 197), [Delete/Archive](#) (page 200), [Access Policy](#) (page 204), [Due Date Policy](#) (page 205) and [Email Mapping](#) (page 210).

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 [View Tickets](#) (page 197).

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 on the [View Summary](#) (page 194) and [Delete/Archive](#) (page 200) page.

- `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.

Ticketing

Note: Default values are system wide and may not be different for different machine group IDs or administrator roles.

Note: Email Mapping (page 210) can override the default values selected here for tickets created using Email Reader (page 208).

<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.

Update

Click [Update](#) to confirm changes to field labels, default values, or list values.

New

Click [New](#) to create a new field.

Email Reader

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 210) and converted into tickets.

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.

- `~ticaid='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 administrator. The administrator 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 210), 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 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.

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.

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.

Filter Emails

Enter text to reject 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
```

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 > Email Mapping

The [Email Mapping](#) page assigns default values for tickets created using the [Email Reader](#) (page 208). 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 207).

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 (Select Machine or Group ID)

Click the [Select Machine or Group ID](#) link to associate tickets created using this map with either a machine ID or group ID.

Assignee

Enter the name of the administrator responsible for solving this problem.

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

Edit Profile / User Profiles

Agent > Edit Profile

Ticketing > User Profiles

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:

- Notes and contact information can also be maintained using the [Agent Settings](#) tab of the [Machine Summary](#) (page 21) page.

- The contact information in the [Edit Profile](#) page can be automatically populated when a new account is created using the [Agent > Create](#) (page 341) page.
- The user can update his or her contact name, contact email and contact phone number using the [Change Profile](#) option on the [User Access](#) page.

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](#).
4. The newly entered settings are shown in the respective machine ID account's fields.

Notes

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.

Show notes as tooltip

If checked, [Edit Profile](#) notes are included as part of the tooltip that displays whenever the cursor hovers over a machine ID's [check-in status icon](#) (see "Check-in Status" on page 473).

Auto assign tickets

Auto assign a ticket to this machine ID if the [Ticketing email reader](#) (page 208) receives an email from the same email address as the [Contact Email](#). Applies when new emails come into the ticketing email reader that do not map into any of the [email mappings](#) (page 210)

Note: if multiple machine IDs have the same contact email, then only one machine ID can have this checkbox checked.

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.

Note: A Contact Email address is required for users to receive a new password using the [Get New Password](#) option on the [User Access Welcome Page](#) (page 484). See [Agent > User Access](#) (page 212) for more information.

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 of the individual responsible for administering support to the managed machine. This can be the administrator, but is often someone who is part of the IT staff of the company that owns the managed machine. This setting is displayed in the [Admin Email](#) column.

Ticketing

Language Preference

The language selected in the [Language Preference](#) drop down list determines the language displayed by an [agent menu](#) (page 361) on a managed machine. The languages available are determined by the language packages installed using System > [Preferences](#) (page 377).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

User Access

[Agent](#) > [User Access](#)

[Ticketing](#) > [User Access](#)

The [User Access](#) page determines whether users can perform the following tasks from their own machine or from another machine using the [User Access Welcome Page](#) (page 484):

- Remote control or FTP *their own managed machine from another machine*. This is the same remote control capability administrators have, except it restricts users to their own machine.
- *Initiate* a chat session with a KServer administrator from their own machine or any other machine.

Note: An administrator can always initiate a chat (page 279) session with a user regardless of this setting.

- Create or display tickets for their own machine or any other machine.
- Use any other menu option on the User Access Welcome Page from another machine as though they were currently logged into their own managed machine. For example, send email.

Note: Remote Cntl, Ticketing and Chat must be enabled using this page for these options to be visible on the User Access Welcome Page.

Note: You can download a User Access Quick Start Guide from the first topic of online help.

Accessing the User Access Welcome Page Remotely

A user can display the User Access Welcome Page associated with their own machine from another machine as follows:

1. Log into http://your_KServer_address/access/ page, substituting the appropriate target KServer name for `your_KServer_address` in the URL text.

Note: This is the same page that administrators use to log into the KServer.

2. Log into the KServer by entering either:
 - The machine ID.group ID and the password assigned to the machine ID using this page, or
 - The user name and password assigned to the machine ID using this page.

The User Access Welcome Page displays. The user can click any menu option as though he or she were logged in from their own managed machine. The 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.

Re-Enabling User Logons

User logons follow the same [Logon Policy](#) (page 403) as administrator 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.

Generating a New User Access Password

If a user has forgotten their user access password, they can generate a new password as follows:

1. Log into http://your_KServer_address/access/ page, substituting the appropriate target KServer name for `your_KServer_address` in the URL text.

Note: This is the same page that administrators use to log into the KServer.

2. Enter their user name in the [Username](#) field.
3. Click the [Get New Password](#) menu option.

A new random password is sent to the user email address of record for the managed machine. This user email address is set using the [Contact Email](#) field in Agent > [Edit Profile](#) (page 210).

Customizing the User Access Welcome Page

Master administrators can customize the web page seen by users using System > [Customize](#) (page 403), adding their company's logo, look, and feel to the web experience for their users.

Logon Name

Enter the [Logon Name](#) the user must use to log into the KServer 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. If no logon name is specified, then the [Logon Name](#) defaults to the machine.group name

Note: All logon names must be unique in the system. Since users may also logon using their machine ID, logon names, machine IDs, and administrator names must all be unique.

Create Password, Confirm Password

Define a password for the user logon. Passwords must be at least 6 characters long. The user can change the password after the administrator assigns him one. See [Generating a New User Access Password](#) above.

Apply

Click [Apply](#) to apply the logon name and password to the selected machine ID.

Ticketing

Clear

Permanently remove the logon [credential](#) (page 473) from the selected machine ID.

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Logon Name

The logon name assigned to this machine ID. Users that have been granted remote access to their machine may logon using [either](#) their machine ID or logon name.

User Web Logon

Displays `Enabled` if a logon name and password has been assigned to this machine ID, even if [Remote Cntl](#), [FTP](#) and [Chat](#) are not checked. Indicates that a user can log into the user page from a web browser on any machine. They can always get to that same page by double clicking the agent icon on their own machine or selecting [Contact Administrator...](#) from the [agent menu](#) (page 469).

Enable Remote Cntl

Check this box to allow users remote control access to their machine when they log on to the VSA through any web browser.

Enable Ticketing

Check this box to allow users to create and modify tickets for their own machines. Users can only see tickets assigned to their machine.

Enable Chat

Check this box to allow users to initiate a chat session with a logged in administrator. They will only be able to chat with administrators that have access rights to the group ID that the user's machine belongs to.

Chapter 8

Patch Management

In This Chapter

Patch Mgmt Tab	216
Scan Machine	221
Patch Status	222
Initial Update	224
Pre/Post Script: Patch Management	226
Automatic Update	227
Machine History	228
Machine Update	229
Patch Update	231
Rollback	234
Cancel Updates	234
Create/Delete: Patch Policy	235
Membership: Patch Policy	236
Approval by Policy	238
Approval by Patch	240
KB Override	242
Windows Auto Update	243
Reboot Action	245
File Source	248
Patch Alert	250
Office Source	254
Command Line	256
Patch Location	258

Patch Mgmt Tab

Use the **Patch Mgmt** tab to monitor, scan, install, and verify Microsoft patches on managed machines. Patch management automates the process of keeping all your machines up to date with the latest patches. You decide how and when updates are applied on a per machine basis. See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

Note: You can view Patch Management demos at <http://www.kaseya.com/get-started/demo.aspx>.

Functions	Description
Scan Machine (page 221)	Determine what patches are missing on managed machines.
Patch Status (page 222)	Display a summary view of installed, missing and denied patches for each managed machine.
Initial Update (page 224)	Perform <i>one-time</i> processing of <i>all</i> approved patches on managed machines.
Pre/Post Script (page 226)	Run scripts before and/or after patch Initial Update.
Automatic Update (page 227)	Update missing approved patches on managed machines automatically on a <i>recurring</i> basis.
Machine History (page 228)	Display a detailed view of patch scan results for each managed machine.
Machine Update (page 229)	Schedule the installation of missing patches for an individual machine.
Patch Update (page 231)	Apply individual patches to multiple machines.
Rollback (page 234)	Uninstall patches from managed machines.
Cancel Updates (page 234)	Cancel pending patch installations.
Create Delete (page 235)	Create and delete machine patch policies.
Membership (page 236)	Assign machine IDs as members of one or more patch policies.
Approval by Policy (page 238)	Approve or deny patches by patch policy.
Approval by Patch (page 240)	Approve or deny patches by patch.
KB Override (page 242)	Override patch policy default approval status by Microsoft knowledge base article.
Windows Auto Update (page 243)	Remotely set the Windows Automatic Updates settings on selected machines.
Reboot Action (page 245)	Determine whether or not to reboot the machine automatically after installing new patches.
File Source (page 248)	Specify where each machine gets new patch installation files from.
Patch Alert (page 250)	Configure alerts for patch-related events, such as when a new patch becomes available for a managed machine.
Office Source (page 254)	Specify an alternate source location for MS Office installation files.
Command Line (page 256)	Set the command line parameters used to install

	patches.
Patch Location (page 258)	Specify the URL to download a patch from when the system can not automatically locate it.

Methods of Updating Patches

The VSA provides **five** methods of applying Microsoft patches to managed machines:

- **Initial Update** is a *one-time* processing of all approved Microsoft patches applicable to a managed machine based on **Patch Policy** (page 478). **Initial Update** ignores the **Reboot Action** (page 245) policy and reboots the managed machine **without warning the user** as often as necessary until the machine has been brought up to the latest patch level. **Initial Update** should only be performed during non-business hours and is typically performed on newly added machines.
- **Automatic Update** is the *preferred* method of updating managed machines on a *recurring* basis. Obeys both the **Patch Policy** and the **Reboot Action** policy.
- **Patch Update** - If you're using **Automatic Update**, then **Patch Update** is used on an exception basis to apply individual patches to multiple machines or for patches that originally failed on certain machines. Overrides the **Patch Policy** but obeys the **Reboot Action** policy.
- **Machine Update** - If you're using **Automatic Update**, then **Machine Update** is used on an exception basis to apply patches to individual machines. Overrides the **Patch Policy** but obeys the **Reboot Action** policy. **Machine Update** is often used to test a new patch prior to approving it for general release to all machines.
- **Patch Deploy** - You can also use a user defined script to install a Microsoft patch using Scripts > **Patch Deploy** (page 55). 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 script for these hot fixes, via this wizard, that can be used to schedule the installation on any desired machine.

Note: You can install non-Microsoft applications using Scripts > Application Deploy (page 56). When a pre-defined install solution cannot be used, use Scripts > Packager (page 58) to create a self-extracting file ready for automated distribution.

You can also cancel a pending patch installation or uninstall patches.

- Cancel pending patch updates using **Cancel Updates** (page 234).
- Use the **Patch Update** (page 231) page to cancel the pending update of a specific patch on all machines.
- Remove patches from managed machines using **Rollback** (page 234).

Configuring Patch Management

Analyzing Patch Status

You can determine the patch status of managed machines using the following pages:

- Determine what patches are missing on managed machines using **Scan Machine** (page 221).
- Display a summary view of installed, missing and denied patches for each managed machine using **Patch Status** (page 222).
- Display a detailed view of patch scan results for each managed machine using **Patch History** (page 228).

Configuring Patch Management

The following configuration pages apply to **Initial Update**, **Automatic Update**, **Patch Update**, and **Machine Update** unless indicated otherwise.

Patch Management

- Optionally create a [patch policy](#) (page 478) using Patch Mgmt > [Create/Delete](#) (page 235). Patch policies are required to set approval policies. Applies to [Automatic Update](#) and [Initial Update](#).
- Optionally assign machine IDs to a patch policy using Patch Mgmt > [Membership](#) (page 236). Applies to [Automatic Update](#) and [Initial Update](#).
- Optionally set patch approval policies using [Approval by Policy](#) (page 238), [Approval by Patch](#) (page 240) or [KB Override](#) (page 242). Applies to [Automatic Update](#) and [Initial Update](#).
- Optionally change the reboot policy for machine IDs using [Reboot Action](#) (page 245). Applies to [Automatic Update](#), [Patch Update](#) and [Machine Update](#).
- Optionally change the [File Source](#) (page 248) location machines use to download patches.
- Optionally change command line parameters for installing selected patches using the [Command Line](#) (page 256) page.
- Optionally change the URL patches are downloaded from using [Patch Location](#) (page 258).
- Optionally configure alerts for patch-related events using [Patch Alert](#) (page 250).
- Optionally enable or disable [Windows Auto Update](#) (page 243) on managed machines.
- If a [credential](#) (page 371) has been created for a machine ID, then all patches are installed on that machine ID using the rights of that credential. A credential must be defined to use the [Office Source](#) page.
- Optionally create an alternate source location for Office patches using [Office Source](#) (page 254).
- Optionally run scripts before or after [Initial Update](#) (page 224). Applies to [Initial Update](#) only.

Patch Processing

When you schedule a patch the following occurs:

1. The agent on the managed machine is told to start the update process at the scheduled time.
2. The patch executable is downloaded to the managed machine from where ever the [File Source](#) (page 248) is set for that machine ID.
3. The patch file is executed on the managed machine using the parameters specified in [Command Line](#) (page 256). You should never have to set these switches yourself, but just in case, this capability is there.
4. After all the patches have been installed the managed machine is rebooted. *When* reboots occur for a machine ID depends on the [Reboot Action](#) (page 245) assigned to that machine ID. Applies to [Machine Update](#) (page 229), [Patch Update](#) (page 231) and [Automatic Update](#) (page 227). Reboots in response to an [Initial Update](#) (page 224) always occur immediately and without warning the user.
5. The managed machine is rescanned automatically. It takes 2 to 3 minutes after the reboot is complete for this data to show up on the VSA. Wait several minutes before checking the patch state after a reboot.

Note: If you schedule multiple patches for installation on the same machine, all the patches are installed at the same time. After all the patches have been installed the machine reboots once. This technique saves time and reboots.

Note: Service packs are always installed separately. If you are installing a service pack with other patches you will see a reboot after the service pack install and than another single reboot after all the other patches are installed.

Superseded Patches

A superseded patch is a patch that doesn't have to be installed because a later patch is available. A typical example is a service pack, which bundles many other patches that have been been released before the service pack. If you install the service pack, you don't have to install all the earlier patches.

Patch Management only reports patches superseded by a service pack. Superseded patches have a string appended to the title of patch that indicates that it is superseded by Service Pack X. This string is displayed as **dark red text with a yellow background** to make it stand out.

Example: **Superseded By: KB936929 Windows XP Service Pack 3 (KB936929)**

The installation process installs superseded updates *only if* the service pack that supersedes these updates *is not* selected for installation. If the superseding service pack is selected for installation, the superseded updates *are not* downloaded or installed. A script log entry is added to indicate the update was skipped because it was superseded.

In addition:

- Patch titles in the [Patch Management](#) (page 299) report include Superseded By: Service Pack X, when applicable.
- The patch filter on the patch approval pages now include the ability to filter on superseded/not superseded.
- Occasionally, the Superseded By warning displays as Superseded By: Unspecified. This is typically caused by a cross-operating system patch that is superseded by one or more service packs. This is likely to be seen on updates dealing with Media Player.

Update Classification

Microsoft updates are organized as follows:

Update Classification	Classification Type (Non-Vista / Vista)	Included in WSUSSCN2.CAB*
Security Updates	High Priority / Important Includes critical, important, moderate, low, and non-rated security updates.	Yes
Critical Updates	High Priority / Important	Yes
Update Rollups	High Priority / Important	Yes
Service Packs	Optional – Software / Recommended	Yes
Updates	Optional – Software / Recommended	No
Feature Packs	Optional – Software / Recommended	No
Tools	Optional – Software / Recommended	No

In those cases where a machine does not have Internet connectivity at the time of a machine patch scan, Kaseya uses Microsoft's WSUSSCN2.CAB data file. Microsoft publishes this CAB file as needed. It contains a sub-set of the Microsoft Update Catalog. As seen in the table above, scan data for only the high priority updates and service packs are included in the CAB file. The KServer automatically downloads the CAB file on a daily basis to make it available for those machines needing this type of scan. See [Windows Automatic Update](#) (page 486).

Patch Failure

After the patch installation attempt completes—including the reboot if requested—the system re-scans the target machine. If a patch still shows missing after the re-scan, failure is reported. Patches can fail for several reasons:

- [Insufficient Disk Space](#) - Patches are downloaded, or copied from a file share, to the local machine's hard disk. Several patches, especially service packs, may require significant additional local disk space to completely install. Verify the target machine has plenty of disk space available.
- [Bad Patch File](#) - The phrase Bad Patch File in the [Comments](#) column indicates the patch file failed to execute for some reason. If you schedule multiple patches to install as a batch and even *one* of them fails, all the patches are marked as Bad Patch File. The system is reporting a script failure and can not distinguish which patch in the script caused the failure. You

Patch Management

can determine which patch failed by looking at the [Script Log](#) (page 309) for this machine. The log indicates which patches successfully installed prior to the script failure.

- **Corrupted Patch File** - The downloaded patch file is corrupt.
- **Missing Patch Location** - The phrase `Missing patch location` in the **Comments** column means the URL used to download patches from on the Microsoft website is missing. You can manually enter the correct location using the [Patch Location](#) (page 258) page.
- **No Reboot** - Several patches require a system reboot before they take effect. If your **Reboot Action** (page 245) settings did not allow a reboot, the patch may be installed but will not be effective until after the reboot.
- **Command Line Failed** - If the command line parameters set in the **Command Line** (page 256) function are incorrect, the patch executable typically displays a dialog box on the managed machine stating there is a command line problem. This error causes patch installation to halt and the patch installation script to terminate. The patch file remains on the managed machine and `Install Failed` is displayed. Enter the correct command line parameters for the patch and try again.

Note: Command line parameters for each patch apply globally and can only be changed by a master administrator.

- **MS Office Command Line Failed** - The only command line parameter permitted for use with Microsoft Office related patches is `/Q`. Because MS Office patches may require the Office installation CD(s), the use of the `/Q` command line parameter might cause the patch install to fail. If an Office related patch fails, remove the `/Q` command line parameter and try again.

Warning: The only switch permitted for use with Microsoft Office 2000, XP, and 2003 related patches (marked as Office) is `/Q`. If `/Q` is not specified, Microsoft Office 2000, XP, and 2003 switches will be reset to `/INSTALL-AS-USER`. Microsoft Office 2003 patches may also include the `/MSOCACHE` switch used to attempt a silent install if the `MSOCache` exists on the machine and the `/INSTALL-AS-USER` switch is set.

- **Patch Download Blocked** - The patch file was never delivered to the machine. The system downloads the patch directly from the internet to either the KServer, a file share, or directly to the managed machine, depending on your **File Source** (page 248) settings. Your firewall may be blocking these downloads. A patch file delivered to the agent with a size of only 1k or 2k bytes is an indication of this problem.
- **User not logged in** - In some cases a user on the machine being patched must be logged in to respond to dialogs presented by the install during the patch. The patch script automatically detects whether a user is currently logged in and will not continue if a user is not logged in. Reschedule the installation of the patch when a user is available and logged in to the machine.
- **Manual install only** - Not a patch failure, but a requirement. Some patches and service packs require passwords or knowledge of a customized setup that the VSA can not know. The VSA does not automatically install patches having the following warnings:

Manual install only

Patch only available only available from Windows Update web site

No patch available; must be upgraded to latest version

These updates must be installed manually on each machine.

Troubleshooting Patch Installation Failures

When patch scan processing reports patch installations have failed, a `KBxxxxxxx.log` and the `WindowsUpdate.log` are uploaded to the KServer. These logs can be reviewed using **Scripts > Get File** (page 59) for a specific machine and can help you troubleshoot patch installation failures. The **Reports > Logs** (page 309) > **Script Log** contains entries indicating these log files have been uploaded to the KServer for each machine.

Scan Machine

Patch Mgmt > Scan Machine

The [Scan Machine](#) page schedules scans to search for missing patches on each managed machine. Scanning takes very little resources and can be safely scheduled to run at any time of day. The scanning operation does not impact users at all.

Scanning Frequency

System and network security depends on all your machines having the latest security hot fixes and patches applied. Patches are released at irregular and unpredictable intervals. To insure your machines are updated you should scan all managed machines on a daily basis.

Scanning the KServer

To scan the KServer, you must install an agent on the KServer. Once installed, you can scan the KServer just like any other managed machine.

Remind me when machines need a patch scan scheduled

If checked, a warning message displays the number of machine IDs not currently scheduled. The number of machine IDs reported depends on the [Machine ID / Group ID filter](#) (*page 17*) and machine groups the administrator is authorized to see using System > [Group Access](#) (*page 385*).

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

Click [Cancel](#) to cancel execution of this task on selected managed machines.

Run Now

Click [Run Now](#) to run this task on selected machine IDs immediately.

Scan every N periods

This task is always performed as a recurring task. Enter the number of times to run this task each time period.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task 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, ...

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.

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.

Patch Management

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Last Scan

This timestamp shows when a machine ID was last scanned. When this date changes, new scan data is available to view.

Next Scan

This timestamp shows the next scheduled scan. The timestamp displays **as red text with yellow highlight** if the scheduled time is in the past.

Interval

The interval for the scheduled task to recur.

Patch Status

Patch > Patch Status

- Similar information is provided using Reports > Patch Management (page 299) and the Patch Status tab of the Machine Summary (page 21) page.

The [Patch Status](#) page provides a summary view of the patch status for each of your managed machines. You can quickly identify machines that are missing patches or are indicating errors. The total of all missing patches is the sum of the [Missing Approved](#), [Missing Denied](#), and [Missing Manual](#).

Patch Test

Most patch problems are the result of configuration and/or permissions issues. The test function exercises the entire patch deployment process without actually installing anything on the target machine or causing a reboot. If a machine ID's operating system does not support patching, the operating system is displayed. The system resets test results every time a machine ID's [File Source](#) (page 248) or [Set Credential](#) (page 371) changes.

Warning: Test cancels any pending patch installs except Initial Updates (page 224).

Note: Machines being processed by Initial Update are *not* tested. The Initial Update status message and date/time is displayed instead of the column totals.

Test

Click [Test](#) to verify patches can update selected machine IDs. Does not actually install any patches.

Cancel

Click [Cancel](#) to stop the test.

Auto Refresh Table

If checked, the paging area is automatically updated every five seconds. This checkbox is automatically selected and activated whenever [Test](#) is clicked.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (*page 476*) displayed is based on the [Machine ID / Group ID filter](#) (*page 17*) and the machine groups the administrator is authorized to see using [System > Group Access](#) (*page 385*).

Install Patches

The number of patches installed.

Missing Approved

The number of approved patches missing.

Missing Denied

The number of unapproved patches missing.

Missing Manual

The number of approved patches missing that must be installed manually. These patches cannot be processed by [Automatic Update](#) (*page 227*) or [Initial Update](#) (*page 224*).

Pending Patches

The number of patches scheduled to be installed.

User Not Logged In

The number of patches not installed because the the patch requires the user to be logged in.

Patch Management

Failed Patches

The number of patches that attempted to install but failed.

Test Results

The status returned after clicking the [Test](#) button:

- Untested
- Pending
- Passed
- Failed

Initial Update

Patch Mgmt > Initial Update

Initial Update is a *one-time* processing of all approved Microsoft patches applicable to a managed machine based on [Patch Policy](#) (page 478). **Initial Update** ignores the [Reboot Action](#) (page 245) policy and reboots the managed machine **without warning the user** as often as necessary until the machine has been brought up to the latest patch level. **Initial Update** should only be performed during non-business hours and is typically performed on newly added machines. See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

Note: The agent for the KServer is not displayed on this page. Initial Update cannot be used on the KServer.\

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 upgrade, 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.

Scripting

Scripts can be configured to be executed just before an **Initial Update** begins and/or after completion. For example, you can run scripts to automate the preparation and setup of newly added machines before or after **Initial Update**. Use Patch Mgmt > [Pre/Post Script](#) (page 226) to configure these scripts on a per-machine basis.

Schedule

Click [Schedule](#) to schedule this task on selected machine IDs using the schedule options previously selected.

Cancel

Click [Cancel](#) to cancel execution of this task on selected managed machines.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (*page 476*) displayed is based on the [Machine ID / Group ID filter](#) (*page 17*) and the machine groups the administrator is authorized to see using [System > Group Access](#) (*page 385*).

Note: Displays the following message if applicable: Not a member of a Patch Policy - All missing patches will be installed!

Scheduled

This timestamp shows the scheduled [Initial Update](#).

Updated

If checked, an [Initial Update](#) has been performed successfully on the machine ID. This timestamp shows when the Status being reported was completed.

Status

During processing, the [Status](#) column displays the following types of messages, if applicable:

- Started
- Processing Windows Installer
- Processing operating system service packs
- Processing operating system update rollups
- Processing operating system critical updates
- Processing operating system non-critical updates
- Processing operating system security updates
- Processing Office service packs

Patch Management

- Processing Office update rollups

Processing Office updates When all processing has been completed, the [Status](#) column displays either:

- Completed - fully patched
- Completed - remaining patches require manual processing

If the latter status displays, select the appropriate machine ID in Patch Mgmt > [Machine Update](#) (page 229) to determine why all patches were not applied. Some patches might require manual install or for the user to be logged in. In the case of patch failures, manually schedule failed patches to be reapplied. Due to occasional conflicts between patches resulting from not rebooting after each individual patch, simply reapplying the patches typically resolves the failures.

Pre/Post Script: Patch Management

Patch Mgmt > Pre/Post Script

Use the [Pre/Post Script](#) page to run scripts either before and/or after [Initial Update](#) (page 224). For example, you can run scripts to automate the preparation and setup of newly added machines before or after [Initial Update](#).

Note: Post scripts run even if there are patch installation failures.

To Run a Pre/Post Script

1. Select machine IDs or [machine ID template](#) (page 477).
2. Click the [select script](#) link to select a script to run before or after [Initial Update](#).
3. Click [Set](#).

Set

Click [Set](#) to run selected scripts before or after an [Initial Update](#) on selected machine IDs.

Run Select Script Before Initial Update Starts

If checked, runs the selected script *before* an [Initial Update](#) on selected machine IDs.

Run Select Script After Initial Update Completes

If checked, runs the selected script *after* an [Initial Update](#) 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled

 The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Pre Script / Post Script

This column lists the scripts set to run before and/or after an [Initial Update](#).

Automatic Update

Patch Mgmt > Automatic Update

The [Automatic Update](#) page is the *preferred* method of updating managed machines with Microsoft patches on a *recurring* basis. [Automatic Update](#) obeys both the [Patch Approval Policy](#) (page 478) and the [Reboot Action](#) (page 245) policy. Use [Initial Update](#) (page 224) if you are installing patches for the first time on a managed machine. See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

- Service packs and patches that require manual intervention are not included in [Automatic Updates](#). These are shown in the [Missing Manual](#) column of the [Patch Status](#) (page 222) page and on the individual [Machine Update](#) (page 229) page.
- Patch installation only occurs when a new missing patch is found by [Scan Machine](#) (page 221).
- [Automatic Update](#) is suspended for a machine while [Initial Update](#) is being processed. [Automatic Update](#) automatically resumes when [Initial Update](#) completes.

Set Auto

Click [Set Auto](#) to schedule an automatic update of new patches on selected machine IDs on a recurring basis.

Daily / Weekly / Monthly / Run Once

Perform this task every day, every week, every month *or one time only*. Weekly displays a day of week drop-down list. Monthly displays a 1-31 drop down list. If a month has fewer days than the day selected, the task is performed on the last day of the month. Use the [Run Once](#) option if you want to run Automatic Update manually on an irregular schedule.

Time

Enter the hour and minute to schedule this task.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task 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, ...

Cancel

Click [Cancel](#) to cancel execution of this task on selected managed machines.

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.

Patch Management

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Note: Displays the following message if applicable: Not a member of a Patch Policy - All missing patches will be installed!

Auto Update Time

The day and time this task is scheduled to recur.

Machine History

Patch Mgmt > Machine History

- Similar information is provided using [Reports > Patch Management](#) (page 299) and the [Patch Status](#) tab of the [Machine Summary](#) (page 21) page.

The [Machine History](#) page displays the results from the most recent patch scan of managed machines. All [installed](#) and [missing](#) patches applicable to a managed machine are listed, regardless of whether the patch is approved or not.

- Click a machine ID link to display its patch history.
- Patches are grouped by [update classification](#) (page 483) first and knowledge base article number second.
- Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.
- Patches classified as security updates have a security bulletin ID (MSYY-xxx). Clicking this link displays the security bulletin.
- The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is Common Windows Component. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

Note: If [Patch location not available](#) is displayed, then the KServer does not know where it can download the patch file executable from. See [Patch Mgmt > Patch Location](#) (page 258) to remedy this.

(Status)

The following status messages can appear next to a patch:

- Installed (date unknown)
- Installed (<datetime>)
- Missing
- Denied by Patch Approval
- Denied (Pending Patch Approval)
- Manual install to VSA database server only - Applies to SQL Server patches on the database server where our database is hosted
- Manual install to KServer only - Applies to Office or any "install-as-user" patches on the KServer
- Patch Location Pending - Applies to patches with an invalid patch location. See [Invalid Patch Location Notification in System > Configure](#) (page 394).
- Missing Patch Location
- Ignore

Superseded Patches

A patch may be superseded and not need to be installed. See [Superseded Patches](#) (page 218) for more information.

Machine Update

Patch Mgmt > Machine Update

- [Print a report of similar information using Reports > Patch Management](#) (page 299).

The [Machine Update](#) page manually installs Microsoft patches on individual machines. [Machine Update](#) overrides the [Patch Approval Policy](#) (page 478) but obeys the [Reboot Action](#) (page 245) policy. If you're using [Automatic Update](#), then [Machine Update](#) is used on an exception basis. [Machine Update](#) is often used to test a new patch prior to approving it for general release to all machines. See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

Using Machine Update

1. Click a machine ID to display all patches missing on that machine. Patches are grouped by [update classification](#) (page 483) first and knowledge base article number second.

The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

1. Optionally click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.
2. Optionally click a [Security Bulletin](#) link to review a security bulletin, if available. Patches classified as security updates have a security bulletin ID (`MSYY-xxx`).
3. Check the box next to patches you want installed on the selected machine ID.
4. Select install parameters.
5. Click the [Schedule](#) button to install patches using the install parameters.
6. Click the [Cancel](#) button to remove any pending patch installs.

Superseded Patches

A patch may be superseded and not need to be installed. See [Superseded Patches](#) (page 218) for more

Patch Management

information.

Schedule

Click [Schedule](#) to schedule the update of selected missing patches on a machine ID using the schedule options previously selected.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click [Cancel](#) to cancel execution of this task on selected managed machines.

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.

Hide patches denied by Patch Approval

If checked, hides patches denied patch approval. Patches with the status `Pending Approval` are considered denied by [Patch Update](#).

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.

(Status)

The following status messages can appear next to a patch:

- Pending
- Install Failed - See [Patch Failure](#) (page 219).
- Awaiting Reboot
- User not logged in
- User not ready to install
- Install Failed - Missing Network Credential
- Install Failed - Invalid Network Credential or LAN Server Unavailable
- Install Failed - Invalid Credential
- Missing
- Denied by Patch Approval
- Denied (Pending Patch Approval)
- Manual install to VSA database server only - Applies to SQL Server patches on the database server where our database is hosted
- Manual install to KServer only - Applies to Office or any "install-as-user" patches on the KServer
- Patch Location Pending - Applies to patches with an invalid patch location. See [Invalid Patch Location Notification](#) in System > [Configure](#) (page 394).
- Missing Patch Location
- Ignore

Patch Update

Patch Mgmt > Patch Update

- [Print a report of similar information using Reports > Patch Management \(page 299\)](#).

The [Patch Update](#) page updates missing Microsoft patches on all machines displayed in the paging area. [Patch Update](#) overrides the [Patch Approval Policy \(page 478\)](#) but obeys the [Reboot Action \(page 245\)](#) policy. If you're using [Automatic Update](#), then [Patch Update](#) is used on an exception basis to apply individual patches to multiple machines or to re-apply patches that originally failed on certain machines. See [Methods of Updating Patches \(page 217\)](#), [Configuring Patch Management \(page 217\)](#), [Patch Processing \(page 218\)](#), [Update Classification \(page 219\)](#) and [Patch Failure \(page 219\)](#) for a general description of patch management.

Patches Displayed

The display of patches on this page are based on:

- The [Machine ID/Group ID filter \(page 477\)](#).
- The patches reported using [Scan Machine \(page 221\)](#). Managed machines should be scanned daily.
- The patches of machines using [Automatic Update \(page 227\)](#). If the [Hide machines set for Automatic Update](#) box is checked, these patches are *not* listed here. These patches are automatically applied at the [Automatic Update](#) scheduled time for each machine.
- If the [Hide patches denied by Patch Approval](#) box is checked, patches that are denied or pending approval are not listed here.
- The patches of machines being processed by [Initial Update \(page 224\)](#). These patches are excluded from this page until [Initial Update](#) completes.

Duplicate Entries

Microsoft may use a common knowledge base article for one or more patches, causing patches to appear to be listed more than once. [Patch Update](#) displays patches sorted by [Update Classification](#) or [Product](#) first and knowledge base article number second. Check the [Product](#) name or click the [KB Article](#) link to distinguish patches associated with a common knowledge base article.

Superseded Patches

A patch may be superseded and not need to be installed. See [Superseded Patches \(page 218\)](#) for more information.

Using Patch Update

1. Optionally click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.
2. Patches classified as security updates have a security bulletin ID (MSYY-xxx). Optionally click the [Security Bulletin](#) link to review the security bulletin, if available.
3. Optionally click the box next to a [KB Article](#) to schedule that patch on all managed machines missing that patch.
4. Optionally click the [Machines...](#) button to schedule a patch on individual machines or to set machines to ignore a patch. The [Ignore](#) setting applies to the selected patch on the selected machines. If [Ignore](#) is set, the patch is considered [Denied](#). Patches marked as [Ignore](#) on the selected machines cannot be installed by any of the installation methods. To be installed, the [Ignore](#) setting must be cleared.

Note: A warning icon  indicates the patch status for one or more machines should be checked before installing this patch. Click the [Machines](#) button and review the [Status](#) column for each machine missing this patch.

Patch Management

5. Select install parameters.
6. Click the [Schedule](#) button to install the patches using the install parameters.
7. Click the [Cancel](#) button to remove any pending patch installs.

Hide machines set for Automatic Update

If checked, hides patches missing from machine IDs set to [Automatic Update](#) (page 227).

Hide patches denied by Approval Policy

If checked, hides patches denied by [Patch Approval Policy](#) (page 478).

Patch Group By

Display patch groups by [Classification](#) or [Product](#).

Schedule

Click [Schedule](#) to schedule a update of selected patches on all machine IDs missing this patch, using the schedule options previously selected.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click [Cancel](#) to cancel execution of this task on selected managed machines.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task 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, ...

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.

Show Details

Click the [Show Details](#) checkbox to display the expanded title and installation warnings, if any, of each patch.

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.

Status Warning Icon

A warning icon  indicates the patch status for one or more machines should be checked before installing this patch. Click the [Machines](#) button and review the [Status](#) column for each machine missing this patch.

Machines...

Click [Machines...](#) to list all machines missing this patch. On the details page, the following status messages can appear next to a patch:

- Pending

- Install Failed - See [Patch Failure](#) (page 219).
- Awaiting Reboot
- User not logged in
- User not ready to install
- Install Failed - Missing Network Credential
- Install Failed - Invalid Network Credential or LAN Server Unavailable
- Install Failed - Invalid Credential
- Missing
- Denied by Patch Approval
- Denied (Pending Patch Approval)
- Manual install to VSA database server only - Applies to SQL Server patches on the database server where our database is hosted
- Manual install to KServer only - Applies to Office or any "install-as-user" patches on the KServer
- Patch Location Pending - Applies to patches with an invalid patch location. See [Invalid Patch Location Notification](#) in System > [Configure](#) (page 394).
- Missing Patch Location
- Ignore

KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

Missing

The number of machines missing this patch.

Auto

Displays only if the [Hide machines set for Automatic Update](#) box is *not* checked. The number of machines scheduled to install this patch by [Automatic Update](#).

Ignore

The number of machine set to ignore a patch using the [Machines](#) button. The [Ignore](#) setting applies to the selected patch on the selected machines. If [Ignore](#) is set, the patch is considered [Denied](#). Patches marked as [Ignore](#) on the selected machines cannot be installed by any of the installation methods. To be installed, the [Ignore](#) setting must be cleared.

Product

The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is [Common Windows Component](#). Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

Update Classification

See [Update Classification](#) (page 219) for an explanation of [Classification](#) and [Type](#).

Rollback

Patch Mgmt > Rollback

The [Rollback](#) page removes patches after they have been installed on a system. Not all patches may be uninstalled. The system only lists patches supporting the rollback feature. Patches are grouped by [update classification](#) (page 483) first and knowledge base article number second. Includes the date the patch was installed, if available.

Warning: Removing Windows software in the wrong order may cause the operating system to stop functioning.

Follow these steps to remove a patch from any managed machine:

1. Click the machine ID that you want to remove a patch from.
2. Check the box to the left of the patch you want to uninstall.
3. Specify the date and time to perform the rollback operation.
4. Click the [Rollback](#) button.

Rollback

Click [Rollback](#) to schedule a update of selected machine IDs using the schedule options previously selected.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click [Cancel](#) to clear a scheduled rollback.

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.

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.

KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

Security Bulletin

The security bulletin associated with a patch. Patches classified as security updates have a security bulletin ID (MSyy-xxx). Click the [Security Bulletin](#) link to review the security bulletin, if available.

Cancel Updates

Patch Mgmt > Cancel Updates

The [Cancel Updates](#) page clears all *pending* patch installations on selected machine IDs.

Note: Use the [Patch Update \(page 231\)](#) page to cancel the pending update of a specific patch on all machines.

Warning: This page also cancels initial updates ([page 224](#)).

Warning: If an installation script has already begun, Cancel Updates might not stop the script from running.

Cancel

Click [Cancel](#) to clear **all** pending patch installations on selected machine IDs.

Show Patch List

Check this box to list all *pending patch IDs* on each machine ID in the [Pending Update Install Status](#) column. If unchecked, the *total number of pending patches* are listed for each machine ID.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs \(page 476\)](#) displayed is based on the [Machine ID / Group ID filter \(page 17\)](#) and the machine groups the administrator is authorized to see using [System > Group Access \(page 385\)](#).

Create/Delete: Patch Policy

Patch Mgmt > Patch Policy: Create/Delete

The [Create/Delete](#) page creates or deletes patch policies. Patch policies contain all active patches for the purpose of approving or denying patches. An active 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*.

Patch Management

- 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 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](#) (page 224) and [Automatic Update](#) (page 227) require patches be approved before these patches are installed.
- [Approval by Policy](#) (page 238) approves or denies patch by *policy*.
- [Approval by Patch](#) (page 240) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- [KB Override](#) (page 242) 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](#) (page 231) and [Machine Update](#) (page 229) can install denied patches.
- Standard administrators can only see patch policies they have created or patch policies that have machine IDs the administrator is authorized to see based on the administrator roles they are assigned.

Create

Click [Create](#) to to define a new patch policy, after entering a new machine patch policy name in the edit field.

Delete

Click [Delete](#) to delete selected patch policies.

Enter name for a new patch policy

Enter the name for a new patch 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.

Edit Icon

Click the edit icon  to the left of a patch policy to rename it.

Policy Name

Lists all machine patch policies defined for the entire system.

Member Count

Lists the number of machines that are members of each patch policy.

Show Machines

Click [Show Machines](#) to list the members of a patch policy.

Membership: Patch Policy

[Patch Mgmt](#) > [Patch Policy: Membership](#)

The [Membership](#) page assigns machine IDs to one or more patch policies. Patch policies contain all active patches for the purpose of approving or denying patches. An active 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 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](#) (page 224) and [Automatic Update](#) (page 227) require patches be approved before these patches are installed.
- [Approval by Policy](#) (page 238) approves or denies patch by *policy*.
- [Approval by Patch](#) (page 240) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- [KB Override](#) (page 242) 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](#) (page 231) and [Machine Update](#) (page 229) can install denied patches.

Standard administrators can only see patch policies they have created or patch policies that have machine IDs the administrator is authorized to see based on the administrator roles they are assigned.

Add

Click [Add](#) to add selected machine IDs to selected patch policies.

Remove

Click [Remove](#) to remove selected machine IDs from selected patch policies.

Assign machines to a patch policy

Click one or more patch policy names to mark them for adding or removing from selected machine IDs.

Always show all Patch Policies to Standard Administrators

If checked, standard administrators can see all patch policies. This allows standard administrators to deploy patch policies, even if they did not create the patch policies and don't have machines yet that use them. If blank, standard administrators only see patch policies that contain machines to which they have access or those which they created. Master administrators always see all patch policies. This option only displays for [master administrators](#) (page 469).

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Policy Membership

Displays a comma separated list of patch policies that each machine ID is a member of.

Approval by Policy

Patch Mgmt > Approval by Policy

The [Approval by Policy](#) page approves or denies the installation of Microsoft patches on managed machines by *patch policy*. Patches pending approval are considered denied until they are approved. This gives you the chance to test and verify a patch in your environment before the patch automatically pushes out. See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

Setting Patch Approval Policies

Patch policies contain all active patches for the purpose of approving or denying patches. An active 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 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](#) (page 224) and [Automatic Update](#) (page 227) require patches be approved before these patches are installed.
- [Approval by Policy](#) (page 238) approves or denies patch by *policy*.
- [Approval by Patch](#) (page 240) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- [KB Override](#) (page 242) 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](#) (page 231) and [Machine Update](#) (page 229) can install denied patches.
- Standard administrators can only see patch policies they have created or patch policies that have machine IDs the administrator is authorized to see based on the administrator roles they are assigned.

Superseded Patches

A patch may be superseded and not need to be installed. See [Superseded Patches](#) (page 218) for more information.

Policy

Select a patch policy by name from the drop-down list.

Save As...

Click [Save As...](#) to save the currently selected patch policy to a new policy with identical settings. All patch approval/denial statuses are copied as are the default approval statuses for the policy. Machine membership is *not* copied to the new policy.

Copy Approval Statuses to Policy <Policy> / Copy Now

Select a policy to copy approval statuses *to*, from the currently selected policy. Then click [Copy Now](#). This enables you to perform patch testing against a group of test machines using a test policy. Once testing has been completed and the patches have been approved or denied, use the copy feature to copy only the approved or denied statuses from the test policy to a production policy.

Policy View / Group By

Display patch groups by classification or product.

Patch Approval Policy Status

This table displays the approval status of patches by [update classification](#) (page 483) or product group. [Approved](#), [Denied](#), [Pending Approval](#), and [Totals](#) statistics are provided for each update classification or product group.

Select a [Default Approval Status](#) for any category for this patch policy. Newly identified patches for this patch policy are automatically set to this default value. Choices include:

-  - Approved
-  - Denied
-  - Pending Approval

Note: If the same patch is assigned two different Default Approval Status settings—one by update classification *and* the other by product group—then the more restrictive of the 2 defaults has precedence: Denied over Pending Approval over Approved.

Click any link in this table to display a [Patch Approval Policy Details](#) page listing individual patches and their approval status. The list is filtered by the type of link clicked:

- [Classification](#) or [Product](#)
- [Approved](#)
- [Denied](#)
- [Pending Approval](#)

Totals In the [Patch Approval Policy Details](#) page you can:

- Approve or deny approval of patches individually.
- Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

Note: Microsoft may use a common knowledge base article for one or more patches, causing patches to appear to be listed more than once. Check the Product name or click the KB Article link to distinguish patches associated with a common knowledge base article.

- Click the [Security Bulletin](#) link to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSYY-xxx).
- The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.
- See [Update Classification](#) (page 219) for an explanation of [Classification](#) and [Type](#).
- Click the [Show Details](#) checkbox to display the expanded title, patch status notes and installation warnings, if any, of each patch.
- Click [Filter...](#) to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

Patch Management

- Optionally add a note, up to 500 characters, using [Patch Status Notes](#). The note is added when the [Approve](#) or [Deny](#) buttons are selected. If the text box is empty when the [Approval](#) or [Deny](#) buttons are selected, the note is removed for selected patches.

Override Default Approval Status with Denied for "Manual Install Only" updates in this policy

If checked, all existing and future `Manual Install Only` updates are set to denied for this policy.

Override Default Approval Status with Denied for "Windows Update Web Site" updates in this policy

If checked, all existing and future `Windows Update Web Site` updates are set to denied for this policy.

Note: Checking these two override checkboxes has a *one-time effect* on existing patches for these two categories of patches. If you approve an *existing* patch for one of these two categories *after* checking these boxes, the patch will remain approved regardless of the settings of these two checkboxes. Future patches will continue to default to denied.

Approval by Patch

Patch Mgmt > Approval by Patch

The [Approval by Patch](#) page approves or denies the installation of Microsoft patches on managed machines by *patch* for *all* patch policies. This page only displays for [master administrators](#) (page 469). Changes affect patches installed by all administrators. This saves you the trouble of approving pending patches separately for each patch policy. See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

Setting Patch Approval Policies

Patch policies contain all active patches for the purpose of approving or denying patches. An active 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 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](#) (page 224) and [Automatic Update](#) (page 227) require patches be approved before these patches are installed.
- [Approval by Policy](#) (page 238) approves or denies patch by *policy*.
- [Approval by Patch](#) (page 240) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- [KB Override](#) (page 242) 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](#) (page 231) and [Machine Update](#) (page 229) can install denied patches.

- Standard administrators can only see patch policies they have created or patch policies that have machine IDs the administrator is authorized to see based on the administrator roles they are assigned.

Superseded Patches

A patch may be superseded and not need to be installed. See [Superseded Patches](#) (page 218) for more information.

Patch Status Notes

Optionally add a note, up to 500 characters, using [Patch Status Notes](#). The note is added when the [Approve](#) or [Deny](#) buttons are selected. If the text box is empty when the [Approval](#) or [Deny](#) buttons are selected, the note is removed for selected patches.

Approve

Click [Approve](#) to approve selected patches for all patch policies.

Deny

Click [Deny](#) to deny selected patches for all patch policies.

Show Details

Check [Show Details](#) to display multiple rows of information for all patches. This includes the title of a patch, the number of patch policies that have been approved, denied, or are pending approval for a patch, patch status notes, and installation warnings, if any.

Filter...

Click [Filter...](#) to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

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.

KB Article

Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

Note: Microsoft may use a common knowledge base article for one or more patches, causing patches to appear to be listed more than once. Check the Product name or click the KB Article link to distinguish patches associated with a common knowledge base article.

Security Bulletin

Click the [Security Bulletin](#) link to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSYY-xxx).

Product

The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

Classification / Type

See [Update Classification](#) (page 219) for an explanation of [Classification](#) and [Type](#).

Published

The date the patch was released.

Language

The language the patch applies to.

KB Override

Patch Mgmt > KB Override

The [KB Override](#) page sets overrides of the *default* approval status of patches set using [Approval by Policy](#) (page 238) by *KB Article* for *all* patch policies. It also sets the approval status for *existing* patches by *KB Article* for all patch policies. This page only displays for [master administrators](#) (page 469). Changes affect patches in *all* patch policies installed by *all* administrators. See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

For example, KB890830, "The Microsoft Windows Malicious Software Removal Tool" is released monthly. If you decide to approve all patches associated with this KB Article using KB Override, then not only are existing patches approved but all *new* patches associated with this KB article are automatically approved each month the new patch is released.

Setting Patch Approval Policies

Patch policies contain all active patches for the purpose of approving or denying patches. An active 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 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](#) (page 224) and [Automatic Update](#) (page 227) require patches be approved before these patches are installed.
- [Approval by Policy](#) (page 238) approves or denies patch by *policy*.
- [Approval by Patch](#) (page 240) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- [KB Override](#) (page 242) 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](#) (page 231) and [Machine Update](#) (page 229) can install denied patches.
- Standard administrators can only see patch policies they have created or patch policies that have machine IDs the administrator is authorized to see based on the administrator roles they are assigned.

KB Article

Enter the KB Article to approve or deny.

Note: See [Approval by Policy \(page 238\)](#) or [Approval by Patch \(page 240\)](#) for a listing of all available KB Articles.

Approve

Click [Approve](#) to approve patches associated with this KB Article. Multiple patches can be associated with a KB Article.

Deny

Click [Deny](#) to deny patches associated with this KB Article. Multiple patches can be associated with a KB Article.

KB Article

Click the [KB Article](#) link to display the knowledge base article.

Override Status

Approved or Denied. Applies to all patches associated with this KB Article.

Admin

The administrator who approved or denied patches associated with this KB Article.

Changed

The date and time the administrator approved or denied patched associated with this KB Article.

Windows Auto Update

Patch > [Windows Auto Update](#)

The [Windows Auto Update](#) page determines whether [Windows Automatic Updates](#) on managed machines is disabled, left for the user to control, or configured.

Window Automatic Updates

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, and Windows 2000 SP3 or later. While Windows Millennium Edition (Me) has an Automatic Updates capability, it cannot be managed as the above operating systems can. Patch Mgmt > [Windows Auto Update \(page 243\)](#) can enable or disable this feature on managed machines.

Windows Automatic Update Cannot Use Template Accounts

Windows Automatic Updates is one feature that cannot be preconfigured in a [machine ID template \(page 477\)](#). This is because Windows Automatic Updates is only supported on Windows 2000 SP3/SP4, Windows XP, and Windows Server 2003. Since a machine ID template cannot have a specified operating system, a setting for this feature cannot be stored in the machine ID template. Also, we need to know the machine's current settings before we can override those settings. The current settings are obtained when a [Scan Machine \(page 221\)](#) is performed.

Note: A checkbox does not display for any machine that either has an operating system that does not support Windows Automatic Updates or for which an initial Scan Machine has not been completed.

Patch Management

For Windows XP SP2 machines: Whenever an administrator disables or forces a specific configuration for Windows Automatic Updates, a registry setting is updated to prevent the bubble warning from the Security Center icon in the system tray to be displayed for Windows Automatic Updates. This is done to avoid end-user confusion since the end-user will not be able to make any changes to the Windows Automatic Updates configuration. It is possible that some anti-malware tools will see this registry setting change as an attempt by malware to eliminate the user warning and therefore will reset the warning to "on".

Disable

Select [Disable](#) to disable Windows Automatic Updates on selected machine IDs and let [Patch Management](#) control patching of the managed machine. Overrides the existing user settings and disables the controls in Windows Automatic Updates so the user *cannot* change any of the settings. Users can still patch their systems manually.

User Control

Let machine users enable or disable Windows Automatic Updates for selected machine IDs.

Configure

Forces the configuration of Windows Automatic Updates on selected machine IDs to the following settings. Overrides the existing user settings and disables the controls in Windows Automatic Updates so the user *cannot* change any of the settings. Users can still patch their systems manually.

- [Notify user for download and installation](#) - Notifies the user when new patches are available but does not download or install them.
- [Automatically download and notify user for installation](#) - Automatically downloads updates for the user but lets the user choose when to install them.
- [Automatically download and schedule installation](#) - Automatically downloads updates and installs the updates at the scheduled time.

Schedule every day / <day of week> at <time of day>

Applies only if [Automatically download and schedule installation](#) is selected. Perform this task every day or once a week at the specified time of day.

Force auto-reboot if user is logged on

Optionally check the box next to [Force auto-reboot if user is logged on](#). By default, [Windows Auto Update](#) does *not* force a reboot. [Reboot Action](#) ([page 245](#)) settings do not apply to [Windows Auto Update](#).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled

 The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Machine Updated

Displays the status of configuring Windows Automatic Updates on selected machine IDs using this page.

- Pending - Windows Automatic Updates is being configured on the selected machine ID.
- Timestamp - The date and time Windows Automatic Updates was configured on the selected machine ID.

Windows Automatic Update Configuration

The Windows Automatic Update configuration assigned to each selected machine ID.

Note: If the Windows Automatic Update Configuration column displays `Automatic Update not initialized on machine`, the user must select the Windows Automatic Updates icon in the system tray to run the Windows Automatic Updates Setup wizard to setup Windows Automatic Updates.

Reboot Action

Patch Mgmt > Reboot Action

The [Reboot Action](#) page defines how reboots are performed after a patch install. Patch installs do not take effect until after a machine is rebooted. The [Reboot Action](#) policy applies to [Machine Update](#) (page 229), [Patch Update](#) (page 231) and [Automatic Update](#) (page 227). It does *not* apply to [Initial Update](#) (page 224). See [Methods of Updating Patches](#) (page 217), [Configuring Patch Management](#) (page 217), [Patch Processing](#) (page 218), [Update Classification](#) (page 219) and [Patch Failure](#) (page 219) for a general description of patch management.

Warning: It is strongly recommended that the Reboot Action for the agent on the KServer be set to `Do not reboot after update`! Automatic rebooting of the KServer can have adverse effects on other KServer processes!

The patch installation script runs at the scheduled time and performs the following steps:

- Downloads, or copies from a file share, all the patch files to a local drive, typically the same drive the agent is installed on.
- Executes each patch file, one at a time.
- Performs a reboot of the machine, as specified by this page.

Note: If you schedule multiple patches for installation on the same machine, all the patches are installed at the same time. After all the patches have been installed the machine reboots once. This technique saves time and reboots.

Note: Service packs are always installed separately. If you are installing a service pack with other patches you will see a reboot after the service pack install and then another single reboot after all the other patches are installed.

Apply

Click [Apply](#) to apply the selected [Reboot Action](#) radio option to selected machine IDs.

Patch Management

Reboot immediately after update.

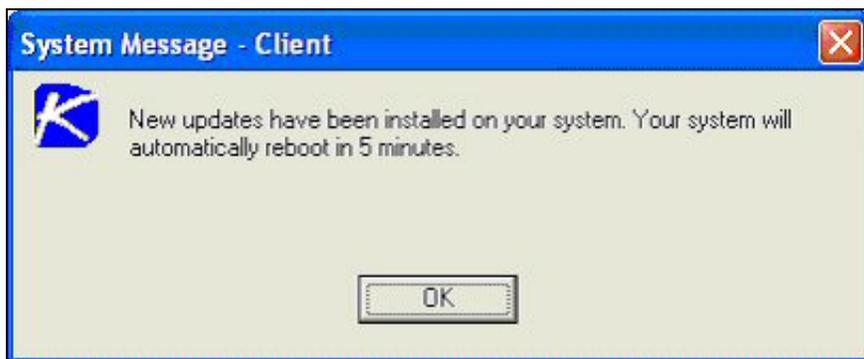
Reboots the computer immediately after the install completes.

Reboot <day of week> at <time of day> after install.

After the patch install completes the computer is rebooted at the selected day of week and time of day. Use these settings to install patches during the day when users are logged in—to get the UNC path—then force a reboot in the middle of the night. Selecting **every day** reboots the machine at the next specified time of day following the patch installation.

Warn user that machine will reboot in N minutes (without asking permission).

When the patch install completes, the message below pops open warning the user and giving them a specified number of minutes to finish up what they are doing and save their work. If no one is currently logged in, the system reboots immediately.

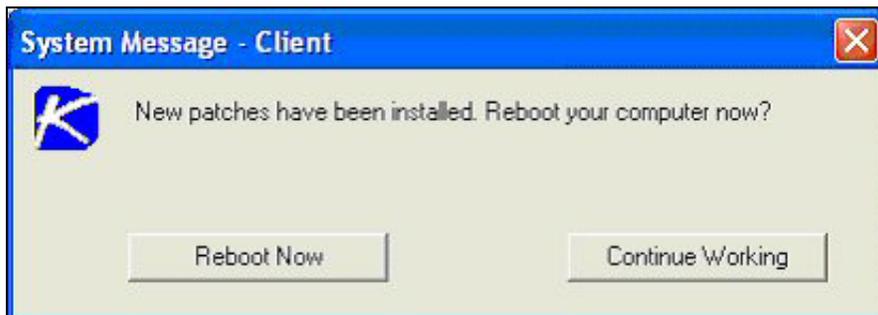


Skip reboot if user logged in.

If the user is logged in, the reboot is skipped after the patch install completes. Use this setting to avoid interrupting your users. This is the default setting.

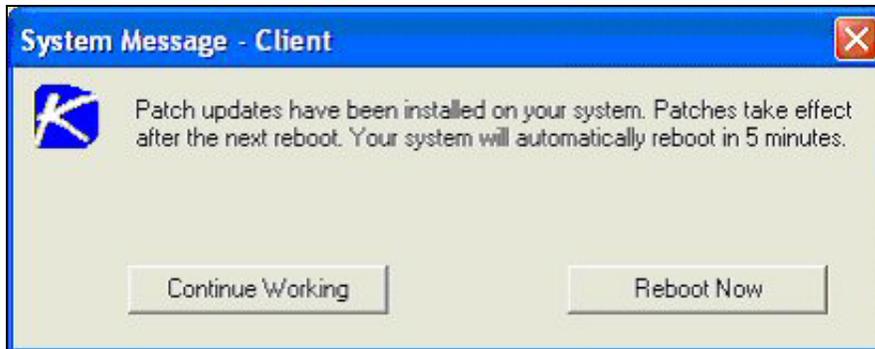
If user logged in ask to reboot every N minutes until the reboot occurs.

This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer or they answer no, the same message appears every N minutes repeatedly, until the system has been rebooted. If no one is currently logged in, the system reboots immediately.



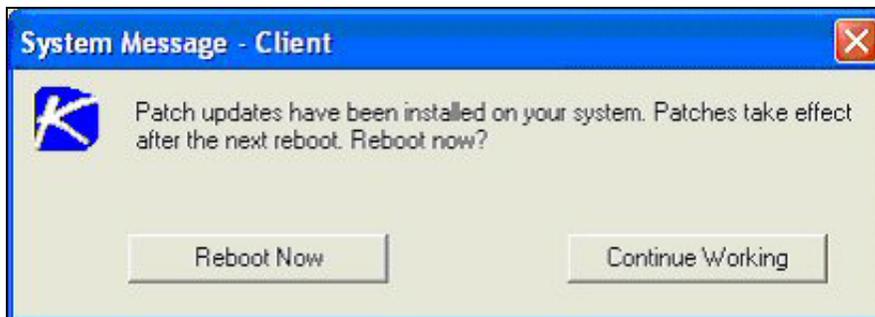
If user logged in ask permission. Reboot if no response in N minutes. Reboot if user not logged in.

This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, it reboots automatically after N minutes *without saving* any open documents. If no one is currently logged in, the system reboots immediately.



If user logged in ask permission. Do nothing if no response in N minutes. Reboot if user not logged in.

This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, the reboot is skipped. If no one is logged in, reboot immediately.



Do not reboot after update

Does not reboot. Typically used if the machine is a server and you need to control the reboot. You can be notified via email when a new patch has been installed by checking [Email when reboot required](#) and filling in an email address.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete

Patch Management



The agent is online but remote control is disabled



The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Reboot Action

The type of reboot action assigned to each machine ID.

File Source

Patch Mgmt > File Source

The [File Source](#) page defines where each machine gets patch executable files from prior to installation and where these patch executables are copied to on the local machine. File source locations include:

- The internet
- The KServer
- A file share

Note: Selecting the File share located on option below affects where Backup and Disaster Recovery and Kaseya Endpoint Security is installed from.

Note: Patch download links with a `.cab` extension are always downloaded directly from the Internet, regardless of the File Source setting.

Apply

Click [Apply](#) to apply the selected patch source option to selected machine IDs.

Copy packages to temp directory on local drive with most free space

Patches are downloaded, or copied from a file share, to the managed machine's hard disk. Several patches, especially service packs, may require significant additional local disk space to completely install. Check this box to download patches to the temporary directory specified in [Temp Directory](#) (page 366), but use the drive on the managed machine with the most free disk space. Uncheck this box to always use the drive specified in [Temp Directory](#) for the machine ID.

Delete package after install (from temp directory)

The install package is typically deleted after the install to free up disk space. Uncheck this box to leave the package behind for debugging purposes. If the install fails and you need to verify the [Command Line](#) (page 256) switches, do not delete the package so you have something to test with. The package is stored in the temporary directory specified in [Temp Directory](#) on the drive specified in the previous option.

Download from Internet

Each managed machine downloads the patch executable file directly from the internet at the URL specified in [Patch Location](#) (page 258).

Pulled from system server

First the KServer checks to see if it already has a copy of the patch file. If not, the new patch executable is downloaded automatically and stored on the KServer, then used for all subsequent

distributions to managed machines. When a patch needs to be installed on a managed machine, this patch file is pushed to that machine from the KServer.

Note: The default location for patch files stored on the KServer is
 C:\Kaseya\WebPages\ManagedFiles\VSAPatchFiles\

Clear Cache

Click [Clear Cache](#) to clear all downloaded patches stored on the KServer.

Pulled from file server using UNC path

This method can be best if you support many machines on the same LAN. The patch executable file is copied from a file share accessible to a managed machine.

1. Use the [Machine Group Filter](#) drop-down list to select a group ID.
2. Select a machine ID from the [File share located on](#) drop down list.
3. Enter the file share name in the [in local directory](#) field.

Note: The value in the [in local directory](#) field must be in full path format, such as `c:\shareddir\dir`. The value in the [Pulled from file server using UNC path](#) must be in UNC format such as `\\computername\sharedname\dir\`.

- First the KServer checks to see if the patch file is already in the file share. If not, the agent automatically loads the patch file either directly from the internet, or gets it from the KServer. In either case, the managed machine with the file share **must have an agent** on it.
 4. [File Server automatically gets patch files from](#) - Select one of the following options:
 - [the Internet](#) - Use this setting when the managed machine running the file share has full internet access.
 - [the system server](#) - Use this setting when the managed machine running the file share is blocked from getting internet access.
 5. [Download from Internet if machine is unable to connect to the file server](#) - Optionally check this box to download from the internet. A bad network credential, for example, may prevent a machine from connecting to the file server. This is especially useful for laptops that are disconnected from the company network but have internet access.
 6. After the patch file has been downloaded *to* the file share, the agent on the managed machine being patched connects to the file share to download the patch *from* the file share. A user credential is required to connect to the file share. Two methods are available:
 - [Set Credential](#) - If a [credential](#) (*page 371*) has been specified for machine ID with the file share, the patch install script uses that credential to access the file share and to install the patch files.
 - [User Logged In](#) - If a credential has **not** been set for this machine ID, then a user **must be logged in** during the install process in order for the agent to connect to the remote file share.
- The patch file is then downloaded from the file share and installed 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:

Patch Management

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Patch Source

Lists the patch source selected for each machine ID. A [Clear Cache](#) button displays in this column if the [Pulled from file server using UNC path](#) option is selected for a machine ID. Clicking this [Clear Cache](#) button clears patches from the specified file server UNC path. The [Clear Cache](#) button is *not* machine specific. All patches stored on that file server for the specified path will be deleted.

Patch Alert

[Patch Mgmt](#) > [Patch Alert](#)

[Monitor](#) > [Alerts](#) (page 100)

Select [Patch Alert](#) from the [Select Alert Function](#) drop-down list. The [Patch Alert](#) page creates 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.

Passing Alert Information to Emails and Scripts

The following types of monitoring alert emails can be sent and formatted:

- New Patch Available
- Path to Patch Executable Missing - Enabled by selecting the *first* row in the paging area, called [Patch Location Missing](#), and clicking the [Apply](#) button.
- Patch Install Failed
- Patch Approval Policies Updated - Enabled by selecting the *second* row in the paging area, called [Patch Location Missing](#), and clicking the [Apply](#) button.
- Agent Credential Invalid
- Windows Auto Update Configuration Changed

To Create a Patch Alert

1. Check any of these checkboxes to perform their corresponding actions when a an alarm 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 Scripts

The following types of patch alert emails can be sent and formatted:

- New Patch Available
- Path to Patch Executable Missing
- Patch Install Failed
- Patch Approval Policies Updated
- Agent Credential Invalid
- 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 in scripts.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<au>	#au#	auto update change
<bi>	#bi#	bulletin ID
<bl>	#bl#	new bulletin list
<db-view.column>	not available	Include a view.column (page 415) 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 alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > [Dashboard List](#) (page 88), Monitor > [Alarm Summary](#) (page 96) and Reports > [Logs](#) (page 309) > Alarm Log.

Patch Management

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in administrator displays in the [Email Recipients](#) field. It defaults from System > [Preferences](#) (page 377).
- 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 alarm condition is encountered.
- 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 [Removed](#) is clicked, all email addresses are removed [without modifying any alert parameters](#).
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the [From Address](#) using System > [Configure](#) (page 394).

Apply

Click [Apply](#) to apply alert 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 triggers an alarm whenever the system discovers one of three different patch alert conditions for a selected machine ID:

- [New patch is available](#)
- [Patch install fails](#)
- [Agent credential is invalid or missing](#)
- [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:



Agent has checked in



Agent has checked in and user is logged on. Tool tip lists the logon name.

-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Patch Location Missing

Displays as the first row of data. If selected and the [Apply](#) button clicked, an alert is generated if the system discovers the [Patch Location](#) (page 258) path for a patch is missing. This is a system alert and not associated with any machines.

Approval Policy Updated

Displays as the second row of data. If selected and the [Apply](#) button clicked, an alert is generated when a new patch is added to all patch policies. See [Patch Approval Policy](#) (page 478). This is a system alert and not associated with any machines.

ATSE

The ATSE response code assigned to machine IDs:

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- 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 Mgmt > [Windows Auto Update](#) (page 243).

Note: A log entry in the machine's Configuration Changes log is made regardless of this alert setting.

Office Source

Patch Mgmt > Office Source

The [Office Source](#) page sets *alternate* source locations for installing Office and Office component applications. The source location can be changed from the default CD-ROM, which is the typical installation source, to a network share or a directory on a local hard drive. By changing the installation source to a network share or a local directory, those patches that require the Office installation source for installation can get access **without prompting the user for the installation media**. This alternate source location can be configured to be read-only. It must contain an exact copy of the installation media contents including all hidden files and/or directories.

An Office source for a managed machine is only available after you have run [Scan Machine](#) (*page 221*) at least once for the managed machine. Machine IDs are displayed on this page only if they:

- Currently match the [Machine ID / Group ID filter](#) (*page 17*).
- Have Office or Office component applications installed for Office 2000, XP, or 2003.

Note: Office 2007 is not displayed on this page. Office 2007 installs a full set of source installation files on a machine, so an alternate source location is not required.

Multiple Entries

Multiple entries may be displayed for a machine because the machine contains one or more Office component applications, such as FrontPage or Project, that were installed separately from their own installation source and were not part of the Office installation.

Credential Required

Managed machines must have a [credential set](#) (*page 371*) to use the Office Source page. The agent must have a credential to use the alternate Office source location.

Validation

The specified location is validated to be sure that the location is accessible from the machine and that the installation source in the specified location contains the correct edition and version of Office or the Office component application. Only after the validation succeeds is the machine's registry modified to use the specified location.

Installing Office Products

Some patches—particularly Office service packs—still display progress dialogs even though the silent installation switch (/Q) is included using Patch Mgmt > [Command Line](#) (*page 256*). These progress dialogs do not require any user intervention.

Some patches and service packs display a modal dialog indicating the update has completed, again even though the silent installation switch (/Q) is used. This requires the user to click on the OK button to dismiss the dialog. Until this happens, the patch installation script appears to be hung and will not complete until this dialog is dismissed!

Some Office service packs fail for no apparent reason. Checking the machine's application event log reveals that another Office component service pack failed. This has been observed with Office 2003 service pack 2 requiring the availability of FrontPage 2003 service pack 2. When the Office source location for the FrontPage 2003 is configured, the Office 2003 service pack 2 finally successfully installs.

Filter on Office Product

Because each managed machine may be listed multiple times—once for each Office product or Office component application installed—you can filter the Office products/components displayed. This ensures selecting the same product code for multiple machines when setting the installation source location.

Apply

Click [Apply](#) to apply the Office source location specified in [Location of Office installation source](#) to selected machine IDs.

Location of Office installation source

Add the network share as a UNC path (i.e., [\\machinename\sharename](#)) or a local directory as a fully qualified path (i.e., `C:\OfficeCD\Office2003Pro`) in the installation source text box.

Reset

Click [Reset](#) to restore selected machine IDs back to their original installation source, typically the CD-ROM.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (*page 476*) displayed is based on the [Machine ID / Group ID filter](#) (*page 17*) and the machine groups the administrator is authorized to see using `System > Group Access` (*page 385*).

Status

Displays one of the following:

- Missing Credential
- Update Script Failed
- Validation Script Failed
- Original Source
- Pending Validation
- Updating Machine
- Incorrect Edition
- Processing Error
- Restoring Original
- Office Source Updated

Office Product

Displays the name of the Office product.

Office Source

Displays the current installation source location for this Office product on this machine ID.

Product Code

Displays the Office product code.

Command Line

Patch Mgmt > Command Line

The [Command Line](#) page defines the command line switches used to silently install a specified patch. Occasionally a patch is released that does not use normal switch settings or the patch database has not been updated with the new switches. If you find a patch does not successfully install with its assigned switch settings, you can change them with this page. Locate patch switches by clicking the [KB Article](#) link and reading through the knowledge base article.

Warning: Changes to the switches effect all administrators. Only a master administrator can access this page.

Suppress Automatic Reboot

Usually you want to load a patch without requiring any user interaction at all. The system supports batch installs of multiple patches at the same time and reboots once at the end of all patch installations. Therefore, use switch settings to suppress automatic reboot wherever possible.

Switch Settings

Typical patch file switch settings for [silent, unattended installs without reboot](#):

- `/quiet /norestart` - This is the standard setting for most patches in recent years.
- `/u /q /z` - Typical switch settings used to silently install older patches that do not use the Windows Installer technology.
- `/m /q /z` - Typical switch settings to silently install older patches released for Windows NT4.
- `/q:a /r:n` - Internet Explorer and other application switch settings to install in quiet administrator mode (`/q:a`) and not automatically reset (`/r:n`) when the install completes.
- Other switch settings found with Microsoft patch installations include:
 - `/?` - Display the list of installation switches.
 - `/u` - Use Unattended mode.
 - `/m` - Unattended mode in older patches.
 - `/f` - Force other programs to quit when the computer shuts down.
 - `/n` - Do not back up files for removal.
 - `/o` - Overwrite OEM files without prompting.
 - `/z` - Do not restart when the installation is complete.
 - `/q` - Use quiet mode (no user interaction).
 - `/l` - List the installed hotfixes.
 - `/x` - Extract files without running Setup.

Microsoft Office command line switches

The only switch permitted for use with Microsoft Office 2000 and Office XP related patches is `/Q`. If `/Q` is not specified, Microsoft Office 2000 and Microsoft Office XP switches will be automatically reset to `/INSTALL-AS-USER`. Microsoft Office 2003 patches may also include the `/MSOCACHE` switch

used to attempt a silent install if the MSOCache exists on the machine. These settings are enforced by the application.

Note: The `/MSOCACHE` switch only applies to Office 2003. When the patch database is updated, this switch is automatically added to all Office 2003 patches where a user has never modified a particular patch's command line switches. It is not automatically added to Office 2003 service packs. When this switch is used, the system determines if the MSOCache exists on the target machine. If the MSOCache does exist and this switch is used, the system automatically uses the run silently switch (`/Q`) thereby relying on the MSOCache rather than requiring the actual installation media. If the MSOCache does not exist on the target machine, the existing switch is used. If a patch installation fails that uses the `/MSOCACHE` switch, it typically means that the MSOCache could not be used by the patch. In this case, you must clear out all command line switches for this patch and set the `/INSTALL-AS-USER` switch. Re-running the patch installation should now succeed. Unfortunately, this requires user intervention and also probably requires the Office 2003 installation media.

Server-side command line switches

Special server-side command line switches can be combined with patch specific switches:

- `/INSTALL-AS-USER` - Tells the system to only install this patch as a user. Some rare patches do not install successfully unless someone is logged onto the machine. Add this switch if you find a patch is failing to install if no one is logged in.

Warning: This setting conflicts with the Skip update if user logged in setting found in Reboot Action (page 245). `/INSTALL-AS-USER` requires that a user be logged in to install.

- `/DELAY-AFTER=xxx` - After the install wait `xxx` seconds before performing the reboot step. The reboot step starts after the install package completes. Some rare installers spawn additional programs that must also complete before rebooting. Add this switch to give other processes time to complete after the main installer is done.

Filter patches by

Based on the patch category selected, this page displays all patches and service packs for all machines, both missing and installed, that match the current [Machine ID/Group ID filter](#) (page 477).

New Switches

Enter the command line switches you want to apply to selected patches.

Apply

Click [Apply](#) to apply the specified command line switches to selected patches.

Reset

Click [Reset](#) to reset the command lines of selected patches back to their default 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.

KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

Patch Name

The patch install filename.

Patch Management

Security Bulletin

The security bulletin associated with a patch. Patches classified as security updates have a security bulletin ID (MSyy-xxx). Click the [Security Bulletin](#) link to review the security bulletin, if available.

Product

The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

Switches

The command line switches used to install this patch.

Patch Location

Patch Mgmt > Patch Location

The [Patch Location](#) page defines the URL from which each patch is downloaded. Only patches *missing* from machine IDs that currently match the [Machine ID / Group ID filter](#) (*page 17*) are displayed here. You should consult this page if, when attempting to install a patch, you are notified of a `Path Missing`.

The KServer maintains a list of each patch and the URL it should be downloaded from. In most cases the download URLs provided for patches are correct. `Path Missing` errors may occur for the following reasons:

- Each language may require a separate URL to download from.
- The URL may change for one or more patches.
- The KServer's record for the URL may be entered incorrectly or be corrupted.

In such cases, administrators can change the download path associated with a patch. Manually entered URLs are shown in **dark red**.

Note: Only master administrators can access this page. Changes effect patches installed by all administrators.

To find the URL to a missing path

1. Click the [KB Article](#) listed for the missing path.
2. Read through the knowledge base article and locate the download URL for the patch.

Note: There may be several products referenced by the same KB Article. For instance, each Windows operating system is a different product. Also, patches can be different for specific service packs of the operating system.

3. Click on the download link for your patch. If a *different patch is available for each language*, you will be prompted to select a language.
4. Select the appropriate language for the download, if applicable.
5. Click the [Download](#) link or button and download the patch file.
6. On your web browser, click the [History](#) icon to view your URL history.
7. Locate the file you just downloaded from your history list. Typically, the file will be in the `download.microsoft.com` folder.
8. Right-click the filename you just downloaded and select [Copy](#) from the menu. This copies the entire URL into your clipboard.
9. Return to the [Patch Location](#) page and:

- a. Paste the URL into the [New Location](#) edit box.
- b. Select the radio button to the left of the [KB Article](#) for which you are entering a new patch location.
- c. Click the [Apply](#) button.

Filter Patch By

Select the patches displayed in the paging area by patch category.

New Location

Enter a new URL.

Apply

Click [Apply](#) to apply the URL listed in the [New Location](#) field to the selected patch.

Remove

Click [Remove](#) to delete the download URL associated with a patch ID. The default path is restored the next time `refresh patch database` runs.

Warning: Removing a path disables patching managed machines using this patch until the correct path is entered.

KB Article

The knowledge base article describing the patch. Click the [KB Article](#) link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

Product

The [Product](#) column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (i.e., Windows XP, Windows Server 2003, Vista, etc.), the product category is `Common Windows Component`. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, etc.

Chapter 9

Remote Control

In This Chapter

Remote Cntl Tab	262
Control Machine	263
Video Streaming	265
Reset Password	267
Power Mgmt	268
Select Type	269
Set Parameters	271
Preinstall RC	272
Uninstall RC	273
Admin Role Policy	274
Machine Policy	276
FTP	277
Chat	279
Send Message	281
Task Manager	283

Remote Cntl Tab

View and operate managed machines as if they were right in front of you simply by clicking its machine ID.

- Automatically connects the administrator to the remote computer independent of any gateway or firewall configurations, even behind NAT.
- Remote control even without a agent using video streaming.
- Work independently or with the user to solve problems interactively where both parties can see what is happening in real time
- Policy settings allow users to block remote control or require administrators to ask permission before accessing a machine
- Integrates four best of breed remote control packages: WinVNC, pcAnywhere™ (Symantec), RAdmin (Famatech), or Terminal Server (Microsoft)
- 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.

Note: You can view Remote Control demos at <http://www.kaseya.com/get-started/demo.aspx>.

Functions	Description
Control Machine (page 263)	Allows administrators to view and/or take control of a managed machine's desktop remotely for troubleshooting and/or instructional purposes.
Video Streaming (page 265)	Remote control machines that do not have an agent installed.
Reset Password (page 267)	Reset the password for an local account on a managed machine.
Power Mgmt (page 268)	Powers on, powers off or reboots vPro-enabled machines.
Select Type (page 269)	Specify the type of remote control software the VSA uses on a per machine basis. WinVNC, Remote Administrator, pcAnywhere, and Terminal Server are all supported.
Set Parameters (page 271)	Specify the remote control settings to use with each remote control package.
Preinstall RC (page 272)	Install the remote control service
Uninstall RC (page 273)	Uninstall the remote control service
FTP (page 277)	Initiate an FTP session with any remote managed machine.
Chat (page 279)	Start a chat session between an administrator and any remote machine.
Send Message (page 281)	Allows administrators to send network messages to selected managed machines.
Task Manager (page 283)	Remotely executes the NT task manager and displays data in the browser.

Control Machine

Remote Ctrl > Control Machine

The [Control Machine](#) page establishes a remote control session between the administrator's local machine and a selected machine ID. Select the type of package to remote control a managed machine using [Select Type](#) (page 269). Set parameters for remote control sessions using [Set Parameters](#) (page 271).

Note: Use [Video Streaming](#) (page 265) to remote control a target machine that does not have an agent.

Automatic Installation

If [WinVNC](#), [K-VNC](#) or [RAdmin](#) are *not* installed on a machine and a remote control session is initiated using [Control Machine](#) (page 263) or [Video Streaming](#) (page 265), then these packages are 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 [WinVNC](#), [K-VNC](#) or [RAdmin](#) on any managed machine using [Preinstall RC](#) (page 272).

Note: Uninstalling an agent does not remove the installed remote control package. Before you delete the agent, use [Remote Control > Uninstall RC](#) (page 273) to uninstall remote control on the managed machine.

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  icon can be connected to target machines and have live links; all others will be inactive.

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 361).

ActiveX Control

An ActiveX control automatically configures and runs the remote control or FTP package for you. The first time you use any remote control or FTP package 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 administrator or user is presented with a link to manually download and run the remote control package manually.

Helper Applications

In setting up a remote control or FTP session, gateway and port blocking problems are eliminated by always initiating outbound connections from both the target machine and the administrator machine. Helper applications, unique to each supported remote control or FTP package, automatically

Remote Control

determine the optimal routing path between the administrator machine and the target machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

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 KServer itself. Use this feature to remotely manage your own KServer. Only master administrators can remote control the KServer.

Remote Control and FTP for Users

Administrators can provide users with the same remote control and FTP access that administrators have using Agent > [User Access](#) (page 212).

Remote Control Malfunctions

Some reasons for remote control failure—for both target machines with and without an agent—are:

- The administrator 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 KServer address - Remote control can only connect through the primary KServer address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address using Agent > [Check-in Control](#) (page 363).
- XP supports only one [RDP/Terminal Service](#) session on the target machine and logs off other users. Starting a remote logon session from a second machine logs off the first remote logon session. The VSA uses the port relay to get through firewalls and gateways. To Windows XP, it appears as if the Terminal Server session is connecting from the localhost.

Warning: Using the credential of a currently logged on user confuses XP. It can not determine if the user is reactivating the existing session locally or remotely initiating a new connection. As a result Window XP may hang, requiring a reboot to recover. The VSA can not protect you from this. Do not log on using the user name of an already logged on account.

- Your [pcAnywhere](#) viewer is connecting to your administrator machine, not the target machine. The KServer relay is telling the viewer to connect to localhost. **If you have a pcAnywhere host running on the machine you are viewing from**, then the viewer connects to it and not the VSA relay. Right click the pcAnywhere icon in the system tray and select [Cancel Host](#).
- [pcAnywhere](#) presents an error dialog saying Cannot find callhost file: C:\Document and Settings\All Users\Application Data\Symantec\pcAnywhere\Network.CHF. There is no Network remote control item configured in pcAnywhere.
 1. Open the [pcAnywhere](#) application and click on the [Remote Control](#) function.
 2. Click [Add Remote Control Item](#).
 3. Create an item named [Network](#).
 4. Select [TCP/IP](#) as the connection device.
 5. Leave the host name blank.
 6. Close [pcAnywhere](#).

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Remote Control Package

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using [Select Type](#) (page 269).

-  WinVNC
-  K-VNC
-  Remote Administrator
-  pcAnywhere
-  RDP/Terminal Server

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Only machine IDs with an  icon can be remote controlled and have live links; all others will be inactive.

Current User

The user currently logged into the managed machine.

Active Admin

The administrator currently conducting a remote control session to this machine ID.

Video Streaming

Remote Cntl > Video Streaming

The [Video Streaming](#) page establishes a remote control session between the administrator's local machine and a machine [without an agent](#). Use it to help someone quickly on an infrequent basis. If you plan to provide continuous support we recommend you install an agent.

The following conditions apply:

- The remote user must log into a URL after the administrator has started the video streaming session.
- The remote user must have administrator privileges on the local machine.
- Each administrator can only initiate a single video streaming session at a time.

Set parameters for remote control sessions using [Set Parameters](#) (page 271). See [Select Type](#) (page 269) for a description of the different types of remote control packages.

Remote Control

Note: Use [Control Machine](#) (page 263) to remote control a target machine that has an agent.

Automatic Installation

If [WinVNC](#), [K-VNC](#) or [RAdmin](#) are *not* installed on a machine and a remote control session is initiated using [Control Machine](#) (page 263) or [Video Streaming](#) (page 265), then these packages are automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute.

Automatic Uninstallation

When either side terminates the [Video Streaming](#) session, the remote server on the target machine uninstalls automatically, removing all remote control files and registry additions.

ActiveX Control

An ActiveX control automatically configures and runs the remote control or FTP package for you. The first time you use any remote control or FTP package 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 administrator or user is presented with a link to manually download and run the remote control package manually.

Helper Applications

In setting up a remote control or FTP session, gateway and port blocking problems are eliminated by always initiating outbound connections from both the target machine and the administrator machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the administrator machine and the target machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

Remote Control Malfunctions

Some reasons for remote control failure—for both target machines with and without an agent—are:

- The administrator 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 KServer address - Remote control can only connect through the primary KServer address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address using Agent > [Check-in Control](#) (page 363).

Start

Click the [Start](#) button. Ask the remote user to display the **Error! Hyperlink reference not valid.** web page and click your administrator name to begin the video streaming session.

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.

Select remote control package to use

The default remote control service uses [WinVNC](#). See [Select Type](#) (page 269) for a description of the different types of remote control packages.



Specify the default HTML message seen by users when no administrator is waiting to help.

This is the message displayed if the user displays the **Error! Hyperlink reference not valid.** web page and no administrator is logged into the KServer.

Reset Password

Remote Cntl > Reset Password

The [Reset Password](#) page creates a new password and, if necessary, a new user account on a managed machine. 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 script to delete the user account or use remote control to manually delete the user account.

Resetting the Administrator Password

Use [Reset Password](#) to reset the Administrator password on all your managed machines when:

- Your Administrator password is compromised.
- Someone leaves your organization who knew the Administrator password.
- It is time to change the Administrator password as part of a good security policy.

Note: On non-domain controllers, only the local user account on the target 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 as an administrator.

Password / Confirm

Enter a new password.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Status

The status of pending password changes and user account creations.

Power Mgmt

Remote Cntl > Power Mgmt

The [Power Mgmt](#) page powers on, powers off or reboots vPro-enabled machines. Power management options are executed using the agent of the managed machine that originally identified the vPro-enabled machine using [LAN Watch](#) (page 348). A [vPro](#) (page 486) credential is required to execute power management options on a vPro-enabled machine.

Note: You can display the hardware assets of vPro-enabled machines with credentials using [Agent > View vPro](#) (page 358).

This page provides you with the following actions:

- [Schedule](#) - Display a popup window of the following schedule options:
 - [Schedule / Cancel](#) - Schedule or cancel these schedule options.
 - [Schedule Date/Time](#) - Select the date and time to schedule this task.
 - [Recurrence](#) - Select whether to run this task once, hourly, daily monthly. If more than once, enter the number of times to run this task for the period selected.
 - [Skip if offline](#) - Check to perform this task only at the scheduled time. 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.
 - [Stagger by N minutes](#) - 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, ...
- [Run Now](#) - Run the power management options now on selected machine IDs.
- [Cancel](#) - Cancel schedule options for selected machined IDs.

- [Power Up / Power Down / Reboot](#) - Select the power management option to execute.

Host Name

The unique local name and domain name of a vPro enabled-machine on a network, using the format <domainname>.<computername>.

Proxy Agent

The machine ID.group ID of another managed machine used to execute power on, power off or reboot this vPro-enabled machine. The [Proxy Agent](#) must be on the same LAN as the vPro machine.

Machine ID. Group ID

The machine ID.Group ID of this vPro-enabled machine, if an agent is installed. Blank, if no agent is installed.

Type

The power management option scheduled to be executed.

Last Power Mgmt

The last time a power management option was executed.

New Power Mgmt

The next time a power management option is scheduled to be executed.

Credentials

If not-checked, a vPro credential is not registered in the VSA for this vPro-enabled machine and you cannot execute power management option. If checked, a vPro credential is registered in the VSA. In either case, you can click any cell in the [Credentials](#) column to display a popup window that lets you register a credential.

Recur Interval

The interval for the scheduled task to recur.

Skip if Machine Offline

If a checkmark  displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

Stagger By

The number of minutes to stagger this task on multiple machines.

Select Type

[Remote Cntl](#) > [Select Type](#)

The [Select Type](#) page specifies which remote control package is used by [Control Machine](#) (*page 263*) to remote control a managed machine. You can assign different packages to different machines. Each machine ID displays the icon of the remote control package it is currently assigned to use.

Virtual Network Computing

[Virtual Network Computing \(VNC\)](#), also called [remote control](#) or [remote desktop](#), is a graphical desktop

Remote Control

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 KServer 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 target machine that shares its screen. The [VNC client \(or viewer\)](#) is the program on the administrator's machine that watches and interacts with the target machine. The VNC client machine requires user access rights to the VNC server machine. Since Kaseya VNC sessions are relayed through the KServer, all VNC sessions are protected by the Kaseya 256 bit rolling encryption protocol.

The VSA supports the following third party remote control packages.

- [WinVNC](#)  - This open source, freely available, remote control package comes bundled with the VSA. WinVNC is the default package used on all managed machines. The VSA automatically installs WinVNC servers on selected machines the first time you remote control that machine.
- [K-VNC](#)  - The enterprise version of VNC. This is the only remote control option available for Vista. It can also be used on Windows 2000, XP and 2003. The VSA automatically installs the K-VNC server on selected machines the first time you remote control that machine.
- [Remote Administrator](#)  - RAdmin is a commercially available remote control package offering both high speed and file transfer capability. Use RAdmin where bandwidth limitations exist or you need remote file transfer to the machine. The VSA automatically installs the RAdmin server on selected machines the first time you remote control that machine. The RAdmin package bundled with the VSA expires after 30 days. Obtain licenses from www.radmin.com.
- [pcAnywhere](#)  - pcAnywhere is a widely used remote control package available from Symantec. The VSA fully supports pcAnywhere but does not automatically install it. You must purchase pcAnywhere separately and install it on the workstation before you can use this option. Combining the VSA with existing installations of pcAnywhere allows you to remote control machines behind gateways without mapping ports or opening firewalls.
- [Terminal Server](#)  - Microsoft Terminal Server is only available with Windows NT, 2000, XP, or 2003. The VSA does not automatically install Terminal Server but does allow you to remote control machines behind gateways without mapping ports or opening firewalls. XP comes pre-installed with Terminal Service access for a single user. For other operating systems see Terminal Service Client Access License requirements on the Microsoft website.

To Assign Remote Control Packages to Machine IDs

1. Select the type of package to use from the drop down list.
2. Check the box to the left of machine IDs you want to use this remote control package.
3. Click the [Select](#) button.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete

-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Remote Control Package

The remote control package assigned to this machine ID.

-  WinVNC
-  K-VNC
-  Remote Administrator
-  pcAnywhere
-  RDP/Terminal Server

Set Parameters

Remote Cntl > Set Parameters

The [Set Parameters](#) page sets the default parameters for your remote control session. These settings are remembered on a [per administrator](#) basis. Changes take effect immediately and are reused every time you start remote control. See [Select Type](#) (page 269) for a description of the different types of remote control packages.

WinVNC and K-VNC Options

- [View Only Mode](#) - The administrator can view the remote machine. No mouse or keyboard events are sent to the target machine.
- [Hide WinVNC system tray icon on the remote machine](#) - Check this box to hide the WinVNC icon on the remote machine.
- [Restrict to 64 colors](#) - The display on the listening machine is set to 64 colors. This is useful for slower connections.
- [Full Screen mode](#) - The entire display of the administrator machine is used to display the screen contents of the target machine. Exit by displaying the remote control menu (default **F8**) and unselect [Full screen](#).

RAdmin Options

- [Full Control](#) - The administrator can view and/or control the screen keyboard and mouse of the target machine.
- [View Only](#) - The administrator can view the remote machine. No mouse or keyboard events are sent to the target machine.
- [File Transfer](#) - Start a file transfer (FTP) session with the remote machine. This mode presents you with two standard file browsers, one for the target machine and one for the administrator machine. Drag and drop files between the two machines in this mode.
- [Full Screen View Mode](#) - The entire display of the administrator machine is used to display the screen contents of the target machine. This option is only available in a Full Control or View Only session.
- [Encrypt Data Stream](#) - Checking this box encrypts all traffic between the administrator and target machines.

Remote Control

- [Update/sec](#) - Sets the maximum number of update per second RAdmin generates. Higher update rates consume more CPU cycles on the remote machine.
- [Color Format](#) - Specifies the number of colors used for remote control. Large color formats use more bandwidth.

Terminal Service Options

- [Console mode](#) - Remote control the console session of the remote machine.
- [Full Screen mode](#) - Use your full screen to remote control the remote machine.
- [Fixed Screen size](#) - Set a fixed width and height for your remote control session.
- [Share Disk Drives](#) - Connect your disk drives to the remote machine.
 - [Only share the following disks](#) - Enter the specific drive letters to share or leave blank to share all disks.
- [Share Printers](#) - Connect your printers to the remote machine.
- [Disable Desktop Wallpaper](#) - Turn off wallpaper on remote computer for faster processing.

Preinstall RC

Remote Cntl > Preinstall RC

The [Preinstall RC](#) page installs [WinVNC](#), [K-VNC](#) or [RAdmin](#) on selected machine IDs without initiating a remote control session. Select the type of package to remote control a managed machine using [Select Type](#) (page 269). When an install is pending on any machine ID this page automatically refreshes every 5 seconds until the script completes.

Note: Preinstall RC does not install pcAnywhere or Terminal Server.

Automatic Installation

If [WinVNC](#), [K-VNC](#) or [RAdmin](#) are *not* installed on a machine and a remote control session is initiated using [Control Machine](#) (page 263) or [Video Streaming](#) (page 265), then these packages are 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 [WinVNC](#), [K-VNC](#) or [RAdmin](#) on any managed machine using [Preinstall RC](#) (page 272).

Note: Uninstalling an agent does not remove the installed remote control package. Before you delete the agent, use [Remote Control > Uninstall RC](#) (page 273) to uninstall remote control on the managed machine.

Install

Click [Install](#) to install [WinVNC](#), [K-VNC](#) or [RAdmin](#) on selected machine IDs.

Cancel

Click [Cancel](#) to clear pending install scripts 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:



Agent has checked in



Agent has checked in and user is logged on. Tool tip lists the logon name.

-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Remote Control Package

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using [Select Type](#) (page 269).

-  WinVNC
-  K-VNC
-  Remote Administrator
-  pcAnywhere
-  RDP/Terminal Server

Last Status

`Pending` indicates the install will run the next time that machine checks into the KServer. Otherwise, this column displays when the remote control package was installed on the machine ID.

Uninstall RC

Remote Cntl > Uninstall RC

The [Uninstall RC](#) page uninstalls [WinVNC](#), [K-VNC](#) or [RAdmin](#) on selected machine IDs. Multiple types of remote control packages may be installed on a single machine ID. Select the type of package to uninstall from a managed machine using [Select Type](#) (page 269). When an uninstall is pending on any machine ID this page automatically refreshes every 5 seconds until the script completes.

If an existing installation of [WinVNC](#) or [RAdmin](#) has problems then the VSA may not be able to establish a remote control session. If remote control fails then running [Uninstall RC](#) on that machine ID cleans out any existing problem installs. A fresh copy of the remote control package is installed the next time a remote control session is started or using [Preinstall RC](#) (page 272).

Note: Uninstall RC does not uninstall pcAnywhere or Terminal Server.

Note: Uninstalling an agent does not remove the installed remote control package. Before you delete the agent, use [Remote Control > Uninstall RC](#) (page 273) to uninstall remote control on the managed machine.

Automatic Uninstallation

[Uninstall RC](#) is not required for [Video Streaming](#). When either side terminates the [Video Streaming](#) session, the remote server on the target machine uninstalls automatically, removing all remote control files and registry additions.

Uninstall

Click [Uninstall](#) to uninstall [WinVNC](#), [K-VNC](#) or [RAdmin](#) on selected machine IDs.

Remote Control

Cancel

Click [Cancel](#) to clear pending uninstall scripts 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Remote Control Package

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using [Select Type](#) (page 269).

-  WinVNC
-  K-VNC
-  Remote Administrator
-  pcAnywhere
-  RDP/Terminal Server

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.

Admin Role Policy

Remote Cntl > Admin Role Policy

The [Admin 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 [administrator roles](#) (page 383).

Note: See [Machine Policy](#) (page 276) to apply remote control notification policies by machine ID. Machine policy takes precedence over administrator role policy.

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 cancelled.

Notify user when session terminates.

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 administrators 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 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.

Delete

Click the delete icon  next to an administrator 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 **administrator roles** (*page 383*).

Policy

The remote control policy applied to an administrator role.

Message

The **Session Termination Message** applied to an administrator role.

Machine Policy

Remote Cntl > 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 [Admin Role Policy \(page 274\)](#) to apply remote control notification policies by machine ID. Machine policy takes precedence over administrator role policy.

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 cancelled.

Notify user when session terminates.

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 administrators 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 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.

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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Policy

The remote control policy applied to a machine ID.

Message

The [Session Termination Message](#) applied to a machine ID.

FTP

Remote Cntl - FTP

The [FTP](#) page establishes a FTP session between the administrator's local machine and a selected machine ID. The VSA uses the FTP client built into [Internet Explorer](#) so you can operate with the same Windows look and feel. 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.

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 administrator's 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 KServer 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 KServer, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.

Initiating FTP

Initiate a FTP session 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  icon can be connected to target machines and have live links; all others will be inactive.

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled

Remote Control

 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 361).

ActiveX Control

An ActiveX control automatically configures and runs the remote control or FTP package for you. The first time you use any remote control or FTP package 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 administrator or user is presented with a link to manually download and run the remote control package manually.

Helper Applications

In setting up a remote control or FTP session, gateway and port blocking problems are eliminated by always initiating outbound connections from both the target machine and the administrator machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the administrator machine and the target machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

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 KServer itself. Only master administrators can FTP the KServer.

Remote Control and FTP for Users

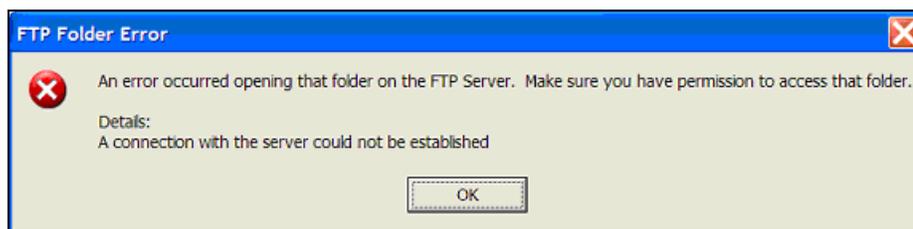
Administrators can provide users with the same remote control and FTP access that administrators have using **Agent > User Access** (page 212).

FTP Malfunctions

Some reasons for FTP failure with managed machines are:

- The administrator 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 KServer address - Remote control can only connect through the primary KServer address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address using **Agent > Check-in Control** (page 363).
- You accessed the KServer 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 KServer to Windows. Say you downloaded the helper application from www.yourKServer.net. Then you open a new browser and access the KServer by typing in its IP address 192.168.1.34. The KServer 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) ([page 476](#)) displayed is based on the [Machine ID / Group ID filter](#) ([page 17](#)) and the machine groups the administrator is authorized to see using [System > Group Access](#) ([page 385](#)).

Enter a drive letter to FTP to

Enter the drive letter to FTP to instead of selecting a remote fixed drive option.

Note: The KServer determines how many fixed disks a managed machine has via its Latest Audit ([page 33](#)).

Chat

Remote Cntl > Chat

The [Chat](#) page initiates or continues chat sessions with 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.

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 the next time it checks in. Enter text in the text pane. Click the [Send](#) button to send the message.

Remote Control

To Respond to a Chat Session

If a chat popup window displays while you are logged into the KServer, respond by entering text in the text pane. Click the [Send](#) button to send the message.

Join Session link

Multiple administrators may participate in the same chat session with a 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 Administrators

The names of [logged in administrators](#) with [Group Access](#) (*page 385*) rights to the group IDs currently displayed by the machine ID.group ID filter display on the [Chat](#) page as well. Click the link of another logged in administrator to initiate a chat with that administrator. \

Enable / Disable the User's Ability to Initiate Chat with Administrators

Administrators can enable / disable the user's ability to initiate a chat session using Agent > [User Access](#) (*page 212*).

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](#).

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 administrators.

Remove your name from chat list seen by users

Check this box to remove your name from the chat list seen by users.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Send Message

Remote Cntl > Send Message

The [Send Message](#) page sends network messages to a select group of users. 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 user click's the flashing icon the message displays.

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.

Note: Send and receive messages to and from other administrators using [Home > View Dashboard](#) (page 28).

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.

Remote Control

Send Now

Click [Send Now](#) to send the message when the recipient's machine conducts its next check-in. The message displays in the [Messages Not Yet Sent](#) column until the message is received by the recipient machine.

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 recipient machine.

Display Immediately/Flash Icon

This setting determines how managed machine users are notified once their message has been retrieved from the KServer.

- [Display Immediately](#) notifies the user immediately.
- [Flash Icon](#) flashes the agent icon in the [system tray](#) (on page 483) until the user clicks the icon. The message is then displayed according to the settings in [Select display window](#).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Current User

Displays the currently logged on user.

Messages Not Yet Sent

This column displays messages not yet sent.

Task Manager

Remote Cntl > 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.

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.

Chapter 10

Reports



In This Chapter

Reports Tab	286
Set Logo	287
Schedule Reports	287
Executive Summary	289
Aggregate Table	294
Advanced Filtering	295
Machine Summary	296
Machine Changes	298
Patch Management	299
Inventory	301
Software	303
Disk Utilization	305
Network Statistics	306
Uptime History	308
Logs	309
Ticketing	311
Backup	312
Monitor	314
Security	316
User State	318
Power Savings	319

Reports Tab

The **Reports** tab allows administrators to generate detailed reports about managed machines. These reports are based on all the other tasks performed by the VSA.

- Maintain reports using the report wizards in **Run Reports**.
- Schedule the running of existing reports using **Schedule Reports**.
- Set the logo displayed in reports using **Set Logo**.

Note: You can view Reports demos at <http://www.kaseya.com/get-started/demo.aspx>.

Functions	Description
Set Logo (page 287)	Allows custom logos to be placed on generated reports.
Schedule Reports (page 287)	Automatically run reports at a scheduled time. Reports may be posted or delivered via email.
Executive Summary (page 289)	Create a concise summary report reflecting the system health of a selected group of machines.
Aggregate Table (page 294)	Create a single table with one row per machine and using any data as columns.
Machine Summary (page 296)	Generate reports on deployed Agents and the machines they reside on.
Machine Changes (page 298)	Run a difference report between each machine's latest audit and either the baseline or latest audit from a selected machine.
Patch Management (page 299)	Displays composite and individual patch status reports
Inventory (page 301)	Inventory summary for the selected audit category.
Software (page 303)	Get detailed information regarding the software installed and used by managed machines.
Disk Utilization (page 305)	Generate graphical report on capacity and usage of all fixed disks.
Network Statistics (page 306)	View detailed network usage information, from the entire network down to a managed machine.
Uptime History (page 308)	Chart the powered up, online, and abnormal shutdown history of each machine vs. time.
Logs (page 309)	Generate reports on all logged information collected by the VSA.
Ticketing (page 311)	Report status of all trouble tickets.

Backup (page 312)	Report on the backup log and status
Monitor (page 314)	Report summarizing data retrieved from monitoring managed machines.
Security (page 316)	Reports security protection data on managed machines.
User State (page 318)	Reports user state management data on managed machines.

Set Logo

Reports > Set Logo

The [Set Logo](#) page customizes the header of reports generated by an administrator. When you run a report, the report displays the unique HTML header you enter here at the top of every report. You have full control over the HTML entered. Make the header as simple or as complex as you want.

Note: If you do not want other administrators to change the custom header, block them from seeing the Set Logo page using [System > Function Access](#) (page 387).

Modify the HTML used for the header here

Enter the HTML you want to use in the header of all your reports.

Note: The master administrator can customize the default report header seen by all administrators. Click [System > Customize](#) (page 403) and enter the custom header in the field labeled Header HTML shown on all reports.

Apply

Click [Apply](#) to update changes to the HTML you want to use in the header of all reports.

Default

Click [Default](#) to restore the header HTML to the product default setting.

Schedule Reports

Reports > Schedule Reports

The [Schedule Reports](#) page automatically exports reports to a URL on the VSA web site that *does not require a logon* to access. Schedule recurring reports to generate reports your users can access. Since the system runs these reports without the administrator logging on, only *saved* reports can be scheduled.

Note: Standard administrators can not schedule reports that use <All Groups>. Only master administrators can schedule <All Groups> reports.

Set Filter Settings

Set unique [Machine ID / Group ID](#) filter settings for each scheduled instance of a report. This lets you define a single report and schedule it to run for each individual machine or group of machines. For instance, you could create a single [Software](#) report and then schedule it to output a unique report for

Reports

each group ID. *The machine ID / group ID filter settings you specify in [Schedule Reports](#) overrides the filter settings saved with the report.*

Email the Report

Depending on how email notification is formatted using [Format Email](#), either the entire report or a short message with a URL link to the report can be sent to email recipients. Customize the message content by clicking the [Format Email](#) button.

Note: Only master administrators can change the format of the scheduled reports email.

Where Scheduled Reports are Stored

Reports are posted to the `dataReports` directory, on the VSA website, in a sub directory named after the administrator logon that scheduled the report and a sub directory for the [Machine ID / Group ID](#) filter. This convention groups all reports for a specific machine or group of machines into a common directory. For example:

http://www.your_vsa.com/dataReports/joe_admin/mach.group/report_name.htm

Show reports from all administrators

Checking this box displays all saved reports, shared and private, for all administrators. Check this box to view/delete/modify scheduled reports for any administrator.

Note: Only master administrators can show reports for all administrators.

Select report to schedule

This drop-down list shows all saved reports visible to the currently logged in administrator. Select the report to be scheduled from this list. The output report web page has the same filename as the report. Selecting a new report from this drop-down list resets the [machine ID / group ID](#) settings to those saved with the report. You can override the default machine ID / group ID settings using the [Specify accounts to run this report on](#) fields.

Report Type

Once a report is selected, the [Report Type](#) displays below the selected report.

Schedule

Click [Schedule](#) to run the report at the specified time and save the file in the `dataReports` directory.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Run at recurring interval every <N> <periods>

Check the box to make this task a recurring task. Enter the number of times to run this task each time period.

Enter email address to notify when report is ready

Comma separate each email address to send multiple notifications/reports. Leave this field blank to disable email notification.

Format Email

Depending on how email notification is formatted using [Format Email](#), either the entire report or a short message with a URL link to the report can be sent to email recipients. Customize the message content by clicking the [Format Email](#) button. Special tags are available to insert unique report data.

- <at> Time stamp of when the report was created
- <er> Embed full report - **NOTE: Report completely replaces entire message body**
- <gr> group ID
- <id> machine ID
- <rt> Report title
- <ru> report URL

Filename

List of reports that have run or are scheduled to run. If the report has already run, the filename appears as a link to the report.

Report Type

Type of report that has been scheduled. For example, [Disk Utilization](#).

Last Run

Time when the report was last produced.

Account Filter

Specify the machine ID / group ID filter settings to use when running this scheduled report. *The machine ID / group ID filter settings you specify in [Schedule Reports](#) overrides the filter settings saved with the report.*

Next Run

Time the report is scheduled to run next. If this field is blank, the report is not scheduled to run again.

Email Address

Comma separated list of addresses notified about this report.

Recurring

Recurring interval at which the report runs.

Executive Summary

[Reports](#) > [Executive Summary](#)

The [Executive Summary](#) reports page creates a summary report of the status of all selected machines. This includes a [network health score](#) (*page 291*) representing the overall health of all selected machines as a group.

Executive Summary Sections

The [Executive Summary](#) report can include the following sections:

- [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.

Reports

- [Show Ticket Status](#) - Displays a summary of ticket status over the specified number of days.
- [Show Disk Space Used](#) - Displays a graph of the percentage free disk space on all selected machines. Restrict this chart to servers only by checking the [Show servers only](#) box.
- [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 291) 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 separately purchased the Kaseya Endpoint Security add-on module.

- [Show Alarm Notifications](#) - Summarizes alerts issued in 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.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Summarize data collected in the last N days

Patch, ticket, alarm, and status information is time dependent. Only data collected in the specified number of days contributes to this report.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Network Health Score

[Reports](#) > [Executive Summary](#) > [Change Score...](#)

The [Network Health Score](#) section of the [Executive Summary](#) (page 289) report gives you a summary view of the health and usability of selected machines as a group. The score is broken into categories. Each category is assigned one of five possible percentage scores—typically 100%, 75%, 50%, 25% and 0%—based on a count of a specified criteria. In most cases, you can customize the counts used to assign percentage scores.

- You can adjust how heavily each category effects the final score by adjusting the [weight](#) value for each category. Set the weight to 0 to turn off that category.
- You can modify the percentage scores assigned the [OS Score](#).
- You cannot modify the [Patch Score](#) criteria.

The final network health score computes the weighted average of the above percentage scores and normalizes them to provide the final percentage score. 100% represents perfect.

For example, say you set one category to 10 and seven other weight categories to 1. The total weight is 17. The percentage associated with the 10 category is multiplied by 10/17 in the final percentage score calculation. In contrast, the percentages associated with the other seven weight categories are multiplied only by 1/17 in the final percentage score calculation.

[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:

Vista/2008	100%
------------	------

Reports

XP/2003	100%
2000	75%
Mac OS	100%
All others	0%

Note: The OS score weighting can be customized. You can individually weight the OS score given to Vista, 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%
-------------------	-----

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 Kaseya Endpoint Security addon module.

Script Score - Scripts provide a recurring beneficial service to a machine. The more often the script runs, the better shape that machine is likely to be in. The longer it has been since the script ran, the lower the score. The weighted thresholds for the script score count the number of days since the script last ran on the machines. The default values provide the following score:

1	0 to 3 days since script ran	100%
2	4 to 9 days since script ran	75%
3	10 to 19 days since script ran	50%
4	20 or more days since script ran	25%

System Activity

Reports > Executive Summary > Change Rows...

The **System Activity** section of the **Executive Summary** (page 289) 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 Scripts** tab of the **Machine Summary** (page 296) page to identify search filter phrases to use for a script-based row type.
- **Log Monitoring** does not display in **Pending Scripts**. Review **Log Monitoring in Agent Logs** in the **Machine Summary** page 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.	*Success THEN* or *Failed ELSE* or *Success ELSE*	Not applicable.
Script Log	Select a system, private or public script.	*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	*device error*	Not applicable.

Reports

	Parser (page 184) .		
Log Monitoring Custom	Select a Log File Parser with a numeric parameter.	EventCode or ErrorCode	Average, Count, Min, Max Or Total

Aggregate Table

Reports > Aggregate Table

The [Aggregate Table](#) reports page creates 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 [Not Displayed](#) list, then click [Add>>](#). To remove items, click items in the [Displayed](#) list, then click [<<Remove](#). To change the order items are listed, click an item in the [Displayed](#) list, then click the up arrow  or down arrow .

Advanced Filter

Click [Advanced Filter \(page 295\)](#) to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators \(page 469\)](#). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

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. 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

NOT

Search for a string not containing the match data.

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

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.

Reports

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

Returns all data whose value is numerically less than, if a number. If this is alphabetic data then it returns all strings appearing earlier in the alphabet.

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

For example: < 3 returns all values numerically less than "3".

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)

Returns all data whose value is numerically greater than, if a number. If this is alphabetic data then it returns all strings appearing after it in the alphabet.

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

For example: > 3 returns all values numerically greater than "3".

Machine Summary

Reports > Machine Summary

- Similar information is provided using Audit > Machine Summary (page 21).

The [Machine Summary](#) reports page produces a detailed report for each machine ID matching the machine ID / group ID filter. 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. The Audit > [Machine Summary](#) (page 21) page displays similar information.

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 33) that have appeared on the machine since the [Baseline Audit](#) (page 33) was run.
- [Apps Removed Since Baseline](#) - All applications that were present when the [Baseline Audit](#) (page 33) was ran but are missing when [Latest Audit](#) (page 33) 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 File](#) - List files being distributed to the managed machine by the KServer.
- [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.

- [Recurring Scripts](#) - Lists scripts that are executed on a scheduled basis on the managed machine.
- [Pending Scripts](#) - Lists scheduled scripts on the managed machine.
- [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.
- [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.
- [System Info](#) - All items collected by the [System Info](#) (page 35) function under the Audit Tab. 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 [Not Displayed](#) list, then click [Add>>](#). To remove items, click items in the [Displayed](#) list, then click [<<Remove](#). To change the order items are listed, click an item in the [Displayed](#) list, then click the up arrow  or down arrow .

Advanced Filter

Click [Advanced Filter](#) (page 295) to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Reports

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Machine Changes

Reports > Machine Changes

- Similar information is provided using [Audit > System Info](#) (page 31), [Installed Apps](#) (page 36), and [Disk Volumes](#) (page 40).

The [Machine Changes](#) page creates 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 select 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](#) - If checked, the selected machine ID's baseline audit is used for comparison instead of the selected machine ID's latest audit.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Patch Management

Reports > Patch Management

- Similar information is provided using [Patch Mgmt > Patch Status](#) (page 222), [Machine History](#) (page 228), [Machine Update](#) (page 229) and [Patch Update](#) (page 228).

The [Patch Managements](#) page creates a report that lists the patch state for all selected machines. 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.

Patch Management Sections

The [Patch Management](#) report can include the following sections:

- [Show machine patch summary pie chart](#) - Display a pie chart showing the number of machines that are:
 - Fully patched systems
 - Missing 1 or 2 patches

Reports

- Missing 3, 4, or 5 patches
- Missing more than 5 patches
- Have never been scanned
- [Show machine patch summary table](#) - Display a machine patch summary table.
- [Show missing patch occurrence bar chart](#) - Display a bar chart illustrating which patches have the most machines that are missing that patch.
- [Show 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, knowledge base article number, and patch title. If [Show list all machines missing each patch](#) is also checked, then the report lists each machine ID missing the patch.
- [Show 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 [Show 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 list all machines containing each patch](#) is also checked, then the report lists each machine ID with the patch installed.
- [Show 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 summaries for each patch](#) is checked the summary describing the patch is also displayed.
- [Show missing patches for each machine](#) - For each machine ID a list only of missing patches are shown. Patches are grouped by application. If [Show summaries for each patch](#) is checked that the summary describing the patch is also displayed.
- [Show 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.

Report Filtering

The [Patch Management](#) report can be filtered as follows:

- [Filter patches by](#) - 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 and include all patches whether approved or denied.
- [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.

Running the Report

1. *Select* the data you want to display in the report.
2. *Filter* the data you want to display in the report.
3. Enter the title of the report.
4. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (*page 469*). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (*page 477*) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (*page 287*).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Inventory

Reports > Inventory

- Similar information is provided using [Audit > System Info](#) (*page 35*) and [PCI & Disk HW](#) (*page 41*).

The [Inventory](#) page creates 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

This inventory report option displays additional fields for filtering the data in the report.

Note: To display any data for a managed machine in a PCI & Disk HW inventory report, an audit must be run with the PCI and Disk Audit option enabled for that managed machine using [Audit > Run Audit](#) (*page 33*).

Reports

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Software

Reports > Software

- Similar information is provided using **Audit > Installed Apps** (page 36), **Add/Remove** (page 37), **Name/OS Info** (page 38), and **SW Licenses** (page 37).

The **Software** page generates a report displaying a summary of applications present on all selected machines. Each report uses data collected from the latest audit to display the state of each group's software installed base.

Types of Software Reports

There are four primary report types:

- All Applications
- Add/Remove Programs
- Software Licenses
- Summary Licenses
- Operating Systems

All Applications

Generates a table showing each unique application found on all machines by audit. The total number of unique copies of the application are also listed. You can optionally show or hide each column of data. Hiding a column may reduce the number of rows reported if the uniqueness of the data drops. For instance, your report may show 50 copies of an application with v2.0.1 and 127 copies of the same application with v2.8. If you hide the version, by unchecking the box, then the report lists 177 copies of that application. The All Application report lists:

- **Applications** - The application name (theApp.exe)
- **Product Name** - Product name string as provided by the software vendor.
- **Description** - Software description string as provided by the software vendor.
- **Manufacturer** - The software vendor name
- **Version** - Software version number.

Checking **Show unregistered applications** lists all the unregistered applications in addition to registered applications. 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.

If **List machine IDs that contain each application** is checked then the machine ID of each machine containing the application is listed.

Note: Click the **Advanced...** (page 295) link to learn about filtering options.

Add/Remove Programs

Generates a table listing the list of add/remove programs found in a group of machines discovered by audit. If **List machine IDs that contain each application** is checked then the machine ID of each machine containing the add/remove program is listed.

Note: Click the **Advanced...** (page 295) link to learn about filtering options.

Software Licenses

Generates a table listing the number of software licenses found in a group of machines discovered by audit. This report lists the total number of licenses and the number of unique licenses found across all machines. In addition, **Software Licenses** lists:

- **Publisher** - The software vendor name

Reports

- **Title** - The software title for each license found.

If [List machine IDs](#) is checked then the machine ID of each machine containing the application is listed. If [List license codes, product keys, and machine IDs](#) is checked, then license codes and product keys installed are each machine are displayed.

Note: Click the [Advanced...](#) (page 295) link to learn about filtering options.

License Summary

Generates a table summarizing the licenses on all machines in a group or view. 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.

Note: Click the [Advanced...](#) (page 295) link to learn about filtering options.

Operating Systems

Charts a composite view 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.

Three [Operating System](#) report styles are available:

- Pie chart
- Bar chart
- Table

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Disk Utilization

Reports > Disk Utilization

- Similar information is provided using [Audit > Disk Volumes](#) (page 40).

The [Disk Utilization](#) page generates a graphical report representing the free space, used space and total space on each disk drive.

Three types of reports are available:

- [Bar chart showing percent of disk space used](#)
- [Bar chart showing disk space used, free space, and total disk size](#) - Hovering the mouse a bar presents a tool tip with additional information.
- [Table listing disk space used, free space, and total disk size](#)

Running the Report

1. Enter the title of the report.
2. Select the type of report you want to display.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the

Reports

administrator that created the report. [Shared](#) reports can be viewed and run by all administrators. Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (*page 477*) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (*page 287*).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Network Statistics

Reports > Network Statistics

- *Similar information is provided using [System > Statistics](#) (*page 401*).*

The [Network Statistics](#) page 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. There are two types of reports:

- [Applications](#) - Displays a graph outlining each application and corresponding network bandwidth consumption over the time period entered in the [Display <N> Days of Network Statistics](#) setting. The number of applications displayed can set to a maximum of 20.

- **Machines** - Displays a graph outlining the machines selected in the machine ID / group ID filter and corresponding network bandwidth consumption over the time period entered in the [Display <N> Days of Network Statistics](#) setting. The number of machines displayed can set to a maximum of 20.

Note: This report requires the Network Access ([page 48](#)) 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.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) ([page 469](#)). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) ([page 477](#)) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) ([page 287](#)).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Reports

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Uptime History

Reports > Uptime History

The [Uptime History](#) page 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.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Logs

Reports > Logs

The [Logs](#) page generates reports for the following types of log data maintained by the VSA.

- Alarm Log
- Admin Notes
- Agent Log
- Configuration Changes
- Network Statistics
- Remote Control Log
- Script Log
- Event Logs
- Event Log Frequency
- Log Monitoring
- EPS Log

Note: The EPS Log only displays if you have separately purchased the Kaseya Endpoint Security add-on module.

Selecting Log Report Options

The most commonly used options you can select for all log reports are:

- [Choose a log to display](#) - Select the type of log you want in the report.
- [Display log entries for last <N> days](#) - Specify the number of days worth of log data to display.
- [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.
- [Preserve plain text formatting](#) - Check this box to display plain text logs with the formatting from plain text files preserved in the HTML pages.
- [Ignore machines without data](#) - Check this box to only display machine IDs that have data matching the other filter parameters.

Additional fields display, depending on the type of log selected. These include:

- [Alarm Log](#) - Filter the report by the type of alarm. You can also filter alarm log entries by alarm email address, alarm email subject line, and/or alarm email message text.
- [Script Log](#) - Filter the report by script name and/or the administrator who scheduled the script.
- [Event Log](#) - You can also filter the report by a selected event set. By default the built-in [<All Events>](#) event set is selected. Event set alarm categories—[Error](#), [Warning](#), [Information](#), [Success audit](#), [Failure audit](#), [Critical](#), [Verbose](#)—must be checked to include an event in a report.

Reports

- **Event Log Frequency** - Enter a number of days in the [Select the <N> most frequent Event IDs for each Machine ID field](#). Then select an event log type. Event set alarm categories—[Error](#), [Warning](#), [Information](#), [Success audit](#), [Failure audit](#), [Critical](#), [Verbose](#)—must be checked to include an event in a report.
- **Log Monitoring** - Select a Log File Parser. Log file parsers are defined using Monitor > [Log Parser \(page 182\)](#).

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators \(page 469\)](#). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter \(page 477\)](#) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports \(page 287\)](#).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Ticketing

Reports > Ticketing

- Similar information is provided using [Ticketing > View Summary \(page 194\)](#).

The [Ticketing](#) page creates a report listing all trouble tickets assigned to selected machine IDs. Similar information is provided using [Ticketing > View Summary \(page 194\)](#).

The following options apply whether or not [Display all tickets](#) is checked.

- [Display all open tickets plus tickets closed within the last <N> days](#)
- [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 pie chart for each selected list](#) - Select multiple categories to display pie charts for.
- [Display ticket status chart for each admin](#) - Displays a separate ticket status bar chart for each administrator plus for unassigned.

The following options apply only if [Display all tickets](#) is checked.

- [Display all tickets](#) - Check this box to list tickets individually. If blank, only summary tables are displayed.
- [Display notes with each ticket](#) - Check this box to include all the detail notes with each ticket.
- [Hide hidden notes](#) - Check this box to hide hidden notes.
- [Fields...](#) - Click this button to select the columns to include in individually listed tickets.
- [Select column to sort on](#) - Select the column to sort tickets on.
- [ascending / descending](#) - Select whether to sort tickets in ascending or descending order.
- Filter tickets by
 - [Assignee](#)
 - [Category](#)
 - [Status](#)
 - [Priority](#)
 - [SLA Type](#)
 - [Dispatch Tech](#)
 - [Approval](#)

Note: The system does not delete tickets when deleting machine IDs. The ticket summary chart includes tickets matching the Machine ID and Group ID filters. Because no machine data exists for deleted Machine IDs, Views are not applied to this report.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators \(page 469\)](#). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the

Reports

administrator that created the report. [Shared](#) reports can be viewed and run by all administrators. Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (*page 477*) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (*page 287*).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Backup

Reports > Backup

- Similar information is provided using [Backup > Backup Status](#).

The [Backup](#) page generates a report summarizing data retrieved from the backup logs.

Note: Displays only if you have purchased the Backup addon module.

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.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (*page 469*). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (*page 477*) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (*page 287*).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Monitor

Reports > Monitor

- Similar information is provided using [Monitor > Dashboard List \(page 88\)](#) and [Alarm Summary \(page 96\)](#).

The [Monitor Page](#) generates a report summarizing data retrieved from monitoring managed machines.

- [Choose a report type](#) - Select the type of monitoring report to generate. Each monitoring report displays additional options.
- [Monitor Set Report](#)
 - Select Monitor Set
 - Display Last <N> Periods
- [Monitor Log Report](#)
 - Show <N> log entries for each counter and machine
 - Show counter log data
 - Show service log data
 - Show process log data
 - Show SNMP log data
- [Monitor Action Log Report](#) - Displays the actions taken in response to each alarm.
 - Display monitor action log entries for the last <N> days
 - Sort by log event date time: ascending / descending
 - Monitor type: <All Types>, Counter, Process, Service, SNMP, Alert, System Check, EPS, Log Monitoring
 - Message Filter
- [Alarm Summary Report](#)
 - Display all monitoring alarms for the last <N> days
 - Sort by log event date time: ascending / descending
 - Monitor Type: <All Types>, Counter, Process, Service, SNMP, Alert, System Check, EPS, Log Monitoring
 - Alarm Type: Alarm or Trending
 - Message Filter
 - Display message with each alarm
- [Monitor Trending Report](#)
 - Select Machine
- [Monitor Configuration Report](#)
 - Assigned Sets
 - Sets to be Displayed
 - List Only Assigned Sets
- [Monitor 95th Percentile Report](#)

This report specifies two dates and calculates the 95th percentile, meaning 95% of the time the value is below what is calculated in the report. The report supports SLA and planning calculations.

- Select Set
- Display 95th percentile between <start date> and <end date>

- Select the counters to add to the report

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Security

Reports > Security

- Similar information is provided using Security > Security Status, View Logs, and View Threats.

The Security page generates reports for the following types of security data maintained by the VSA.

Note: Displays only if you have purchased the Security add-on module.

Select security report type

Select the type of security report to generate:

- **Configuration Report**
 - Install Time
 - Installer
 - Version
 - License Expiration
 - Assigned Profile
 - Profile Details
 - Alarm Settings
- **Current Threats Report**
 - Summary
 - Threat Category Summary
 - Current Threats
- **Historical Threats Report**
 - Summary
 - Threat Category Summary
 - Current Threats

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for **master administrators** (page 469). Reports are always private for standard administrators. As a master administrator select **Shared** or **Private** to assign access to a report. By default, **Private** access is selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click **Save** to save the current settings.

Save As...

Click **Save as...** to save the current report under a new name.

Rename...

Click **Rename...** to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (*page 477*) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (*page 287*).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

User State

Reports > User State

- Similar information is provided using [User State > Power Status](#).

The [User State](#) page generates reports for the following types of user state data maintained by the VSA.

Note: This report displays only if you have purchased the User State addon module.

Select the subtopics to include in the User State 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 directories shares for the machine.
- [Include machines with no data](#) - Show entries in the report for all machines, including those that have not had user state information collected.

Running the Report

1. Select the data you want to display in the report.
2. Enter the title of the report.
3. Either run the report or export the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for [master administrators](#) (page 469). Reports are always private for standard administrators. As a master administrator select [Shared](#) or [Private](#) to assign access to a report. By default, [Private](#) access is selected. [Private](#) reports can only be viewed and run by the administrator that created the report. [Shared](#) reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#)

to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Power Savings

Reports > Power Savings

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 User State Management client installed*.

Note: This report displays only if you have purchased the User State addon module.

Step 1

Select the power setting states you want to compare.

- **Compare machine baseline audit information 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 KUSM installed along with the results from machines with KUSM installed. Checked by default. Does not include Windows 2000 or Vista machines.
- **Compare most recent power audit data 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 User State was installed on the machine.
 - **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.

Note: 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 472), typically on a daily basis.

Step 2

Set the values that the power savings estimate is based on:

- **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.

Reports

- **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.
 - **Hard Drive Watts** - Enter the number of watts a hard drive uses.
 - **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.
 - **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.
- **% of Machines Powered Down at end of Day** - Enter the number of machines that are physically turned off at the end of the day.
- **Include Monitors for Servers** - If checked, the calculation assumes each server has a monitor attached and the power settings for the monitors are included.
- **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.
- **Show Settings per User** - If checked, the report shows the savings for each user on each machine.
- **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.

Step 3

Report Period - Enter the reporting period for the report: Year, Month, From Baseline Collection Time.

Step 4

Enter the title of the report.

Step 5

Either **Run...** the report or **Export...** the report to HTML, Word or Excel output.

Share Report / Private Report

These two options only display for **master administrators** (page 469). Reports are always private for standard administrators. As a master administrator select **Shared** or **Private** to assign access to a report. By default, **Private** access is selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Saved reports are identified as either private  or shared  in the left-hand navigation pane.

Save

Click [Save](#) to save the current settings.

Save As...

Click [Save as...](#) to save the current report under a new name.

Rename...

Click [Rename...](#) to rename the report.

Delete...

Click [Delete...](#) to delete the report.

Enter title displayed on report header

Enter the title that displays at the top of the report.

Update

Reports are saved with the [Machine ID / Group ID filter](#) (page 477) settings that were current at the time the report was first saved or last updated. *These saved or updated filter settings are used when a report is run, regardless of the current machine ID/group ID filter settings.* Once a report has been saved, the [Update](#) button displays just below the field used to enter the title of the report. Click [Update](#) to apply the latest machine ID / group ID filter settings to a saved report. The machine ID / group ID filter settings of a saved report can be overridden using [Schedule Reports](#) (page 287).

Run...

Click [Run...](#) to run the report using the report options previously selected.

Save the report as HTML, Word or Excel

Click [Export...](#) to display the report as HTML, Word or Excel output. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Remove header from the exported report

If checked, the title, report date and machine filter information do not display at the top of the exported output.

Chapter 11

Agent

In This Chapter

Agent Tab	324
Agent Status	325
Agent Logs	327
Log History	328
Event Log Settings	329
Deploy Agents	331
Create	341
Delete	344
Rename	346
Change Group	347
LAN Watch	348
Install Agents	351
View LAN	354
View AD Computers	354
View AD Users	355
View vPro	358
Copy Settings	358
Import / Export	360
Suspend	360
Agent Menu	361
Check-In Control	363
Temp Directory	366
Edit Profile / User Profiles	367
User Access	369
Set Credential	371
Update Agent	372

Agent Tab

Agent

Functions in the [Agent](#) tab allow administrators to create, edit, and delete machine IDs, customize the appearance of the machine's agent icon  in the [system tray](#) (on page 483), control agent check-in frequency, and update the version of agent software that resides on managed machines.

Note: You can download an [Agent Configuration and Deployment PDF](#) from the first topic of online help.

Functions	Description
Agent Status (page 325)	Displays active user accounts, IP addresses and last check-in times.
Agent Logs (page 327)	Displays logs of: <ul style="list-style-type: none"> • Agent system and error messages • Execution of scripts, whether successful or failed. • Configuration changes made by an administrator. • Send/receive data for applications that access the network. • Application, System, and Security NT Event Log data collected from managed machine.
Log History (page 328)	Specifies how long to store log data.
Event Log Settings (page 328)	Specifies the event log types and categories included in the Log History.
Deploy Agents (page 331)	Creates agent install packages for multiple machines.
Create (page 341)	Creates machine accounts and/or install packages for single machines.
Delete (page 344)	Allows administrators to delete machine accounts.
Rename (page 346)	Renames existing machine ID accounts.
Change Group (page 347)	Reassigns any number of machines to a new group ID.
LAN Watch (page 348)	Uses an existing agent on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran.
Install Agents (page 351)	Installs the agent <i>on a remote system</i> and creates a new machine ID / group ID account for any new PC detected by LAN Watch.
View LAN (page 354)	Displays the results of the latest LAN Watch scan.
View AD Computers (page 354)	Lists all computers listed in an Active Directory when LAN Watch runs on a system hosting Active Directory. Installs agents on AD machines.
View AD Users (page 355)	Lists all Active Directory users discovered by LAN Watch when LAN Watch runs on a system hosting Active Directory. Creates VSA administrators and users from AD users.
View vPro (page 358)	Displays hardware information about vPro-enabled

	machines discovered while running LAN Watch.
Copy Settings (page 358)	Mass copies settings from one machine account to other machine accounts.
Import / Export (page 360)	Imports and exports agent settings, including script schedules, as XML files.
Suspend (page 360)	Suspends all agent operations, such as scripts, monitoring, and patching, without changing the agent's settings.
Agent Menu (page 361)	Customizes the agent menu on managed machines.
Check-In Control (page 363)	Controls agent check-in frequency on agent machines.
Temp Directory (page 366)	Sets the path to a directory used by the agent to store temporary files.
Edit Profile (page 210)	Edits machine account information.
User Access (page 212)	Sets up accounts to allow users remote control access to their own machines.
Set Credential (page 371)	Sets a logon credential for the agent to use in Patch Management, the Use Credential script command, backups, and User State Management.
Update Agent (page 372)	Updates the agent software on managed machines.

Agent Status

Agent > Agent Status

- [Agent status alerts can be defined using Monitoring > Alerts > Agent Status](#) (page 103).

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. The same options available in this display are available in the [Aggregate Table](#) (page 294) report. Paging rows can be sorted by clicking column heading links.

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 into, 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

- [Machine ID](#) - Machine ID label used throughout the system.
- [Group ID](#) - Just the group ID portion of the machine ID.
- [First Checkin Time](#) - Time when a machine first checked into the KServer.
- [Last Checkin Time](#) - Most recent time when a machine checked into the KServer.

Agent

- **Last Reboot Time** - Time of the last known reboot of the machine.
- **Current User** - Logon name of the user currently logged into the machine (if any).
- **Last Logged In User** - Logon name of the last person to log into the machine.
- **User Access Logon** - Logon name given to a user for logging into the KServer.
- **Computer Name** - Computer name assigned to the machine.
- **agent GUID** - A globally unique identifier for a machine ID.group ID account and its corresponding agent.
- **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.
- **Domain/Workstation** - The workgroup or domain the computer belongs to.
- **Operating System** - Operation system type the machine is running.
- **OS Version** - Operation system version string.
- **IP Address** - IP 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 KServer when this machine checks in. If the machine is behind a DHCP server, this will be the public IP address of the subnet.
- **MAC Address** - MAC address of the LAN card used to communicate with the KServer.
- **DNS Server 1,2** - IP address of the DNS servers assigned to the machine.
- **Primary/Secondary WINS** - WINS settings.
- **CPU Type** - Processor make and model.
- **CPU Speed** - Clock speed of the processor.
- **RAM Size** - MBytes of RAM on the machine.
- **Agent Version** - Version number of the Kaseya agent loaded on the machine.
- **User Access Remote Cntl** - Enabled if this user can log in and get remote control access *to their own machine from another machine*. Disabled if access is denied.
- **User Access Ticketing** - Enabled if this user can log in and enter trouble tickets. Disabled if access is denied.
- **User Access Chat** - Enabled if this user can *initiate* chat sessions with an administrator. Disabled if access is denied.
- **Primary/Secondary KServer Address** - IP address / name the machine uses to communicate with the KServer.
- **Quick Checkin Period** - **Quick check in** (*page 473*) time setting in seconds.
- **Contact Name** - User name entered in **Edit Profile** (*page 210*).
- **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.
- **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.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Agent Logs

Agent > Agent Logs

The [Agent Logs](#) page collects event information on or relating to managed machines.

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 328](#)).

Select Log

Select a log from the [Select Log](#) drop down list. Then click the hyperlink of a machine ID. The types of logs available include:

- [Alarm Log](#) - Lists all alarms triggered for the selected machine.
- [Agent Log](#) - Displays a log of agent, system, and error messages.
- [Configuration Changes](#) - Displays a log of configuration changes made by each Administrator.
- [Network Statistics](#) - Displays a log of send/receive data for network applications.
- [Event Logs](#) - Displays event log data collected by Windows. Not available for Win9x. Only event logs that apply to the specific machine selected display in the event log drop-down list.
- [Script Log](#) - Displays a log of successful/failed scripts.
- [Remote Control Log](#) - Displays a log of successful/failed remote control sessions.
- [Log Monitoring](#) - Displays [Log Monitoring](#) ([page 476](#)) entries.

Agent

Events Per Page

Select the number of rows displayed per page.

Start Date / End Date

Select a range of dates to filter log data.

Filter...

Applies to the Event Log 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 the Event Log 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 > 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 327) or printed to a report using [Reports > Logs](#) (page 309). 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 > Configure](#) (page 394). Changes made using this page take effect at the next agent check-in and display **in red text** until then.

Note: Log Settings can also be maintained using the Agent Settings tab of the Machine Summary (page 21) page.

These settings default from the agent install package. Agent install packages are created using [Agent > Deploy Agent](#) (page 331).

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 `nventlog` 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

Set the number of days to keep log data for each type of log:

- [Agent Log](#) - The log of agent, system, and error messages.
- [Configuration Changes](#) - The log of configuration changes made by each administrator.
- [Network Statistics Log](#) - 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 327) > [Network Statistics](#).
- [Script Log](#) - Displays a log of successful/failed scripts.
- [Remote Control Log](#) - Displays a log of remote control events.

- **Alarms Log** - The log of all alarms issued.
- **Event Log** - The log of all events. The events collected are specified in more detail using [Agent > Event Log Settings](#) (page 329).
- **Monitor Log** - The log of data collected by monitoring sets.
- **SNMP Log** - The log of all data collected by SNMP sets.
- **SYS log** - The log of all [System Check](#) (page 154) external systems.

Note: [System > Check-in Policy](#) (page 382) can restrict the number of days administrators can keep log entries, to avoid placing undue stress on servers running the KServer service.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Event Log Settings

Agent > Event Log Settings

The [Event Log Settings](#) page specifies the [event log](#) (page 474) types and categories included in the [Log History](#) (page 328).

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 >](#) or [Add all >>](#) 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.

Agent

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 475)—are uploaded to the KServer 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 log to record that collection has been suspended. 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 KServer. 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

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Delete Icon

Click the delete icon  to delete an event log.

Edit icon

Click the edit icon  next to a event log to automatically set header parameters to those matching the selected event log.

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.
- Verbose - Applies only to Vista.

Deploy Agents

Agent > Deploy Agents

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

Note: You can download a PDF overview of Agent Configuration and Deployment from the top topic of online help.

Note: Use [Agent > Create](#) (page 341) to create a machine ID account and agent install package in two separate steps and apply them to a *single* machine. You can also use [Create](#) to create machine ID templates (page 477) or re-install an agent for an *existing* machine ID.

Note: Use [Install Agent](#) (page 351) to install agents *on remote systems*.

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the [machine ID / group ID](#) (page 476) and the [agent](#) (page 470). The machine ID / group ID is the VSA's [user account name](#) for a managed machine in its 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 machine ID / group ID account name on the VSA. Tasks assigned to a machine ID by a VSA administrator direct the agent's actions on the managed machine.

Using the Wizard

The [Deploy Agents](#) install package is created using a [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.exe`. All settings and pending scripts from the machine ID you copy from—except the machine ID and group ID—are applied to every new machine ID created with the package.

Automatic Account Creation

You must have *automatic account creation enabled* using System > [Check-in Policy](#) (page 382) to automatically create a machine ID account when a [Deploy Agents](#) package is installed.

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

Agent

many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are copied from a selected machine ID template. Typically machine ID templates are 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 341).
- Import a machine ID template using Agent > [Import/Export](#) (page 360). Sample templates can be downloaded from the Kaseya Support Forum and imported.
- Base an agent install package on machine ID template using Agent > [Deploy Agents](#) (page 331).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > [Copy Settings](#) (page 358).
- Identify the total number of machine ID template accounts in your VSA using System > [Statistics](#) (page 401).
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.

Including Credentials in Agent Install Packages

If necessary, an agent install package can be created that includes an administrator [credential](#) (page 473) 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.

Editing Existing Install Packages

Typically an existing [Deploy Agents](#) install package is edited just before re-distribution. The most common changes made to an install package are:

- Pre-selecting a group ID and sub-group ID. A group ID usually represents a single customer. A sub-group ID is sometimes used to represent a specific customer location.
- Assigning a credential, if necessary.

Once edited the install package can be re-created and distributed to the specific customer and location it is intended for.

Distribution Methods

Once created, you can use the following methods to distribute an agent install package:

- [Logon Scripts](#) - Set up an [NT logon script](#) to run the install package every time a user logs into the network. The installer skips installation if it detects an agent is already on a machine.
 1. Create the deployment package using the Agent > [Deploy Agents](#) wizard.
 - ✓ You will probably want to select the silent install option.
 - ✓ It may be necessary to bind an administrator credential if users running the logon script don't have administrator rights.
 2. Download the `KcsSetup.exe` using the `dl.asp` page and copy it to a network share which users can execute programs from.
 3. Add `KcsSetup.exe` with its network path to the logon script.
- [Email](#) - Email `KcsSetup.exe` to all users on the network. Download the 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.
- [LAN Watch](#) - Administrators can discover newly added machines during a [LAN Watch](#) (page 348) and subsequently install agents *remotely* using the Agent > [Install Agents](#) (page 351) page.
- [Manually](#) - You can instruct users to download an install package agent from the <http://your.Kserver.com/dl.asp> website to their target machines. If more than one install package is displayed on the website, instruct them which package should be selected. Users can execute the `KcsSetup.exe` using any of the following three methods:

- Double click `KcsSetup.exe` within Windows to launch it.
 - Open a [command line window](#) and type `KcsSetup.exe` followed by any desired [command line switches](#) (page 335).
 - Select [Run...](#) from the [Windows Start](#) menu and type `KcsSetup.exe` followed by any desired command line switches.
- [Macintosh](#) - See [Deploying Macintosh Agents using Apple Remote Desktop](#) (page 337).

Default Administrator Install Packages

Each administrator can specify their own default install package by selecting the [Set Default](#) radio button to the left of the package name. Administrators can download their own default agent immediately by selecting the [Click to download default Agent](#) link on the [Deploy Agents](#) page.

Unique ID Number

You can tell users which install package to download by referencing the install package's *unique ID number*. Example: <http://your.kserver.com/dl.asp?id=123>. The default install package is displayed with its unique ID number in the header of the [Deploy Agents](#) page.

Assigning New Machine IDs to Machine Group by IP Address

Using [Deploy Agents](#), 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, a `System > Naming Policy` (page 380) assigns it to the correct group ID and/or sub-group ID.

Windows vs. Macintosh

Agent packages can be created to install agents on machines running either Windows or Macintosh operating systems. See [Deploying Macintosh Agents using Apple Remote Desktop](#) (page 337).

Create Package

Click [Create Package](#) to start a [Configure Automatic Account Creation](#) wizard where you can specify all configuration parameters for the install package. 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.
 - Specify the machine ID for this install package.
 - Set the user name of the currently logged on user as the machine ID.
2. Define rules for naming the group ID.
 - [Prompt User](#) - Asks user to enter a group ID. This option is only displayed to master administrators.
 - [Domain Name](#) - Uses the user's domain name.
 - [Existing Group](#) - Select an existing group ID from a drop down list.
 - [New Group](#) - Specify a new group ID. This option is only displayed to master administrators.
3. Specify agent install package [command line switches](#) (page 335) including the ability to install [silently without any task bars or dialog boxes](#) (page 480).
4. Specify the machine ID to copy settings and pending scripts from. All settings and pending scripts from the machine ID you copy from—except the machine ID and group ID—are applied to every new machine ID created with the package.

Note: The statement `Copy settings from unknown.unnamed.unnamed-org` if nothing selected is based on the machine ID or template selected by the Default Install package. See [Editing the Default Install Package](#) below.

Agent

5. Select the operating system you are creating the install package for: Windows or Macintosh. See [Deploying Macintosh Agents using Apple Remote Desktop](#) (page 337).
6. Optionally bind an administrator logon credential to the install package. Fill in the **Administrator Credential** form to securely bind administrator 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.

Note: Credentials are only necessary if users are installing packages on machines and do not have administrator access to their network.

7. Name the install package for easy reference later. This name displays on the **Deploy Agents** page and the `dl.asp` download page.

Note: The filename of the agent install package is always `KcsSetup.exe`.

Install Issues and Failures

See [Install Issues and Failures](#) (page 340) if an agent fails to install.

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 administrator*:

1. Click the **Share** button next to the Default Install package in Agent > Deploy Agents.
2. Click **Take Ownership**.
3. Check **Allow other administrators to modify**.
4. Click **Save**.
5. 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.

Click to download default Agent

Click this link to download the current administrator's default package directly from this page.

Users can download agents from

Right click the displayed link and select the **Copy Shortcut** option, then paste this shortcut 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.

Set Default

Specify your own administrator 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 administrator's lists.

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 a private package with other administrators, administrator roles or to make the package public. If a package is public, click [Share](#) to take ownership of the public package and make changes to it. Only master administrators can make a package public and available to all administrators.

List on dl.asp

Click the [dl.asp](#) link in the column header to display the web page 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.

Agent Install Command Line Switches

Agent install command line switches for `KcsSetup.exe` are case insensitive and order independent. Separate switches with an empty space.

`/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 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 user will be 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 scripts. `/k` or `/r` overrides `/e`.

`/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.

`/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.

Agent

`/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(.).

`/p "install_path"` - Overrides the default installation path by specifying the full directory path, including drive letter, in which to install the agent. By default, the agent installation creates a directory named `Program Files\Kaseya\Agent` off the root of the drive on which Windows is installed.

`/r` - Executes the installation program and reinstalls 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 user during installation. The default title is: "Kaseya Agent".

`/u` - Uses the current user name as the machine ID for the new account. If the 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.

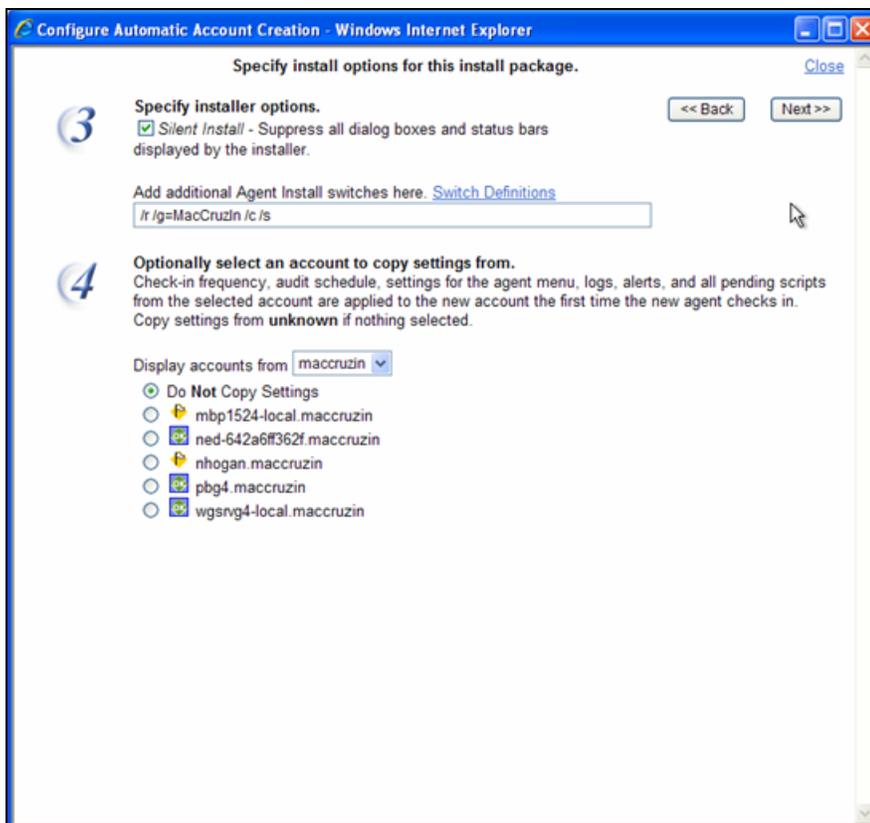
`/w` - Overwrites the existing configuration file with a configuration file included in the agent installation. Use with the `/r` switch to re-install an agent with new server settings. Intended for an existing agent that is attempting to connect to a server that no longer exists.

`/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."

Deploying Macintosh Agents using Apple Remote Desktop

1. Use the **Configure Automatic Account Creation** wizard in Agent > **Deploy Agent** (page 331) to configure an agent installation package with the desired options. Silent mode is recommended, but not required.



2. Select a Macintosh agent type.

Agent

3. Enter an existing OS X **Administrator Credential** username and password for the agent to use. This step is required if you wish to install the agent without a prompt and user/admin interaction.

Download Agent - Windows Internet Explorer

Name the install package. Close

5 Select agent type. Macintosh << Back Save

6 Securely bind administrator credentials to the install package?

Administrator Credential

Username:

Password:

Confirm:

Domain:

Successful installation may require Administrator rights. Fill in the administrator credential form to securely bind administrator rights to the install package. Users with minimal rights can then install the Agent. If the administrator credential is left blank and the user does not have rights to install software, the installer prompts for an administrator credential.

7 Name the install package. Give this package a name and short description so you will remember this configuration when you use it.

Package Name

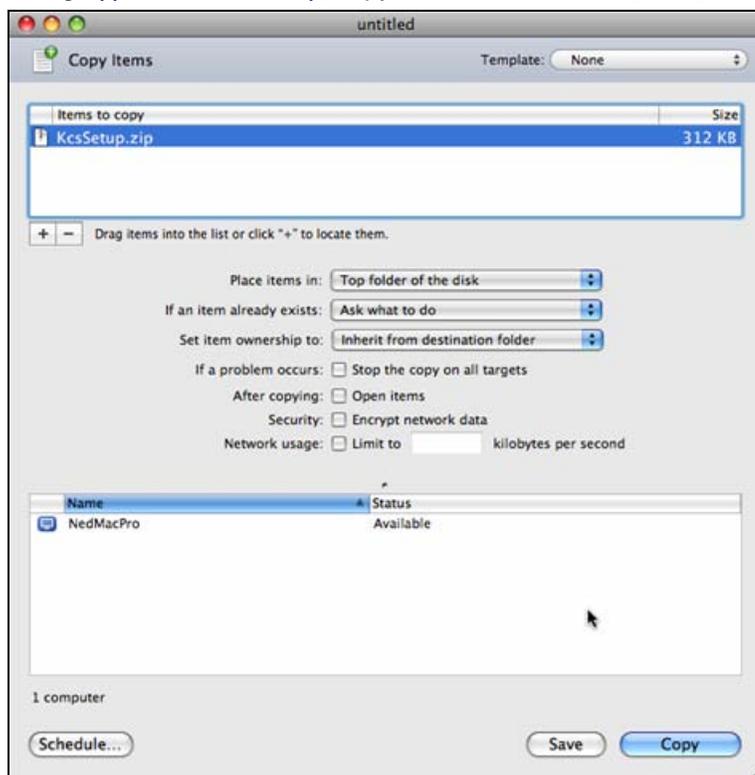
Package description

4. Download and capture the `KscSetup.zip` file created by the Deploy Agent wizard located at http://VSA_server.mydomain.com/dl.asp.

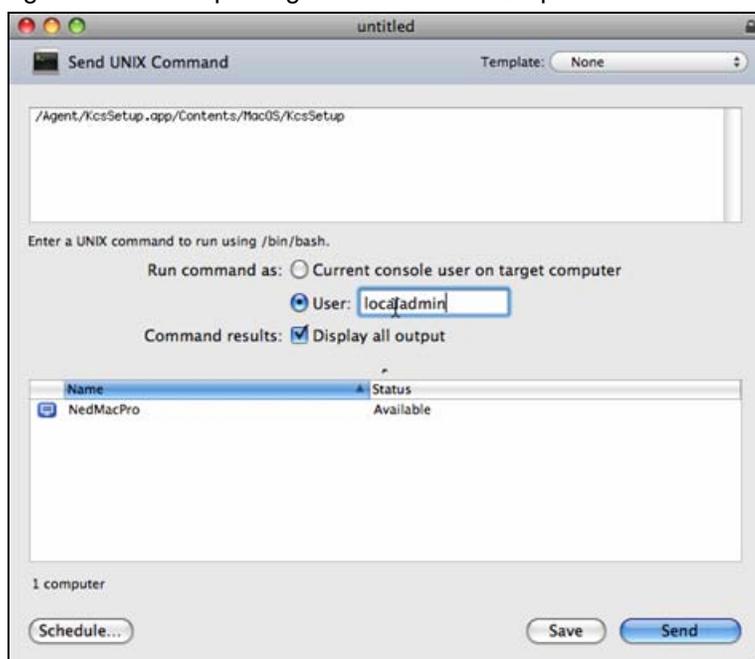
Note: You may need to disable the open feature of "safe" files in Safari.



5. Using [Apple Remote Desktop](#), copy the saved `KcsSetup.zip` file to the desired list of computers.



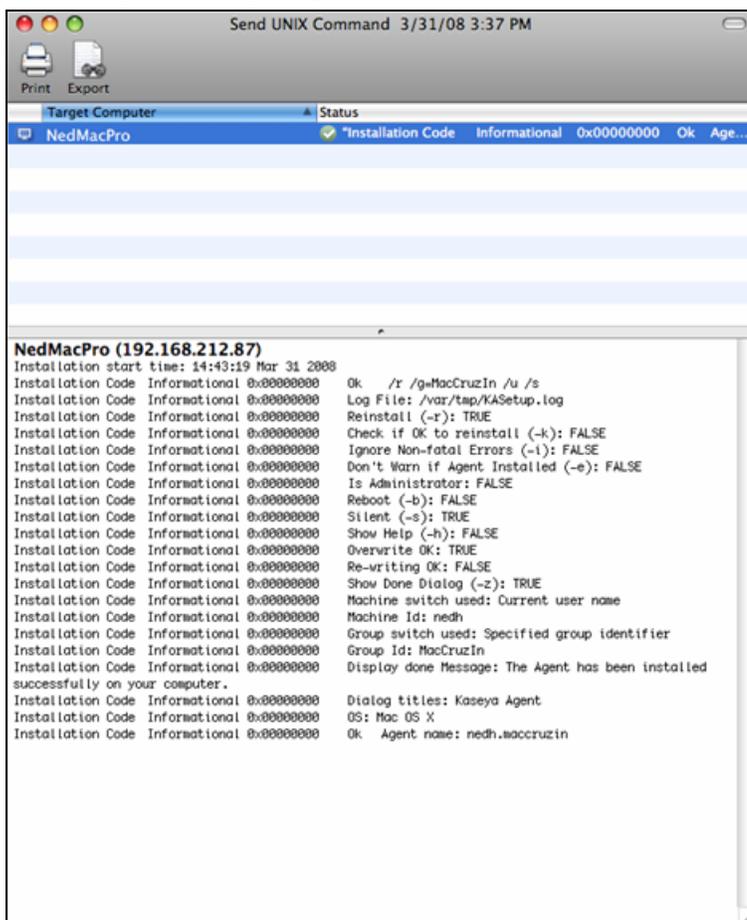
6. Unzip the `KcsSetup.zip` file and execute the `KcsSetup.exe` as either the local admin or a user of your choice. Entering a credential is not required if a credential was included when the agent installation package was created in Step 3 above.



The agent is installed in the background. It then launches and displays the Kaseya icon on the menu bar of any user logged on the Macintosh machine. If no users are currently logged on, the agent launches on next logon,

Agent

- To check the status of the deployment or look for errors, you can review the log file found in `/var/tmp/KASetup.log`.



- To configure custom agent icons for Macintosh machines, see [Creating Custom Agent Icons](#) (page 407).

Install Issues and Failures

The following issues and failures can occur when installing agents:

- Invalid Credential** - The [credential](#) (page 473) 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 username may be a domain administrator of the form `domain\user`.
- 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.

Macintosh

- Macintosh agents cannot be deployed silently.

Using Active Directory

These types of failures apply when an agent is installed using [View AD Computers](#) (page 354) or [View AD Users](#) (page 354):

- [Port Blocked](#) - Active Directory agent deployment will fail if the Kserver assigned port is blocked by a firewall.
- [Authentication Requirement for AD Imported Users](#) - The domain controller that performs the authentication must have [Authenticated users](#) set as a member of [Local Security policy - Access this computer from the network](#).

Create

Agent > 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 477) are not intended for installation to a machine.
- [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 as an administrator to install the package.

Note: Use [Agent > Deploy Agents](#) (page 331) 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 382).

Note: Use [Install Agent](#) (page 351) to install agents *on remote systems*.

Re-Installing Agents

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.

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the [machine ID / group ID](#) (page 476) and the [agent](#) (page 470). The machine ID / group ID is the VSA's [user account name](#) for a managed machine in its 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 machine ID / group ID account name on the VSA. Tasks assigned to a machine ID by a VSA administrator 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 477). Machine ID template accounts are not counted as "used" until you install the agent.

Agent

Including Credentials in Agent Install Packages

If necessary, an agent install package can be created that includes an administrator [credential](#) (page 473) 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.

Windows vs. Macintosh

Agent packages can be created to install agents on machines running either Windows or Macintosh operating systems.

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 copied from a selected machine ID template. Typically machine ID templates are 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 341).
- Import a machine ID template using Agent > [Import/Export](#) (page 360). Sample templates can be downloaded from the Kaseya Support Forum and imported.
- Base an agent install package on machine ID template using Agent > [Deploy Agents](#) (page 331).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > [Copy Settings](#) (page 358).
- Identify the total number of machine ID template accounts in your VSA using System > [Statistics](#) (page 401).
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.

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 KServer defaults. You can copy settings between existing machine ID accounts at any time using Agent > Copy Settings (page 358).

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 `unnamed`. Group IDs are created by an administrator using the System > Admin Accounts: [Create / Delete](#) (page 388) page.

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. Select a group ID.
 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 if a master administrator is logged on.

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. Click the [Set](#) to ensure that new machine IDs created without a group default machine ID copy settings from the master administrator's default machine ID.
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 210*) page. Contact information includes:

- **Contact Email** - Enter the email address of the individual using the managed machine
- **Auto Assign** - Check [Auto Assign](#) 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.

Note: This field is required to generate a new password for the Agent > User Access (*page 212*) page.

- **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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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.

Agent

Note: An install package created using this page is for a specific machine ID account. Use Deploy Agent (page 331) to create install packages for *multiple* machines.

1. Select the operating system you are creating the install package for: Windows or Macintosh.
2. Optionally bind an administrator logon credential to the install package. Fill in the [Administrator Credential](#) form to securely bind administrator 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.
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.exe`.
 - [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

First Checkin

Lists the time that each agent checked into the server for the first time.

Delete

[Agent](#) > [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](#) (page 476) and the [agent](#) (page 470). The machine ID / group ID is the VSA's [user account name](#) for a managed machine in its 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 machine ID / group ID account name on the VSA. Tasks assigned to a machine ID by a VSA administrator 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 477). Machine ID template accounts are not counted as "used" until you install the agent.

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 KServer. 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 KServer.
 - [Uninstall the agent and keep the account](#) - Uninstall the agent from the machine **without** removing the machine ID account from the KServer.
1. Click the [Delete Accounts](#) button.

Note: Uninstalling an agent does not remove the installed remote control package. Before you delete the agent, use [Remote Control > Uninstall RC \(page 273\)](#) to uninstall remote control on the managed machine.

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 KServer 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs \(page 476\)](#) displayed is based on the [Machine ID / Group ID filter \(page 17\)](#) and the machine groups the administrator is authorized to see using [System > Group Access \(page 385\)](#).

Last Check-In

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

Rename

Agent > 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 an unique GUID number. Renaming the agent only changes the name the agent displays, both on the KServer and in the [Set Account...](#) option on the agent menu of the user's managed machine.

Note: See [Alert > Change Group \(page 347\)](#) 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 for machine ID accounts you wish to rename.
 - [Merge offline account <Offline Machine ID> into <Select Machine ID> Delete <Offline Machine ID> after merge](#) - Use merge to combine log data in two different accounts that pertain to the same machine. This could be necessary if an agent was uninstalled and then reinstalled with a different account name. Merge combines the accounts as follows:
 - ✓ Log data from both accounts are combined.
 - ✓ [Baseline Audit \(page 472\)](#) data from the old offline account replaces any baseline data in the selected account.
 - ✓ Alert setting from the selected account are kept.
 - ✓ Pending scripts from the selected account are kept. Pending scripts 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:



Agent has checked in



Agent has checked in and user is logged on. Tool tip lists the logon name.

-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385). 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](#) > [Change Group](#)

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

Moving an 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.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Agent

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

LAN Watch

[Monitor](#) > LAN Watch

[Agent](#) > LAN Watch

LAN Watch uses an existing [agent](#) (page 470) on a managed machine to periodically scan the 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 or [SNMP devices](#) (page 481). Optionally, the VSA can send an [alert](#) (page 471) 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.

Using Multiple Machines on the Same LAN

There are only two reasons to do a SNMP LAN Watch on multiple machines within a scan range:

1. There are multiple SNMP Communities within the scan range and therefore there are multiple machines with different SNMP Community Read values.
2. The user wishes to have redundant SNMP monitoring.

Schedule

Click [Schedule](#) to schedule a recurring LAN Watch scan on each selected machine ID. The scan runs every interval that you set. The default is 1 day.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click [Cancel](#) to stop the scheduled scan. Cancel also deletes all records of the devices identified on a LAN from the VSA. If you re-schedule LAN Watch after clicking Cancel, each device on the LAN generates a new alert.

Run recurring every <N> <periods>

Check the box to make this task a recurring task. Enter the number of times to run this task each time period.

Scan IP Range

Set the minimum and maximum IP addresses to scan here. Selecting a machine ID to scan, by checking the box next to that machine's name, automatically fills in the minimum and maximum IP range based on that machine's IP address and subnet mask.

Note: LAN Watch does not scan more than 2048 IP addresses. If the subnet mask of the machine running LAN Watch specifies a larger IP range, LAN Watch truncates it to 2048 addresses. LAN Watch only detects addresses on the local subnet to the machine you run LAN Watch from. For example, with a subnet mask of 255.255.255.0, there can be no more than 253 other devices on the local subnet.

Enable SNMP

If checked, scan for [SNMP devices](#) (page 481) within the specified [Scan IP Range](#).

Read Community Name / Confirm

LAN Watch can only identify SNMP devices that share the same [SNMP Community](#) (page 481) [Read](#) value as the managed machine performing the LAN Watch. Enter the value in the [Read Community Name](#) and [Confirm](#) text boxes.

Note: Community names are *case sensitive*. Typically the default read community name value is `public`, but may be reset by an administrator to `Public`, `PUBLIC`, etc.

Enable vPro

If checked, identify [vPro](#) (page 486)-enabled machines within the specified [Scan IP Range](#). A machine does not need to be a vPro machine to discover vPro machines using LAN Watch. If a vPro machine is used as the LAN Watch discovery machine, it cannot discover itself.

Note: vPro configuration is a prerequisite to using this feature. Refer to the latest Intel documentation for information on how to configure vPro. At the time of this writing, the following link leads to the Intel documentation: <http://communities.intel.com/docs/DOC-1429>.

Username / Password / Confirm

Enter the appropriate vPro credentials to return hardware asset details about vPro machines discovered during the LAN Watch. Typically the same credentials are defined for vPro machines on the same LAN. The results are displayed using Agent > [View vPro](#) (page 358).

If you don't know the credentials for the vPro machines you want to discover, enter *arbitrary strings* in the [Username](#), [Password](#) and [Confirm](#) fields. This will allow you to discover the existence of the vPro machines, but not return any other hardware assets details.

Note: vPro-enabled machines with a vPro credential can be powered up, powered-down or rebooted using [Remote Cntl > Power Mgmt](#) (page 268).

Enable Alerts

If [Enable Alerts](#) is checked and a new device is discovered by LAN Watch, an alert is sent to all email addresses listed in [Email Recipients](#). LAN Watch alerts and email recipients can also be specified using the [Monitor > Alerts](#) (page 100) page.

Note: Machines that have not connected to the LAN for more than 7 days and then connect are flagged as new devices and will generate an alert.

Email Recipients

If alerts are enabled, enter the email addresses where alert notifications are sent. You can specify a different email address for each managed machine, even if it is for the same event. The [From](#) email address is specified using [System > Configure](#) (page 394).

Ignore devices seen in the last <N> days

Enter the number of days to suppress alerts for new devices. This prevents creating alerts for devices that are connected to the network temporarily.

Agent

After alert run select script on this machine ID

If checked and an alarm condition is encountered, a script is run. You must click the [select script](#) link to choose a script to run. You can optionally direct the script 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 triggered the alarm condition.

Skip alert if MAC address matches existing agent

Checking this box suppresses alerts if the scan identifies that the MAC address of a network device belongs to an existing managed machine with an agent on it. Otherwise a managed machine that was offline for several days and comes back online triggers an unnecessary alert during a LAN Watch.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

IP Range Scanned

The IP addresses that are scanned by the selected machine ID when LAN Watch runs.

Last Scan

This timestamp shows when a machine ID was last scanned. When this date changes, new scan data is available to view.

Primary DC

If a primary domain controller icon  displays, this machine ID is a [primary domain controller](#) (page 479). If checked, performing a scan on a primary domain controller running Active Directory enables you "harvest" the users and computers throughout a domain. You can subsequently install VSA agents automatically on computers listed in Active Directory and create VSA administrators and VSA users based on Active Directory user credentials. See [View AD Computers](#) (page 354) and [View AD Users](#) (page 355).

SNMP Active

If the SNMP icon  displays, SNMP devices are included in the scheduled scan.

vPro Active

If the vPro icon  displays, vPro machines are included in the schedule scan.

Alert Active

If checked  LAN Watch alerts are enabled for this scan.

Install Agents

Agent > Install Agents

The [Install Agents](#) page installs the agent *on a remote system* and creates a new machine ID / group ID account for any new PC detected by [LAN Watch](#) (page 348). [Install Agent](#) remotely installs the packages created using [Deploy Agents](#) (page 331). Remote install is only available for Window NT, 2000, XP and Vista based computers.

A list of machines with scan results are displayed when you first display this page. Clicking any machine ID displays a table listing all machines [with a host name](#) (see "Host name" on page 475). Machines without an agent [display in red text](#).

PSEXEC.EXE

PSEXEC.EXE is a light-weight telnet-replacement that lets you execute processes on other systems without having to manually install client software. It used by Agent > [Install Agents](#) (page 351) to install agents *on remote systems* after a [LAN Watch](#) (page 476).

A valid logon with administrator rights is required to successfully install an agent remotely. Nothing happens if the agent installer detects an agent is already installed on a target machine. The installer exits immediately.

Uploading PSEXEC.EXE to the KServer

Before [Install Agents](#) can be run the first time, the PSEXEC.EXE must be uploaded to the KServer as a shared managed file:

1. Download the PSEXEC.EXE file to your local machine from the following location:
<http://www.microsoft.com/technet/sysinternals/utilities/psexec.msp>
2. Click the [Scripts](#) tab, then click the  toolbar button to display the [Manage Files Stored on Server](#) window.

Note: Only master administrators can upload to shared files.

3. Upload the PSEXEC.EXE file from your local machine to the KServer as a *shared* managed file.

Running PSEXEC.EXE

When [Install Agent](#) is run, PSEXEC.EXE is downloaded from the KServer into the `\temp` directory and run using the following command line. You don't have to create this command line. [Install Agent](#) does it for you.

```
c:\temp\psexec \\hostname -u "adminname" -p "password" -c -f -d
"c:\temp\kcssetup.exe" > c:\temp\LANInsAipAddr.txt
```

The terms `hostname` and `ipAddr` refer to the remote machine. If the agent is on a drive other than `C:` then the temp files are referenced to the same drive the agent is installed on.

Error Messages

If an agent installation fails for any reason, the KServer passes back the results reported by PSEXEC.EXE. Typically, PSEXEC.EXE is simply reporting OS errors that it received trying to execute a call.

Typical Reasons for Install Failure

- **Blocked by Network Security Policy** - PSEXEC.EXE connects to the remote PC through the RPC service and runs as a local account. Remote access to this service is controlled by a Local or Domain **Security Setting**. Open **Local Security Policy** (part of Administrative Tools). Open **Local Policies\Security Options\Network access: Sharing and security model for local accounts**. The policy must be set to **Classic** for PSEXEC.EXE to operate across the network.

Note: Classic is the default setting for machines that are members of a domain. Guest is the default setting for machines that are not in a domain. Microsoft does not allow Windows XP Home Edition to become a domain member.

- **Blocked by Anti-Virus Program** - PSEXEC.EXE is a powerful program capable of remotely running processes on a machine, assuming the it has a valid administrator logon. Some anti-virus programs classify PSEXEC.EXE as a security threat and may block its execution.
- **Invalid Credential** - The **credential** (page 473) must have administrator rights on the local machine. The agent installs as a system service requiring full administrator privileges to install successfully. The username may be a domain administrator of the form **domain\user**.

Testing Agent Install Failures

LAN Watch tries to connect to **Error! Hyperlink reference not valid.** using the credentials that you supplied. First test that the computer is available. Start a command prompt and type the following:

```
ping <IP address>
```

If you don't get a reply see **Troubleshooting** below. If you do get a reply, you know that the machine is turned on and a firewall is not blocking connections. Next, verify that the share is available. Start a command prompt and type the following:

```
start Error! Hyperlink reference not valid.
```

If you have a problem see **Troubleshooting** below. If all is OK a window appears containing the remote computer's **c:\windows** directory. Now, you now know that the machine is turned on and the share exists.

Next verify that the PSEXEC.EXE command works correctly. Remote control the machine *you ran LAN Watch on*. Start a command prompt and type:

```
c:\temp\psexec.exe Error! Hyperlink reference not valid.> -u <username> -p <password> ipconfig
```

You should see the results of **ipconfig** for the target computer displayed on the machine you are running remote control on. If not, the RPC service on the target machine is probably disabled and blocking remote procedure calls.

Troubleshooting

PSEXEC.EXE's ability to run processes remotely requires:

- Both local and remote computers have file and print sharing enabled.
- The default **admin\$** share—a hidden share that maps to the **\Windows** directory—is defined on the remote system.

Types of failures include:

- **Ping Failures** - Either the machine is not on, or there is a firewall on the machine stopping pings. Either of these will stop the process and need to be corrected before continuing.
- **Start Failures** - If Windows does not accept the username/password combination, you will see a box pop up asking you to try again. Correct the mistake and try again.

If you get a message saying that the **network path could not be found**, it means that the **admin\$** share is not available on that machine.

- **PSEXEC.EXE Fails to Connect** - The RPC service is not available on the target machine. For example, XP Home does not support RPC. This prevents anything from remotely executing on that box. On Windows XP you can turn this service on by opening Windows Explorer and selecting **Tools - Folder Option...** - **View** tab. Scroll to the bottom of the list and uncheck **Use simple file sharing**. The XP default configurations are as follows:
 - **XP Pro on a domain** - RPC **enabled** by default. **Use simple file sharing** is unchecked.
 - **XP Pro in a workgroup** - RPC **disabled** by default. **Use simple file sharing** is checked.
 - **XP Home** - RPC **disabled** always. **Use simple file sharing** is not available.
- The `admin$` share is a default share that windows creates when it boots, it is possible to turn this off via the local security policy, or domain policy.
If you want to check the shares on that remote machine you can use PSEXEC.EXE to retrieve a list for you. Type `PSEXEC Error! Hyperlink reference not valid.> "net share"`. Check that the `admin$` share exists and points to `c:\windows` or `c:\winnt` on older operating systems.

Admin Logon Name

The administrator name used to remotely access the selected machine. The **Admin Logon Name** must have administrator rights on the remote selected machine. Multiple accounts may have administrator rights on the same machine. Your domain administrator account may be different than the local administrator account. To ensure you are using the domain account enter the logon name using the `domain\user` format. If the domain is left off, the local account will be used.

Password

The password associated with the **Admin Logon Name**.

Install

Click **Install** to schedule an installation of the selected install package on all selected machines. The install runs using PSEXEC.EXE from the same machine that ran the scan. PSEXEC.EXE attempts to remotely connect to the selected machine across the LAN to perform the agent install using the supplied administrator **credential** (*page 473*) for that machine.

Cancel

Click **Cancel** to cancel execution of this task on selected managed machines.

Select an Agent Package to Install

Select the agent package to remotely install on selected machines. These packages are created using **Deploy Agents** (*page 331*).

Hide devices that match the MAC address of existing machine IDs

Check this box to hide all machines on a LAN with a **MAC address** (on *page 476*) matching the MAC address of an existing machine ID / group ID account.

Hide devices that match the computer names of existing machine in <machine ID>

Check this box to hide machines that have a common computer name in this same group ID. A LAN Watch may discover a managed machine with a second device using a different MAC ID than the one used to report to the KServer. For example, the same managed machine may connect to the internet using direct connection and have a second wireless connection with a different MAC ID. Checking this box hides the second device from this list so that you don't assume you've found a new unmanaged machine.

Agent

Host Name

The host name of each device on the LAN discovered by the latest LAN Watch scan. A host name only displays for computers. Hubs, switches, routers, or other network appliances do not return a host name.

IP Address

The private IP address of each device discovered by the latest LAN Watch scan.

MAC Address

The [MAC address](#) (on page 476) of each device discovered by the latest LAN Watch scan.

Last Seen

The time each device was last detected by the latest LAN Watch scan.

View LAN

Client > View LAN

The [View LAN](#) page displays the results of the latest [LAN Watch](#) (page 348) scan. A list of machines with scan results are displayed when you first display this page. Click any machine ID to display a table listing all machines with and without a [host name](#) (on page 475). Only machine IDs with returned scan data are available. Paging rows can be sorted by clicking column heading links.

Host Name

The host name of each device on the LAN discovered by the latest LAN Watch scan. A host name only displays for computers. Hubs, switches, routers, or other network appliances do not return a host name.

IP Address

The private IP address of each device discovered by the latest LAN Watch scan.

MAC Address

The [MAC address](#) (on page 476) of each device discovered by the latest LAN Watch scan.

Last Seen

The time each device was last detected by the latest LAN Watch scan.

View AD Computers

Agent > View AD Computers

The [View AD Computers](#) page shows all computers listed in an [Active Directory](#) (page 469) when [LAN Watch](#) (page 348) runs on a system hosting Active Directory. Use [View AD Computers](#) to install agents automatically on computers listed in the Active Directory by policy at computer startup. Using this method has the following benefits:

- This policy ensures an agent is always present on a machine at every reboot, even if the agent is subsequently removed by a user.
- Agents can be deployed to an entire AD network even if the VSA administrator does not know the local credentials for each computer.

- A LAN Watch scan performed by an AD machine discovers all computers that are members of a domain, *whether the machines are online or not*.

Note: You must select a *Detail View* to see AD computers listed on this page.

Switching From Summary View to Detail View

1. Select <All Groups> from the [Select Machine Group](#) drop-down list in the [Machine ID / Group ID filter](#) (page 477) to display a *summary view* of all domain controllers discovered by LAN Watch.
2. Identify the machine groups and subgroups listed in the [Discovered By](#) column.
3. Select one of the machine groups or subgroups in Step 2 above from the [Select Machine Group](#) drop-down list to display a *details view* of domain controllers for that machine group.

Summary View

The summary view of [View AD Computers](#) lists all domain controllers that have run LAN Watch for *all machine groups you're authorized to access*.

Discovered By

Lists the machine ID.group ID names of domain controllers that have performed a LAN Watch scan.

Computers Found

Lists the number of computers, *with or without agents*, listed in the domain controller directory.

Agent Installed

Lists the number of computers *with agents* that are also listed in the domain controller's directory.

Details View

The details view of [View AD Computers](#) displays computers listed in Active Directory services hosted on computers that have run LAN Watch *within a specified machine group*.

Installing Agents on Active Directory Computers

You can associate an install package with an AD computer. This installs an agent package when the AD computer reboots, unless the agent is already installed. You can specify the agent package installed for each AD computer.

Note: See [Install Issues and Failures](#) (page 340) if an agent fails to install.

To associate an install package with an AD computer:

1. Select AD computers listed in the [Canonical Name](#) (page 472) column of the paging area.
2. Select an agent package from the [Select an Agent Package to install](#) drop-down list.
3. Click [Install Agent Policy](#).

View AD Users

Agent > View AD Users

The [View AD Users](#) page lists all [Active Directory](#) (page 469) users discovered by [LAN Watch](#) (page 348) when [LAN Watch](#) runs on a system hosting Active Directory. Using [View AD Users](#):

- Agents can be automatically installed on each machine an Active Directory user logs onto.
- VSA administrators can be created based on Active Directory users.

Agent

- VSA users can be created based on Active Directory users.
- Contact information can be extracted from Active Directory users and applied to the contact information for machine IDs.

Note: You must select a *Detail View* to see AD users listed on this page.

Switching From Summary View to Detail View

1. Select <All Groups> from the [Select Machine Group](#) drop-down list in the [Machine ID / Group ID filter](#) (page 477) to display a *summary view* of all domain controllers discovered by LAN Watch.
2. Identify the machine groups and subgroups listed in the [Discovered By](#) column.
3. Select one of the machine groups or subgroups in Step 2 above from the [Select Machine Group](#) drop-down list to display a *details view* of domain controllers for that machine group.

Summary View

The summary view of the [View AD Users](#) page lists all domain controllers that ran LAN Watch for *all machine groups you're authorized to access*.

Discovered By

Lists the machine ID.group ID names of domain controllers that have performed a LAN Watch scan.

Users Found

Lists the number of users contained in Active Directory found on a domain controller that ran LAN Watch.

Assigned

Lists the number of [Users Found](#) whose contact information has been extracted from the Active Directory and assigned to a machine ID.

Details View

The details view of [View AD Users](#) displays a list of Active Directory users on domain controllers that ran LAN Watch *within a specified machine group*.

Installing Agents on Any Machine an AD User Logs Onto

You can associate an install package with an AD user. This installs an agent package on any machine a user logs onto, unless the agent is already installed. Even if the agent is subsequently removed from a machine, the agent will be re-installed the next time the user logs on. You can specify the agent package installed for each AD user.

Note: See [Install Issues and Failures](#) (page 340) if an agent fails to install.

To associate an install package with an AD user:

1. Select AD users listed in the [Canonical Name](#) (page 472) column of the paging area.
2. Select an agent package from the [Select an Agent Package](#) drop-down list.
3. Click [Install Agent Policy](#).
4. Select an AD user and click [Cancel](#) to un-associate an install package with an AD user.

Creating VSA Administrators Based on AD Users

Create VSA administrators based on AD users. Administrators created using this method log onto the VSA using their AD domain, user name, and password. This means administrators only have to maintain credentials in a single location, the Active Directory.

Note: A VSA administrator created based on an AD user cannot use [System > Preferences \(page 377\)](#) to change their username or password. If there are problems with an Active Directory, [System > Set Password \(page 391\)](#) still provides you with the ability of changing a VSA administrator's password, even if that VSA administrator is based on an AD user.

To create a new VSA administrator based on an AD user:

1. Select an AD user from the [Canonical Name](#) column in the paging area.
2. Select an administrator role from the [Select Admin Role](#) drop-down list.
3. Click [Create Admin](#).

You can confirm the creation of the new VSA Administrator using [System > Create / Delete Admin Accounts \(page 388\)](#). VSA administrator names based on AD users are formatted as follows:
<domainname> | <username>.

Creating VSA Users Based on AD Users

Create VSA users based on an AD users. VSA users created using this method log onto the VSA using their AD domain, user name, and password. This means credentials only have to be maintained in a single location, the Active Directory.

VSA users must be associated with a specific machine ID. Assign a Machine ID to an AD user before creating a VSA user based on the AD user.

Note: If a VSA user is created based on an AD user, the VSA user's username and password cannot be changed within the VSA, only in Active Directory.

To create new VSA user based on an AD user:

1. Click the [unassigned](#) link for an AD user listed in the [Canonical Name](#) column of the paging area.
2. Select a machine ID.group ID account in the popup window. The popup window closes.
3. Select the checkbox for this same AD user in the left most column.
4. Click [Create User](#).

You can confirm the creation of the new VSA user using [Agent > User Access \(page 212\)](#).

Updating Contact Information for Machine IDs based on AD Users

If a machine ID is assigned to an AD user, then the VSA updates its own contact information for that machine ID with the latest contact information for that user in the Active Directory each time the user logs onto the machine ID. This enables administrators to update contact information once in the Active Directory and know the contact information for machine IDs in the VSA will be updated automatically.

To assign an AD user to a machine ID:

1. Click the [unassigned](#) link for an Active Directory user listed in the [Canonical Name](#) column of the paging area.
2. Select a machine ID.group ID account in the popup window. The popup window closes.

Converting Your VSA Logon to use your Domain Logon

You can convert your own VSA logon to use your domain logon as follows:

1. Open the [System > Preferences](#) page in the VSA.
2. Enter your current VSA password in the [Old Password](#) field.
3. Enter you domain and domain logon name, formatted *all in lowercase* as `dom/username`, where `dom` is your domain name and `username` is your logon name, in the [Change Logon Name](#) field.
4. Enter your domain password in the [New Password / Confirm Password](#) fields.

This enables you to logon to the VSA using your domain logon and have your VSA logon name and

password managed using Active Directory. At the same time, you can continue to use all your previous VSA share rights, scripts and other administrator settings.

View vPro

The [View vPro](#) page displays hardware information about vPro-enabled machines discovered while running [LAN Watch](#) (page 348). 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:

- Motherboard Asset Information
- BIOS Information
- Processor Information
- RAM Information
- Hard Drive Information

Note: vPro-enabled machines with a vPro credential can be powered up, powered-down or rebooted using [Remote Cntl > Power Mgmt](#) (page 268).

Copy Settings

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

The [Copy Settings](#) page copies selected settings from a single source machine ID to any 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 477) 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.

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 are:

- Credential
- Agent Menu
- Checkin Control
- Temps Dir

- Logs
- User Profile - Refers to settings in Audit > [Edit Profile](#) (page 210) or Ticketing > [User Profiles](#) (page 210).
- View Collections
- User Access
- Remote Control Policy
- Patch Settings
- Patch File Source
- Patch Policy Memberships
- Fixed Alerts - These all the alert types on the Monitor > [Alerts](#) (page 100) page except for Event Log alerts and System alerts.
- Event Log Alerts
- Monitor Sets
- Distribute Files
- Protection
- Script Schedules

Select Machine ID

Click the [Select Machine ID](#) link to specify which machine ID to copy settings from.

Stagger script times by N min

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Status

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

Import / Export

Agent > Import / Export

The [Import / Export](#) page imports and exports machine ID account settings, including script schedules, assigned monitor sets and event sets, as XML files. 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 477](#)), from one KServer to the next.

Note: See [Copy Settings](#) ([page 358](#)) for a list of the types of settings associated with a machine ID account.

Note: For the latest instructions on migrating an existing KServer to a new machine see the article [How do I move my Kaseya Server to a new computer? \(270436\)](#) in the Kaseya Support Knowledge Base Portal.

Note: Sample templates for specific types of machines can be imported and are available on the [Kaseya Support Forum](#).

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 and Group ID fields.
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. 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 KServer.
2. Click [Import](#). A set of additional options displays.
3. Accept or specify the name of the machine ID. A new one is created if this name doesn't already exist in the KServer.
4. Accept or select a different group ID.
5. Optionally check the box next to [Replace existing data if this machine ID already exists](#).
6. Optionally change the email notification address for all alerts defined for this machine ID account.
7. Click [Finish](#) to complete the import.

Suspend

Agent > Suspend

The [Suspend](#) page suspends all agent operations, such as scripts, 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 483](#)).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Suspended

Displays `Suspended` if the machine ID is suspended.

Agent Menu

Agent > Agent Menu

The [Agent Menu](#) page specifies the options that display in the agent menu on a user's machine. The user displays the agent menu by right-clicking the agent icon  in the [system tray](#) (on page 483) 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 11) for a general explanation of how agent icons display on the user's machine.

Note: You can download a [User Access Quick Start Guide](#) from the first topic of online help.

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](#).

Agent

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 becomes invisible to KServer administrators and can no longer receive commands from the KServer.

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 user to display the About box for the installed agent. The default option label `Agent` can be customized.
- [<Contact Administrator>](#) - Check to enable the user to display the [User Access Welcome Page](#) (page 484). The user can use this page to send email or chat with the administrator or create a trouble ticket. This option can display an alternate URL instead. The default option label `Contact Administrator` can be customized.
- [<www.kaseya.com>](#) - Check to enable the user to display the URL specified in the corresponding URL field. The default option label [www.kaseya.com](#) can be customized.
- [Disable Remote Control](#) - Check to enable the user to *disable* remote control on the user's managed machine.
- [Set Account...](#) - Check to enable the user to display their machine ID, group ID and change their KServer address the agent checks into.
- [Refresh](#) - Check to enable the user to initiate an immediate [full check-in](#) (page 473).
- [Exit](#) - Check to enable the user to terminate the agent service on the managed machine.

Update

Click [Update](#) to apply agent menu settings 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

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 will display in the agent menu. A "-" indicates that menu option will not display in the agent menu.

A = About Agent

C = Contact Administrator

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 / Contact URL

The *upper* row of these two columns displays:

- The text displayed on the agent menu for contacting the administrator.
- The URL to display when this agent menu option is selected by the user. The default URL is the User Logon page for the KServer. A different URL can be entered.

Custom Title / Custom URL

The *lower* row of these two columns displays:

- The text displayed on the agent menu for contacting a custom URL.
- The URL to display when this agent menu option is selected by the user.

Check-In Control

Agent > Check-In Control

The [Check-In Control](#) page specifies when and where each machine ID should check in with a KServer. Changes made using this page take effect at the next agent check-in and display **in red text** until then. You can specify the primary and secondary KServers used by the agent to check in, the bandwidth consumed by an agent to perform tasks and the check-in period.

Note: The primary and secondary KServer values and the minimum and maximum check-in periods are subject to the policies set using [System > Check-in Policy](#) (page 382). This prevents administrators from selecting settings that place undue stress on servers running the KServer service.

Note: Check-in Control information can also be maintained using the Agent Settings tab of the Machine Summary (page 21) page.

Migrating Agents from one KServer to Another

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

1. At the original KServer, set the primary KServer setting to point to the [new](#) KServer address.
2. At the original KServer, point the secondary KServer setting to the [original](#) KServer.
3. At the new KServer, set both the primary and secondary KServer to point to the new KServer.
4. Wait for all the agents to successfully check into the new KServer. At that time, the original KServer can be taken off-line.

Note: For the latest instructions on migrating an existing KServer to a new machine see the article [How do I move my Kaseya Server to a new computer? \(270436\)](#) in the Kaseya Support Knowledge Base Portal.

Changing the Port used by Agents to Check into the KServer

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 \(page 394\)](#) page. Enter the new port number in the [Specify port Agents check into server with](#) edit box and click the [Change Port](#) button.

Note: If any Agents have not migrated to the new port before you switch the KServer, 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 475) of the machine ID's primary KServer. This setting is displayed in the [Primary KServer](#) column.

Kaseya agents initiate all communication with the KServer. For this reason the agents must always be able to reach the domain name or IP (Internet Protocol) address assigned to the KServer. 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 KServer. 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 KServer 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 475) 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 KServer. This setting is displayed in the [Secondary KServer](#) column.

Secondary Port

Enter the port number of either the secondary KServer 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 473](#)) with the KServer. A check-in consists of a check for a recent update to the user's account, which is determined by an administrator. If a recent update has been set by a KServer administrator, 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 382](#)).

Best Practices: The agent maintains a persistent connection to the KServer. As a result, quick check-in times do not effect response times from the agent. The quick check-in time sets the maximum time 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.

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 KServer can detect if more than one agent is connecting to the KServer and using the same machine ID.group 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 KServer as an administrator.

Warn if agent on same LAN as server connects through gateway

If you are managing machines that share the same LAN as your KServer then you may get this alert. By default all agents connect back to the KServer using the [external name/IP address](#) ([page 394](#)). TCP/IP messages from these agents travel through your internal LAN to your router, and then back to the KServer. Some routers do a poor job of routing internal traffic back through themselves. Check this box to receive a notification when the KServer detects an agent may be on the same LAN but connecting through the router.

Note: Agents on the same LAN as the KServer should be configured to connect directly to the KServer using the [Check-In Control](#) ([page 363](#)) function.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in

Agent

-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Temp Directory

Agent > Temp Directory

The [Temp Directory](#) page sets the path to a directory used by the agent to store temporary files. Depending on the task at hand, the agent uses several additional files. The server transfers these files to a temporary directory used by the agent on the managed machine. For selected machine IDs you can change the default temporary directory from `C:\temp` to any other location. Change the directory in order to isolate files used by the system from other operations used by other applications on the machine. You can also approve this directory in security programs, such as virus checkers, to allow operations such as remote control from being blocked.

Note: A temporary directory can also be maintained using the Agent Settings tab of the Machine Summary (page 21) page.

Set

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

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

Enter the path of the temp 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 temp directory.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete

-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

Temp Path

The path of the temporary directory assigned to this machine ID. On a Mac 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 / User Profiles

[Agent > Edit Profile](#)

[Ticketing > User Profiles](#)

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:

- Notes and contact information can also be maintained using the [Agent Settings](#) tab of the [Machine Summary](#) (page 21) page.
- The contact information in the [Edit Profile](#) page can be automatically populated when a new account is created using the [Agent > Create](#) (page 341) page.
- The user can update his or her contact name, contact email and contact phone number using the [Change Profile](#) option on the [User Access](#) page.

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](#).
4. The newly entered settings are shown in the respective machine ID account's fields.

Notes

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.

Show notes as tooltip

If checked, [Edit Profile](#) notes are included as part of the tooltip that displays whenever the cursor hovers over a machine ID's [check-in status icon](#) (see "Check-in Status" on page 473).

Auto assign tickets

Auto assign a ticket to this machine ID if the [Ticketing email reader](#) (page 208) receives an email from the same email address as the [Contact Email](#). Applies when new emails come into the ticketing email reader that do not map into any of the [email mappings](#) (page 210)

Note: if multiple machine IDs have the same contact email, 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.

Note: A Contact Email address is required for users to receive a new password using the Get New Password option on the User Access Welcome Page (page 484). See [Agent > User Access](#) (page 212) for more information.

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 of the individual responsible for administering support to the managed machine. This can be the administrator, but is often someone who is part of the IT staff of the company that owns the 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 361) on a managed machine. The languages available are determined by the language packages installed using [System > Preferences](#) (page 377).

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using [System > Group Access](#) (page 385).

User Access

Agent > User Access

Ticketing > User Access

The [User Access](#) page determines whether users can perform the following tasks from their own machine or from another machine using the [User Access Welcome Page](#) (page 484):

- Remote control or FTP *their own managed machine from another machine*. This is the same remote control capability administrators have, except it restricts users to their own machine.
- *Initiate* a chat session with a KServer administrator from their own machine or any other machine.

Note: An administrator can always initiate a chat (page 279) session with a user regardless of this setting.

- Create or display tickets for their own machine or any other machine.
- Use any other menu option on the User Access Welcome Page from another machine as though they were currently logged into their own managed machine. For example, send email.

Note: Remote Cntl, Ticketing and Chat must be enabled using this page for these options to be visible on the User Access Welcome Page.

Note: You can download a User Access Quick Start Guide from the first topic of online help.

Accessing the User Access Welcome Page Remotely

A user can display the User Access Welcome Page associated with their own machine from another machine as follows:

1. Log into http://your_KServer_address/access/ page, substituting the appropriate target KServer name for `your_KServer_address` in the URL text.

Note: This is the same page that administrators use to log into the KServer.

2. Log into the KServer by entering either:
 - The machine ID.group ID and the password assigned to the machine ID using this page, or
 - The user name and password assigned to the machine ID using this page.

The User Access Welcome Page displays. The user can click any menu option as though he or she were logged in from their own managed machine. The 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.

Re-Enabling User Logons

User logons follow the same [Logon Policy](#) (page 403) as administrator 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.

Generating a New User Access Password

If a user has forgotten their user access password, they can generate a new password as follows:

1. Log into http://your_KServer_address/access/ page, substituting the appropriate target KServer name for `your_KServer_address` in the URL text.

Note: This is the same page that administrators use to log into the KServer.

2. Enter their user name in the [Username](#) field.
3. Click the [Get New Password](#) menu option.

A new random password is sent to the user email address of record for the managed machine.

Agent

This user email address is set using the [Contact Email](#) field in Agent > [Edit Profile](#) (page 210).

Customizing the User Access Welcome Page

Master administrators can customize the web page seen by users using System > [Customize](#) (page 403), adding their company's logo, look, and feel to the web experience for their users.

Logon Name

Enter the [Logon Name](#) the user must use to log into the KServer 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. If no logon name is specified, then the [Logon Name](#) defaults to the machine.group name

Note: All logon names must be unique in the system. Since users may also logon using their machine ID, logon names, machine IDs, and administrator names must all be unique.

Create Password, Confirm Password

Define a password for the user logon. Passwords must be at least 6 characters long. The user can change the password after the administrator assigns him one. See *Generating a New User Access Password* above.

Apply

Click [Apply](#) to apply the logon name and password to the selected machine ID.

Clear

Permanently remove the logon [credential](#) (page 473) from the selected machine ID.

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

Logon Name

The logon name assigned to this machine ID. Users that have been granted remote access to their machine may logon using [either](#) their machine ID or logon name.

User Web Logon

Displays `Enabled` if a logon name and password has been assigned to this machine ID, even if [Remote Cntl](#), [FTP](#) and [Chat](#) are not checked. Indicates that a user can log into the user page from a web browser on any machine. They can always get to that same page by double clicking the agent icon on their own machine or selecting [Contact Administrator...](#) from the [agent menu](#) (page 469).

Enable Remote Cntl

Check this box to allow users remote control access to their machine when they log on to the VSA through any web browser.

Enable Ticketing

Check this box to allow users to create and modify tickets for their own machines. Users can only see tickets assigned to their machine.

Enable Chat

Check this box to allow users to initiate a chat session with a logged in administrator. They will only be able to chat with administrators that have access rights to the group ID that the user's machine belongs to.

Set Credential

Agent > Set Credential

The [Set Credential](#) page registers the credential required by an agent to perform administrator 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](#) should always be an *administrator credential*.
- [Patch Status](#) (page 222) - Patch Status resets test results every time a machine ID's [Set Credential](#) changes.
- [Office Source](#) (page 254) - 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 72) - The `Use Credential` script command behaves the same as the `Impersonate User` command except a unique credential can be used to access each machine instead of using a fixed credential in a script.
- [Image Location](#) - 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.
- [User State Management](#) - Installing the client for this add-on 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 an administrator 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 472). 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.

Agent

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.

Update Agent

Agent > 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 469) you have defined for each agent.

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 administrators logon if managed machines under their control need to be updated with the latest version of the agent software. Only agents that belong to the administrator trigger this popup window. Administrators 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 script select script

Select a script 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.

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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of [Machine ID.Group IDs](#) (page 476) displayed is based on the [Machine ID / Group ID filter](#) (page 17) and the machine groups the administrator is authorized to see using System > [Group Access](#) (page 385).

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.

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 363), Pending displays in the [Last Update](#) column until the next check-in occurs.

Chapter 12

System

In This Chapter

System Tab	376
Preferences	377
Create / Delete: Machine Groups	379
Rename Group	380
Naming Policy	380
Check-in Policy	382
Create / Delete: Admin Roles	383
Membership: Admin Roles	384
Group Access	385
Function Access	387
Logon Hours	388
Create / Delete: Admin Accounts	388
Enable / Disable	390
Set Password	391
Admin History	393
Request Support	394
Configure	394
License Manager	399
System Log	400
Statistics	401
Logon Policy	403
Customize	403

System Tab

System

The [System](#) tab allows administrators to maintain policies affecting the entire system:

- [Machine Groups](#)
- [Administrator Roles](#)
- [Administrator Accounts](#)
- [Server Management](#)
- [Database Views](#)

Functions	Description
Preferences (page 377)	Set email where alerts are sent to and to change administrator passwords.
Machine Group Create / Delete (page 379)	Create, edit, and delete machine group IDs.
Rename Group (page 380)	Renames machine groups and sub-groups.
Naming Policy (page 380)	Automatically enforce naming policy based on each machines IP address, network, and computer name
Check-in Policy (page 382)	Set limits on a variety of agent check-in parameters.
Admin Roles Create / Delete (page 379)	Create and delete administrator roles. Assign administrators to roles to inherit administrator rights.
Membership (page 384)	Define which administrators belong to which administrator roles
Group Access (page 385)	Define which machine groups each Administrator role gets access to.
Function Access (page 387)	Defines the functions available to an administrator role
Logon Hours (page 388)	Specifies when administrators can logon into the KServer.
Admin Account Create / Delete (page 388)	Create and delete standard or master administrators.
Enable/Disable (page 390)	Enable or disable standard or master administrator accounts.
Set Password (page 391)	Change administrator account passwords.
Admin History (page 393)	Display the functions visited in the last 30 days for each administrator.
Request Support (page 394)	Access Kaseya support and/or give Kaseya support access to your server.
Configure (page 394)	View server information, license code and subscription information, obtain latest server updates, and server IP information.
License Manager (page 399)	Allocates available agent licenses to group IDs.
System Log (page 400)	Logs events that can not be tracked by machine ID for 60 days.
Statistics (page 401)	Display VSA server performance statistics

Logon Policy (page 403)	Set logon policies.
Customize (page 403)	Customize the logon page and graphical user interface for the system.
Database Views (page 410)	Configures database view access

Preferences

System > Preferences

The [Preferences](#) page sets preference options that typically apply *only to the currently logged in administrator*. This includes changing your administrator logon name and password and the email address where you receive alert messages.

Note: Two options on this page apply to *all administrators* and only display for master administrators: setting the System Default Language Preference and the Download button for installing language packs.

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.

Changing Your VSA Logon Name and/or Password

To change your logon name and password:

1. Enter your old password in the [Old Password](#) field.
2. Enter a new name in the [Change Logon Name](#) field.

Note: The [Change Logon Name](#) field is *display only* if Prevent anyone from changing their logon is checked in System > Logon Policy.

3. Enter a new password in the [New Password](#) field.

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. Click [Change](#).

Note: Your logon name, password and email address can also be changed by other administrators using System > [Create/Delete](#) (page 388).

Note: The logon policy for failed logons and password strength for all administrators is set using System > [Logon Policy](#) (page 403).

Converting Your VSA Logon to use your Domain Logon

You can convert your own VSA logon to use your domain logon as follows:

1. Open the System > [Preferences](#) page in the VSA.

System

2. Enter your current VSA password in the [Old Password](#) field.
3. Enter you domain and domain logon name, formatted *all in lowercase* as `dom/username`, where `dom` is your domain name and `username` is your logon name, in the [Change Logon Name](#) field.
4. Enter your domain password in the [New Password / Confirm Password](#) fields.

This enables you to logon to the VSA using your domain logon and have your VSA logon name and password managed using Active Directory. At the same time, you can continue to use all your previous VSA share rights, scripts and other administrator settings.

Set first function after logon

Select the name of the function you want to see when you first log on to the KServer.

Select time zone offset

Select one of the following time zone offset options, the click [Apply](#).

- [Use time zone of the browser logging into the system](#)
- [Use time zone of the VSA server](#)
- [Use fixed offset from the VSA server <N> hours](#)

Set up language preferences

- [My language preference is](#) - Select the language you prefer displayed when you're logged into the KServer. The languages available depend on the language packs installed.
- [System default language preference is](#) - Select the default language used by the KServer user interface for all administrators. The languages available depend on the language packs installed. This option only displays for [master administrators](#) (*page 469*).
- [Download a Language Pack](#) - Display a dialog box that enables you to download and install language packs. A language pack enables the KServer user interface to be displayed in that language. This option only displays for [master administrators](#) (*page 469*).

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 Home > [View Dashboard](#) (*page 28*) page.

Defaults

Click [Defaults](#) to reset all settings to system defaults for this administrator.

Create / Delete: Machine Groups

System > Machine Groups: Create / Delete

The [Create / Delete](#) page creates and deletes machine groups. Each [agent](#) (page 470) installed on a managed machine is assigned a unique machine ID/group ID name. All machine IDs are associated with a group ID and optionally a subgroup ID. Typically a group ID represents a single customer account. Subgroup IDs typically represent a location or network within a group ID. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.acme.chicago`. In this case `chicago` is a subgroup ID defined within the group ID called `acme`. Only a master administrator, or administrators authorized by a [master administrator](#) (page 469), can create group IDs. Any administrator can create subgroup IDs.

Creating a New Group ID

To create a new machine group:

1. Enter a new group name in the text box.
2. Click [Create](#) to create the new machine group ID. The new machine group is displayed in the list.

You can now assign administrators to administer the new group.

Deleting a Group ID

To delete an *empty* machine group:

1. Select the checkbox next to the machine group ID you wish to delete. More than one checkbox can be selected if you wish to delete multiple machine groups at the same time.
2. Click [Delete](#). A dialog box confirms the deletion.
3. Click [OK](#) to delete, or [Cancel](#).

The empty machine groups are removed from the list.

Enter name for new machine group

Enter the name of a new machine group ID that you wish to create.

Allow standard administrators to create root groups

By default, standard administrators may not create or delete root level machine groups. If checked, standard administrators can create or delete root level machine groups. This option only displays for [master administrators](#) (page 469).

When a standard administrator creates a new root machine group, [permission to access](#) that machine group is automatically granted to [all administrator roles that administrator belongs to](#).

Create as subgroup of

Create [subgroups](#) within machine groups. To create a subgroup select the parent group from this drop-down control prior to clicking [Create](#). To create a new top level root group leave the drop-down control set to `< New Root Group >`.

Create

Click [Create](#) to create a new machine group with the specified name.

Delete

Click [Delete](#) to delete an *empty* machine group. An empty machine group is one with no machines assigned to that group. If any machine is assigned to a machine group, then the checkbox beside the group name is disabled and shown in gray. Deleting a group also deletes any associated subgroups.

System

Total Machines

Displays the total number of machines managed.

Total Groups

Displays the total number of groups defined.

Machine Group

Each machine group defined is displayed under [Machine Group](#). The checkbox beside the machine group is checked only if *no machines are assigned to that group ID*. The checkbox can be selected to mark an empty group for deletion.

Total Group

Displays the number of machines in each machine group, including any associated subgroups. This can be used to evenly distribute machines per group, or to plan migration of some groups to a new server.

Sub Group

Shows the administrator the number of machines in an individual machine group. If the group has subgroups, none of the machines in those subgroups are counted.

Rename Group

System > Rename Group

The [Rename Group](#) page renames any root group or sub-group. You cannot rename both a root group and sub-group at the same time.

For example, you can rename the following:

- `company.dept` -> `company.marketing`
- `company.marketing` -> `company.marcom`
- `company` -> `hughes`

In the last example, all existing sub-groups for the root group `company` move into the new root group name `hughes`.

You cannot rename a root group and sub-group at the same time, as in the following example:

- `company.dept` -> `newco.accounting`

Naming Policy

System > 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 group IDs represent a single customer enterprise 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 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 70), managed machines can run scripts 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.
- Using [Deploy Agents](#) (page 331), 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, a naming policy assigns it to the correct group ID and/or sub-group ID.

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 473). The quick check-in (page 473) cycle does not trigger a rename. To rename a group of machines quickly using Naming Policy, schedule the `Force Check-in` sample script located in the `Scripts > Script Browser` (page 63).

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 in to the KServer.

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.

Force Machine ID

Displays a check mark if [Force machine ID to always be computer name](#) is enabled for a machine group.

Check-in Policy

System > 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 administrators from selecting settings that place undue stress on Windows servers running the KServer.

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 > [Logging Control](#) (page 328). 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 363). To remove a value, enter 0 (zero).

Fixed KServer Address

If these checkboxes are checked and the fields left *blank* and [Update](#) clicked, then the [KServer](#) column of selected group IDs display `Editable`. Administrators 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. Administrators 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 KServer. 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 KServer 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 administrators](#) (page 469). If enabled, new machine ID accounts are created automatically for group IDs that do not have any [Check-in Policy](#) defined, as soon as the machine's agent checks into the KServer 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 changes to 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.

KServer (1st) (2nd)

Lists the IP addresses/host names of the primary (1st) and secondary (2nd) servers used by group IDs. These settings are edited using the [Fixed KServer Address](#) fields in the header, for each 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.

Check-in (Min) / Check-in (Max)

Lists the settings entered in the [Check-In Period](#) fields in the header, for each group ID.

Create / Delete: Admin Roles

[System](#) > [Create / Delete: Admin Roles](#)

The [Create / Delete](#) page creates, renames and deletes administrator roles. The paging area displays all the administrators belonging to each administrator role. Administrators are assigned to administrator roles using [System](#) > [Membership](#) (page 384).

Administrator Roles

[Administrators](#) (page 469) can belong to none, one, or more administrator roles. If an administrator is assigned to multiple roles, and any one of those assigned roles provides access to a function, then the administrator has access to that function. The following policies are assigned by administrator role:

- Access to machine group IDs using [System](#) > [Group Access](#) (page 385)
- Access to VSA modules and functions using [System](#) > [Function Access](#) (page 387)
- Access to the entire VSA by weekday and hour using [System](#) > [Logon Hours](#) (page 388)
- Remote control user notification using [Remote Control](#) > [Admin Role Policy](#) (page 274)

In addition, scripts and agent installation packages can be shared by administrator role. Standard administrators can only see other administrators who are members of the same roles.

Function Access of Created Administrator Role

If a standard administrator creates a new administrator role, the new role gets the same function access as the standard administrator, except for any master-only functions that may have been assigned the currently logged on standard administrator.

Deleting Administrator Roles

You can delete an administrator role even if administrators are assigned to it. The `Master` role cannot be deleted. Server management configuration and other specialized functions apply to the [master administrator](#) (page 469) role only. See [System > Function Access](#) (page 387) for more information.

Renaming Administrator Roles

1. Click the edit icon  to the left of a [Role Name](#).
A dialog box displays.
2. Type in the new name for the administrator role.
3. Click [OK](#) to rename or [Cancel](#).

Create

Click [Create](#) to create a new administrator role based on the text entered in the [Enter name for new administrator role](#) field.

Delete

Click [Delete](#) to delete selected administrator roles.

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.

Edit icon

Click the edit icon  to the left of a role name to rename it.

Role Name

Lists existing administrator roles.

Member Administrators

Lists the administrators belonging to each administrator role.

Membership: Admin Roles

System > Membership

The [Membership](#) page assigns administrators to administrator roles. [Administrators](#) (page 469) can belong to none, one, or more administrator roles. If an administrator is assigned to multiple roles, and any one of those assigned roles provides access to a function, then the administrator has access to that function. The following policies are assigned by administrator role:

- Access to machine group IDs using [System > Group Access](#) (page 385)
- Access to VSA modules and functions using [System > Function Access](#) (page 387)
- Access to the entire VSA by weekday and hour using [System > Logon Hours](#) (page 388)
- Remote control user notification using [Remote Control > Admin Role Policy](#) (page 274)

In addition, scripts and agent installation packages can be shared by administrator role. Standard administrators can only see other administrators who are members of the same roles.

Adding Administrators to Administrator Roles

1. Select one or more administrators in the paging area.
2. Click an administrator role in the [Assign administrators to roles](#) listbox. Hold down the [Ctrl] key to click multiple administrator roles.
3. Click [Add](#) to add selected administrators to selected administrator roles.

Removing Administrators from Administrator Roles

1. Select one or more administrators in the paging area.
2. Click an administrator role in the [Assign administrators to roles](#) listbox. Hold down the [Ctrl] key to click multiple administrator roles.
3. Click [Remove](#) to remove selected administrators from selected administrator roles.

Assign Administrators to roles

Click an administrator role in the [Assign administrators to roles](#) listbox to add or remove them from administrator roles. Hold down the [Ctrl] key to click multiple administrator roles.

Add

Click [Add](#) to add selected administrators to selected administrator roles.

Remove

Click [Remove](#) to remove selected administrators from selected administrator roles.

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.

Standard Admin / Master Admin

Administrators are listed under this column. A background of two alternating shades of *beige* designates master administrators. A background of two alternating shades of *grey* designates [standard administrators](#) (*page 469*).

Admin Role

The list of administrator roles each administrator is a member of.

Group Access

System > Group Access

The [Group Access](#) page determines administrator access to machine groups by assigning machine groups to administrator roles. Since all machine IDs are assigned to group IDs, administrators can be permitted or denied access to machine ID.group ID user accounts using [Group Access](#). Adding or removing a machine *group* to or from an administrator role automatically adds or removes access to any associated *subgroups*. An administrator belonging to multiple administrator roles has access to a machine group if *any* single administrator role permits it. *Only a master administrator may grant/deny <all groups> access to any role.*

Administrator Roles

[Administrators](#) (*page 469*) can belong to none, one, or more administrator roles. If an administrator is assigned to multiple roles, and any one of those assigned roles provides access to a function, then the administrator has access to that function. The following policies are assigned by administrator role:

System

- Access to machine group IDs using System > [Group Access](#) (page 385)
- Access to VSA modules and functions using System > [Function Access](#) (page 387)
- Access to the entire VSA by weekday and hour using System > [Logon Hours](#) (page 388)
- Remote control user notification using Remote Control > [Admin Role Policy](#) (page 274)

In addition, scripts and agent installation packages can be shared by administrator role. Standard administrators can only see other administrators who are members of the same roles.

Adding Machine Groups to Administrator Roles

1. Select one or more administrator roles in the paging area.
2. Click a machine group in the [Give administrator roles access to machine groups](#) listbox. Hold down the [Ctrl] key to click multiple machine groups.
3. Click [Add](#) to add selected administrator roles to selected machine groups.

Removing Machine Groups from Administrator Roles

1. Select one or more administrator roles in the paging area.
2. Click a machine group in the [Give administrator roles access to machine groups](#) listbox. Hold down the [Ctrl] key to click multiple machine groups.
3. Click [Remove](#) to remove selected administrator roles from selected machine groups.

Renaming Administrator Roles

1. Click the edit icon  to the left of an [Admin Role](#) name.
A dialog box displays.
2. Type in the new name for the administrator role.
3. Click [OK](#) to rename or [Cancel](#).

Give administrator roles access to machine groups

Click a machine group in the [Give administrator roles access to machine groups](#) listbox to add or remove them from administrator roles. Hold down the [Ctrl] key to click multiple machine groups.

Add

Click [Add](#) to add machine groups to selected administrator roles.

Remove

Click [Remove](#) to remove machine groups from selected administrator roles.

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.

Edit icon

Click the edit icon  to the left of a role name to rename it.

Admin Role

Administrators are listed under this column. A background of two alternating shades of *beige* designates master administrators. A background of two alternating shades of *grey* designates [standard administrators](#) (page 469).

Machine Group

Lists the machine groups that an administrator role has access to. If the administrator role has access to all groups, `All Groups` displays in this column.

Function Access

System > Function Access

The [Function Access](#) page determines administrator access to VSA modules, folders and function pages, by assigning function pages to administrator roles. This includes administrator access to individual tabs of the [Machine Summary](#) (page 21) page.

You may wish to provide certain personnel limited access to specialized functions. For example, clerical assistants may only require access to trouble tickets and reports. At the other extreme, you may wish to permit only advanced administrators access to SNMP monitoring functions.

Access to Additional Capabilities

You can also control access to additional capabilities, such as [Tasks](#), [Messages](#) and [Administrator Notes](#). These display in **dark red text**.

Master Administrators

Only master administrators have access to the following functions.

- Monitoring > System Alarms in [Alerts](#) (page 100)
- Ticketing > [Email Reader](#) (page 208)
- Patch Mgmt > [Approval by Patch](#) (page 240)
- Patch Mgmt > [KB Override](#) (page 242)
- Patch Mgmt > [Command Line](#) (page 256)
- Patch Mgmt > [Patch Location](#) (page 258)
- System > [Request Support](#) (page 394)
- System > [Configure](#) (page 394)
- System > [License Manager](#) (page 399)
- System > [Statistics](#) (page 401)
- System > [Logon Policy](#) (page 403)
- System > [Customize](#) (page 403)

All other functions can be delegated to [standard administrators](#) (page 469).

Administrator Roles

[Administrators](#) (page 469) can belong to none, one, or more administrator roles. If an administrator is assigned to multiple roles, and any one of those assigned roles provides access to a function, then the administrator has access to that function. The following policies are assigned by administrator role:

- Access to machine group IDs using System > [Group Access](#) (page 385)
- Access to VSA modules and functions using System > [Function Access](#) (page 387)
- Access to the entire VSA by weekday and hour using System > [Logon Hours](#) (page 388)
- Remote control user notification using Remote Control > [Admin Role Policy](#) (page 274)

In addition, scripts and agent installation packages can be shared by administrator role. Standard administrators can only see other administrators who are members of the same roles.

Removing Functions from an Administrator Role

1. Select an administrator role from the [Select administrator role](#) drop down list.
2. Uncheck all the module, folders and function pages you do not want to let this administrator role use.

Enable All / Disable All

Click [Enable All](#) to check all functions. Click [Disable All](#) to uncheck all functions.

Lock Settings to Match

All function access changes made to one administrator role can be automatically applied to all other administrator roles that are locked to it. If you create unique administrator roles to isolate access by machine group, but want to give each administrator role the same list of functions, then you can use this feature to manage all function access changes from a single role.

1. Select the administrator role you want to *lock* using the [Select Administrator Role](#).
2. Select the administrator role you want apply changes *from* using [Lock Settings to Match](#).

Logon Hours

System > Logon Hours

The [Logon Hours](#) page determines *when* administrators can logon into the VSA by specifying the weekdays and hours for each administrator role. Each day of the week can have different hours of operation set.

Administrator Role

[Administrators](#) (page 469) can belong to none, one, or more administrator roles. If an administrator is assigned to multiple roles, and any one of those assigned roles provides access to a function, then the administrator has access to that function. The following policies are assigned by administrator role:

- Access to machine group IDs using System > [Group Access](#) (page 385)
- Access to VSA modules and functions using System > [Function Access](#) (page 387)
- Access to the entire VSA by weekday and hour using System > [Logon Hours](#) (page 388)
- Remote control user notification using Remote Control > [Admin Role Policy](#) (page 274)

In addition, scripts and agent installation packages can be shared by administrator role. Standard administrators can only see other administrators who are members of the same roles.

Select administrator role

Select an administrator role to display and maintain its logon hours settings.

No Hours Restrictions

If checked, administrators can logon into 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 KServer's time zone. For all day access, set start and end time to the same time.

Create / Delete: Admin Accounts

System > Admin Accounts: Create / Delete

The [Create / Delete](#) page creates and deletes administrator accounts. This page can also assign administrators to [administrator roles](#) (page 384) when the administrator account is created.

Note: Each administrator can change their own logon name, password and email address using [System > Preferences](#) (page 377). Administrator role membership can be maintained using [System > Membership](#) (page 384). Passwords can be reset using [System > Set Password](#) (page 391). The logon policy for failed logons and password strength for all administrators is set using [System > Logon Policy](#) (page 403).

Warning: To simplify management and auditing of your VSA, provide each administrator with their own unique logon name. Avoid using generic logons like `Admin` or `Administrator`. Generic logons make it difficult to audit the administrative actions taken by each administrator.

Administrators

Administrators use the VSA application to maintain the KServer and oversee the monitoring of [managed machines](#) (page 477) by the KServer and its [agents](#) (page 470). KServer management configuration and other [specialized functions](#) (page 387) can only be performed by [master administrators](#). [Standard administrators](#) are typically restricted to the administration and monitoring of managed machines. A background of two alternating shades of *beige* designates master administrators. A background of two alternating shades of *grey* designates standard administrators. Access to functions, machine groups and other policies are assigned by [administrator role](#) (page 469). Standard administrators can only see other administrators who are members of the same roles.

Creating a New Administrator

1. Enter the administrator's name in the [Admin Name](#) field.
2. Select an administrator role from the [Set Admin Role Membership](#) drop down list.
 - If the new administrator will be a master administrator, select the `Master` group membership.
3. Enter an email address for the new administrator.
4. Enter the same password in the [Create Password](#) and [Confirm Password](#) fields.

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 [Create Password](#) and [Confirm Password](#) fields. Be sure to write it down before clicking [OK](#) and closing the dialog box.

5. Click [Create](#). The new administrator account is created and displays in the paging area.
6. Optionally assign the new administrator to additional administrator roles using [System > Membership](#) (page 384).

Deleting Administrators

You cannot delete the currently logged in administrator account. Deleting an administrator transfers ownership of all private scripts, agent install packages, not-closed tickets and other private data to the currently logged in administrator. A standard administrator with access to this page can delete a master administrator.

1. Select an administrator from the paging area.
2. Click [Delete](#).

Create

Click [Create](#) to create the new administrator account.

Delete

Click [Delete](#) to delete selected administrator accounts.

System

Admin Name

Enter the name for the administrator being created.

Set Admin Group Membership

Select an administrator role from the [Set Admin Role Membership](#) drop down list. Administrator role membership can be maintained using System > [Membership](#) (page 384).

Admin Email

Enter the administrator's email address. This is the default email address used to contact this administrator.

Create/Confirm Password

Enter the administrator's password and password confirmation in the appropriate fields.

Suggest

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 [Create Password](#) and [Confirm Password](#) fields. Be sure to write it down before clicking OK and closing the dialog box.

Require password change at next logon

If checked, selected administrators are forced to change their password using System > [Preferences](#) (page 377) the next time they log in.

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.

Standard Admin / Master Admin

Administrators are listed under this column. A background of two alternating shades of *beige* designates master administrators. A background of two alternating shades of *grey* designates standard administrators.

Admin Email

The default email address used to contact this administrator.

Last Logon

The last time the administrator logged on.

Account Created

The date and time the administrator account was created.

Enable / Disable

System > [Enable / Disable](#)

The [Enable / Disable](#) page enables or disables administrator accounts. Disabled accounts display [Disabled by Admin](#) in red text in the [Last Logon](#) column. A currently logged on administrator cannot enable or disable his or her own account.

This page also displays an administrator icon  next to each currently logged on administrator. You

can log off any other logged on administrator immediately.

Administrators

Administrators use the VSA application to maintain the KServer and oversee the monitoring of [managed machines](#) (page 477) by the KServer and its [agents](#) (page 470). KServer management configuration and other [specialized functions](#) (page 387) can only be performed by [master administrators](#). [Standard administrators](#) are typically restricted to the administration and monitoring of managed machines. A background of two alternating shades of *beige* designates master administrators. A background of two alternating shades of *grey* designates standard administrators. Access to functions, machine groups and other policies are assigned by [administrator role](#) (page 469). Standard administrators can only see other administrators who are members of the same roles.

Enabling Accounts Disabled During Logon

The system automatically locks out an administrator account if they exceed the number of failed logon attempts, as specified in System > [Logon Policy](#) (page 403). Normally, the administrator has to wait the time specified in [Logon Policy](#). Another administrator with access to this page can enable a disabled account immediately.

Enabling Administrator Accounts

1. Select one or more disabled administrator accounts in the paging area. Disabled accounts display **Disabled by Admin** in red text in the [Last Logon](#) column.
2. Click [Enable Account](#).

Disabling Administrator Accounts

1. Select one or more enabled administrator accounts in the paging area. Enabled accounts do *not* display **Disabled by Admin** in red text in the [Last Logon](#) column.
2. Click [Disable Account](#).

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.

Standard Admin / Master Admin

Administrators are listed under this column. A background of two alternating shades of beige designates master administrators. A background of two alternating shades of grey designates standard administrators.

Last Logon

Displays one of the following:

- Enabled Accounts - The date and time this administrator last logged into the VSA.
- Disabled Accounts - **Disabled by Admin** in red text.

Account Created

The date and time the administrator account was created.

Set Password

System > [Set Password](#)

The [Set Password](#) page changes a selected administrator's password. You can also optionally force administrators to change their passwords at the next logon.

Note: The logon policy for failed logons and password strength for all administrators is set using [System > Logon Policy \(page 403\)](#).

Administrators

Administrators use the VSA application to maintain the KServer and oversee the monitoring of [managed machines \(page 477\)](#) by the KServer and its [agents \(page 470\)](#). KServer management configuration and other [specialized functions \(page 387\)](#) can only be performed by [master administrators](#). [Standard administrators](#) are typically restricted to the administration and monitoring of managed machines. A background of two alternating shades of *beige* designates master administrators. A background of two alternating shades of *grey* designates standard administrators. Access to functions, machine groups and other policies are assigned by [administrator role \(page 469\)](#). Standard administrators can only see other administrators who are members of the same roles.

To change an administrator password:

1. Select the radio button next to an administrator.
2. Enter the new password in the [New Password](#) field.

Note: If you would like the system to generate a strong password for you, click [Suggest Password](#). A dialog box displays showing the new password; the new password is automatically entered in the [Create Password](#) and [Confirm Password](#) fields. Be sure to write it down before clicking OK and closing the dialog box.

3. Confirm the password by re-entering it in the [Confirm Password](#) field.
4. Click [Change Password](#).

The password is changed. Don't forget to notify the administrator of the password change.

New Password

Enter a new password in the [New Password](#) field.

Confirm Password

Enter the same new password in the [Confirm Password](#) field.

Change Password

Click [Change Password](#) after entering the new password and confirmation. A dialog box indicates a successful password change.

Suggest Password

Click [Suggest Password](#) to generate a strong random password for better security. A dialog box displays showing the new password; the new password is automatically entered in the [Create Password](#) and [Confirm Password](#) fields. Be sure to write it down before clicking OK and closing the dialog box.

Clear Total

Clears all of the values shown in the [Total Failed Logons](#) column for selected machines.

Select Account

Select the administrator whose password you want to change.

Standard Admin/Master Admin

Lists all the administrators on the KServer. A background of two alternating shades of *beige* designates master administrators. A background of two alternating shades of *grey* designates standard administrators.

Failed Logons in a Row

Lists the number of failed logons in a row. This information is helpful in monitoring possible system security attacks. If the number of failed logons in a row exceeds the number specified in [Logon Policy](#) (page 403), the administrator's account is disabled for a set amount of time. The administrator's account can only be enabled by waiting the specified amount of time or by having another master administrator manually enable the account.

Total Failed Logons

Lists the total number of failed logons attempted by an administrator.

Change Password At Next Logon

Click [Force Change](#) to force the administrator to change his or her password at the next logon.

Reset Master Admin Password

Forgotten Administrator Password

If you have forgotten your master administrator account password, the system provides a way for you to create a new master administrator account, which enables you to log back in to the system and retrieve the forgotten account information.

Note: You must have administrator (Windows NT/2000) privileges on the server running the system. Due to security reasons, you cannot perform the following procedure remotely.

To create a new master administrator account:

1. Log in to the machine running the server component of the system.
2. Access the following web page:
<http://localhost/LocalAuth/setAccount.asp>
3. Enter a new account name in the [Master Administrator Name](#) field.
4. Enter a password in the [Enter Password](#) field and confirm it by re-typing it in the [Confirm Password](#) field.
5. Click [Create](#).

You will now be logged in to the system as a master administrator.

Changing the Administrator Password

Change your administrator password using System > [Preferences](#) (page 377).

Admin History

System > Admin History

The [Admin History](#) page displays a history, in date order, of every function used by an administrator. The history also displays any actions captured by the [System Log](#) (page 400) performed by the selected administrator. The system saves history data for each administrator for the number of days specified for the [System Log](#).

Click an [administrator name](#) to display the log for that administrator.

Note: This log data does not appear in any reports. Reports are only available for data associated with a machine ID.

Administrators

Administrators use the VSA application to maintain the KServer and oversee the monitoring of

managed machines (page 477) by the KServer and its agents (page 470). KServer management configuration and other specialized functions (page 387) can only be performed by master administrators. Standard administrators are typically restricted to the administration and monitoring of managed machines. A background of two alternating shades of beige designates master administrators. A background of two alternating shades of grey designates standard administrators. Access to functions, machine groups and other policies are assigned by administrator role (page 469). Standard administrators can only see other administrators who are members of the same roles.

Request Support

System > Request Support

The Request Support page provides multiple ways of contacting Kaseya support.

Note: Please reference our additional documentation before calling support.

- **Support Web Site** - Find answers to common questions using the Kaseya Support website at <http://www.kaseya.com/support>. This website provides links to the **Kaseya Support Forum** and to the **Kaseya Support Knowledge Base**. The Support 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.
- **Enable Kaseya Support to Logon** - Kaseya support engineers can solve problems with your system quickly and efficiently when they can directly access your KServer. Click **Create** to create a `kaseyasupport` master administrator 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 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.

- **Create a Ticket** - You can directly create and track tickets in our support system by clicking the **Logon** button.

Note: You can track any and all tickets you submit by clicking the **Logon** button. Tickets submitted via support@kaseya.com or the phone can not be tracked by you through the online system.

- **Email** - Email support requests to support@kaseya.com.
- **Phone** - Call our support engineers from 6am to 6pm Eastern Time, Monday through Friday at 1-415-694-5700, extension 4.

Your Information

Typically Kaseya support needs some basic information about your system to begin providing support. Your administrator name, email address, Customer ID, and system URL are provided for your convenience.

Configure

System > Configure

The **Configure** page manages the configuration of your KServer and related services.

Note: For the latest instructions on migrating an existing KServer to a new machine see the article [How do I move my Kaseya Server to a new computer? \(270436\)](#) in the Kaseya Support Knowledge Base Portal.

Check for Update

Click [Check for Update](#) to determine if your KServer is the latest version available. If an update exists, a message alerts the administrator that an update is currently available and is applied at the next master administrator logon. An update is only downloaded if the version currently running is older than the version available. Otherwise, no action is performed.

Version Number

Shows the version number of the system software and the [hotfix](#) (*page 475*) level of your system.

Warn if the VSA cannot get updates from <http://vsaupdate.kaseya.net> on port 5721

Check this box to display a warning if your VSA cannot connect to <http://vsaupdate.kaseya.net> to fetch the latest hotfix checker list, the latest PCI ID list used by audit, or the VSA software update notifications. Your VSA attempts to automatically fetch this information from <http://vsaupdate.kaseya.net> on port 5721. Verify that [port 5721 outbound](#) is 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.

Note: Each installed agent counts against your license for 30 days. If you uninstall an agent, it will count against your license for 30 more days.

Specify email alert sender address

Specifies the [From](#) email address used by your VSA to send alarms, alerts and other types of email notifications. The email address entered must contain a resolvable domain name that supports SMTP. Click [Set Email](#) to apply the email address entered. Verify the VSA can send email from this address by clicking [Test](#) and entering an address to send an email to.

Note: The system uses the Default SMTP Virtual Server to send email. This 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. If you suspect that you are not receiving emails from the KServer, send test emails to various recipient addresses to confirm whether the Default SMTP Virtual Server can send email or is unable to resolve to a specific domain.

Hotfixes

Several options affect how [hotfixes](#) (*page 475*) update your KServer.

- [Enable automatic check](#) - If checked, your KServer periodically checks for *new only* hotfixes at <http://vsaupdate.kaseya.net>. If any new hotfixes are available, the KServer automatically downloads and applies the hotfixes without any user interaction.
- [Reload](#) - Click to load *all* hotfixes for the version of KServer your system is running. Checking the [Enable automatic check](#) box only checks for *new* hotfixes.
- [Get Latest Hotfix](#) - Click to check if new hotfixes are available *immediately* and, if they are, download and apply them. Otherwise, if the [Enable automatic check](#) box is checked, your KServer checks *periodically* for new hotfixes.
- [Manually apply hotfixes](#) - If your system is not connected to the internet or can not reach <http://vsaupdate.kaseya.net>, then click this list.

System

- **Check Now** - Click to force the system to check for new hotfixes *immediately*. If any new hotfixes are available, they are downloaded and automatically applied. Only *new* hotfixes get loaded.
- **Reload** - Click to re-download and apply all hotfixes for the version of KServer your system is running.

Database

- Click **Reapply Schema** to reinstall 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 scripts.
 - Rebuilds all pre-defined Kaseya script samples.
 - Reschedules default backend processing scripts for the KServer.

This is all completed without the risk of losing any agent data. This is a good self healing routine to run if you observe:

- Scripts 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 401*) page. This might indicate a problem with backend processing scripts.
- Click **Defrag Database** to defragment the physical files on your disk arrays. Fragmented SQL Server data files can slow I/O access.

Warning: Do not use the Microsoft SQL tuning advisor against the schema. It adds keys that conflict with the smooth operation of the system.

Reload Samples

- Check the **Reload sample scripts with every update and database maintenance cycle** box to load sample scripts automatically.
- Check the **Reload sample event sets with every update and database maintenance cycle** box to load sample event sets (*page 120*) automatically.
- Check the **Reload sample monitor sets with every update and database maintenance cycle** box to load sample monitor sets (*page 140*) automatically.
- Click **Reload Samples** to load the latest sample scripts, sample event sets, and sample monitor sets manually.

HTTPS

- **Automatically redirect to https at logon page (except when accessing via localhost)** - If checked, ensures all administrators 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 443*).

Invalid Patch Location Notification

- **Enable Invalid Patch Location Notifications** - Microsoft sometimes prepares patches that do not allow the **File Source** (*page 248*) 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.

Backups

- **Run database backup / maintenance every <N> Days @ <Time>** - The KServer 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 KServer is shut down at the scheduled backup time, the backup will occur the next time the KServer goes online. You can enter zero to disable recurring backups.
- **Backup folder on DB server** - 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 KServer to a database on a different machine by following these steps:
 1. Backup your existing database by clicking [Backup Now](#).
 2. Copy the database backup file to the database server you wish to connect to.
 3. Verify your new database is set to [mixed mode authentication](#).
 - ✓ Open the [SQL Enterprise Manager](#).
 - ✓ Right click the database and select properties.
 - ✓ Click the [Security](#) tab.
 - ✓ Under authentication, select [SQL Server and Windows](#).
 - ✓ Click [OK](#).
 4. Verify your KServer is on the same LAN as your new database server and [port 1433](#) is open on the database server.
 5. Click the [Change DB](#) button.
 6. Enter the database location using one of the following formats:
 - ✓ computer name
 - ✓ computer name\instance name
 - ✓ IP address
 7. 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.
 8. Enter the password associated with this logon name.
 9. Click [Apply](#). The system then connects to the remote database and configures it.
 10. Click [Restore](#) to load the data from the back up file you made in step one into your new database.
- **Backup Now** - Initiate a full database backup now. Use this function *before* you shut down or move your KServer, to ensure you have the latest KServer data saved to a backup. The backup will be scheduled to run within the next 2 minutes.
- **Restore** - Click to restore the KServer's database from a backup file. A file browser displays a list of KServer database backup files you can restore from.

Archive

Archiving of agent logs are enabled, by log and machine ID, using Agent > [Log History](#) (page 328).

System

- [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.
- [Change](#) - Click to the confirm changing the archive file location. A script 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 KServer. A script runs to move any existing archive files in the old file location to the new file location.

Service Status

- [KServer Log](#) - Displays the last 300 kbytes of the KServer'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.
- [Stop Service](#) - Shows the current status of the KServer: **running** or **stopped**. The KServer can be stopped by clicking [Stop Service](#).
- Clear the [Enable alarm generation](#) box to prevent generating unnecessary alarms. This can occur if you stop the KServer, disconnect from the internet, or maintain the system. Otherwise leave this box checked.
- [Enable logging of script errors marked "Continue script if step fail"](#) - If checked, failed steps in scripts are logged. If blank, failed steps in scripts are *not* logged.

Select time format

Click the appropriate radio button to select how time data is displayed. The default is AM/PM format.

- AM/PM format - 9:55:50 pm 9-Apr-07
- 24-hour format - 21:55:50 9-Apr-07

Note: Both these display formats are compatible with Microsoft Excel.

Change external name / IP address of Server

Shows the current external name or IP address of the KServer. 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 KServer. 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.

Change System Server Port

Specify the port used by agents to check into the KServer. Clicking [Change Port](#) switches the port the KServer uses *immediately*.

Warning: Before you change the KServer port ensure that all agents are set to use the new port with their primary or secondary KServer. Agent check-ins are configured using [Agent > Check-in Control \(page 363\)](#).

Version Information

Displays the following information about your VSA configuration.

- OS Version

- IIS Version
- SQL Version
- Database Location
- Agent On KServer

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.

Third Party Copyrights

Click [Third Party Copyrights](#) to display all third party copyrights and licenses associated with open source and third party software components used by the VSA.

License Manager

System > License Manager

The [License Manager](#) page enables a master administrator to allocate machine licenses by group ID. The total number of licenses allocated to a group ID can be distributed between the group itself and any subgroups defined for that group ID. Typically, a group ID represents a single customer and a subgroup represents a customer location. Types of licenses managed include:

- Agent licenses
- Backup and disaster recovery (BUDR) licenses for workstations
- Backup and disaster recovery licenses for servers
- Endpoint Security licenses
- User State Management licenses

Note: Endpoint Security licenses only display on this page if you have separately purchased the Kaseya Endpoint Security addon module.

Note: User State Management licenses only display on this page if you have separately purchased the Kaseya User State Management addon module.

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 477). Machine ID template accounts are not counted as "used" until you install the agent.

Update Code...

Click the [Update Code...](#) to enter a new license code or reapply your existing license code.

System

Expiration Date

Shows the current expiration date of running the system "as is" with the current license code.

Maintenance Expiration Date

Shows the current expiration date of maintenance services, including upgrades, hotfixes and access to tech support.

Apply Limit

- The [Apply Limit](#) table shows the number of licences used and the maximum number of licenses available for agents, BUDR workstation, BUDR servers, and Endpoint Security. You can control the number of licenses of each type assigned to selected groups using the following radio options:
 - No change
 - Limit to a fixed number of licenses
 - Unrestricted

Click [Apply Limit](#) to assign these license settings to 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.

Machine Group

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

Licenses Used / Max

Lists the number of licenses *used* and the *maximum* number of licenses allocated for each group ID, for:

- Agent licenses
- BUDR workstation licenses
- BUDR server licenses
- Endpoint Security licenses
- User State Management licenses

System Log

System > 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
- Video streaming sessions
- Starting/stopping of the KServer
- 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. Reports are only available for data associated with a machine ID.

Statistics

System > Statistics

- Similar information is provided using [Reports > Network Statistics](#) (page 306).

The [Statistics](#) page displays various statistics to provide an indication that the KServer is running optimally. The statistics shown are not affected by the [machine ID/group ID filter](#) (page 477) setting.

Agents currently online

Number of agents currently checking into the system.

Total Licenses Used

Number of licenses used.

Total Template Accounts

Number of [machine ID templates](#) (page 477) defined.

Total Machine IDs

Number of machine IDs defined on the KServer, whether their agents have ever checked in or not.
 $Total Licenses Used + Total Template Accounts = Total Machine IDs.$

KServer CPU usage

over the last 5 minutes: x%
 long term average: x%

Total System CPU usage

over the last 5 minutes: x%
 long term average: x%

Remote Control Sessions

The number of remote control sessions relayed through the KServer 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](#). Click this button to clear out all pending alerts.

System

Pending Patch Scan Results

The number of machines that currently have patch scan results that have been completed but not yet processed. If a KServer 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.

Event log entries last hour

Click [Check](#) to compute the number of event log entries in the last hour for all online managed machines and identify the machine ID that captured the most number of events.

Database Location

Displays the type of 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 KServer.

[New connections in last 10 seconds](#) - Number of new TCP/IP connections accepted by the KServer. 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 KServer.

[Command message queue length](#) - Number of messages, other than check-in, waiting for processing by the KServer.

[Bandwidth - received bytes/second](#) - Bytes per second input into the KServer agent port.

[Bandwidth - sent bytes/second](#) - Bytes per second output from the KServer 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 KServer 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 scripts run in the last hour

This table lists the scripts that have run and completed execution on all online machines in the last hour, with the greatest frequency listed first.

Top scripts pending (online machines only)

This table lists the scripts waiting to execute on all online machines, with the greatest frequency listed first.

Logon Policy

System > Logon Policy

The [Logon Policy](#) page sets logon policies that apply to all administrators and [users](#) (page 212). 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.

To Set Logon Policy

1. Specify the number of consecutive bad logons an administrator or user is allowed before their account is disabled in the [Number of consecutive failed logon attempts allowed before disabling account](#) field. The count is reset to zero after a successful logon.
2. Specify the amount of time, in hours or days, that the account is disabled in the [Length of time to disable account after max logon failures exceeded](#) field.
3. Specify the time period of administrator or user inactivity before the administrator is automatically logged out. Set the number of minutes of inactivity in the [Minutes of inactivity before an administrator session expires](#) field.

Note: To activate the account manually before the lockout time elapses, another master administrator must enable the account using the [System > Enable/Disable](#) (page 390) page.

4. Prevent anyone from changing their logon *name* by checking the box beside [Prevent anyone from changing their logon](#).
5. Hide the [Domain](#) field on the logon page by checking the box beside [Do not show domain on logon page](#).
6. Hide the [Remember my username and domain \(if any\) on this computer](#) checkbox on the logon page by checking the box beside [Do not show remember me checkbox on logon](#).
7. 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](#)
8. Press [Update](#) to apply the settings

Customize

System > Customize

The [Customize](#) page provides four different methods of customizing the user interface that

administrators and users see.

- [Customize the header on the logon page \(both users and administrators\)](#).
- [Customize the function list first seen by users after logon](#).
- [Customize the function list first seen by administrators after logon](#).
- [Customize the graphical user interface](#).

Customize the header on the logon page (both users and administrators).

1. Click the [Customize](#) link associated with this option. This option selects the URL of the top frame seen *by both administrators and users during logon*. Perform the following tasks in any order:
 - Enter the URL of a web page in the [URL of top frame](#) field. Typically this page contains a company logo.
 - Enter the height in pixels of the top most frame of the web page in the [Top frame height](#) field.
 - Click the [Category](#) button at the bottom of the page to create a new category label in the function list. Enter a name for the new category label in the left column text box.
 - Click the [Link](#) button at the bottom of the page to create a new link in the function list. Enter a name for the new link in the left column text box. Enter a URL in the right column text box to direct the browser when the link is selected from the function list.
 - Click the up and down arrow icons  to move a category label or link up or down in the function list. This change is applied immediately.
 - Click the delete icon  next to a existing category label or link to remove the category label or link from the function list.
 - Check or uncheck any of the following display options for the logon page:
 - ✓ [Display Get New Password on logon page](#)
 - ✓ [Display System Status on logon page](#)
 - ✓ [Display System Version on logon page](#)
 - ✓ [Display Customer ID on logon page](#)
2. Click the [Update](#) button at the top of the page to apply your changes to the function list immediately.
3. Click the [Default](#) button at the top of the page to restore the default settings for the home page seen by administrators. This change is applied immediately.
4. Click the [Close](#) link at the top of the page to exit the customization web page.

Customize the function list first seen by users after logon.

1. Click the [Customize](#) link associated with this option. A new web page displays the current function list displayed when a user displays the [User Access Welcome Page](#) (page 484). This option also selects the URL of the top frame seen *by users after logon*. Perform the following tasks in any order:
 - Enter the URL of a web page in the [URL of top frame](#) field. Typically this page contains a company logo.
 - Enter the height in pixels of the top most frame of the web page in the [Top frame height](#) field.
 - Enter the text first shown to users on the web page in the [Default text displayed on the user welcome page](#) text box.
 - Click the [Category](#) button at the bottom of the page to create a new category label in the function list. Enter a name for the new category label in the left column text box.
 - Click the [Link](#) button at the bottom of the page to create a new link in the function list. Enter a name for the new link in the left column text box. Enter a URL in the right column text box to direct the browser when the link is selected from the function list.

- Click the up and down arrow icons  to move a category label or link up or down in the function list. This change is applied immediately.
 - Click the delete icon  next to a existing category label or link to remove the category label or link from the function list.
2. Click the [Update](#) button at the top of the page to apply your changes to the function list immediately.
 3. Click the [Default](#) button at the top of the page to restore the default settings for the home page seen by administrators. This change is applied immediately.
 4. Click the [Close](#) link at the top of the page to exit the customization web page.

Customize the function list first seen by administrators after logon.

1. Click the [Customize](#) link associated with this option. A new web page displays the current function list displayed when an administrator first logs on. Perform the following tasks in any order:
 - Click the [Category](#) button at the bottom of the page to create a new category label in the function list. Enter a name for the new category label in the left column text box.
 - Click the [Link](#) button at the bottom of the page to create a new link in the function list. Enter a name for the new link in the left column text box. Enter a URL in the right column text box to direct the browser when the link is selected from the function list.
 - Click the up and down arrow icons  to move a category label or link up or down in the function list. This change is applied immediately.
 - Click the delete icon  next to a existing category label or link to remove the category label or link from the function list.
2. Click the [Update](#) button at the top of the page to apply your changes to the function list immediately.
3. Click the [Default](#) button at the top of the page to restore the default settings for the home page seen by administrators. This change is applied immediately.
4. Click the [Close](#) link at the top of the page to exit the customization web page.

Customize the graphical user interface.

Click the [Customize](#) link associated with this option. A new web page displays, enabling you to change the entire look of all the web pages. In addition to changing the color scheme, you can customize the top frame of the VSA interface. You can also swap out the Kaseya agent icon displayed in the system tray of each managed machine with your own icon.

Themes

Three themes are provided: [Default](#), [Banner](#) and [Compact](#). You can change any of the attributes of any of the three themes or reset their attributes back to their default settings. The changes you make apply to the graphical display of the entire VSA and to all administrators and users logging into the VSA.

Some of the attributes are only available with specific themes. Principally the three themes differ by how they display the header frame at the top of the page.

Top Frame

- Pixel height of the top frame header
- URL that the logo links to. Applies to Banner theme only.
- Style for unused area to right of menu bar. Applies to Banner theme only.
- Top Frame Header Body Style

System

Module Tabs

- Inactive tab background style
- Active tab background style
- Hover tab background style
- Inactive tab text style
- Active tab text style

Logoff Link

- Logoff link style
- Logoff link hover style

Toolbox

- Toolbox Background Color
- Toolbox Text Color
- Toolbox Text Hover Color

Machine ID.Group ID Filter

- Main Logon / Select Machine ID and Machine Group Body Style
- Select Machine ID and Machine Group Text Style

Function Lists

- Pixel width of the function list frame
- Function List Header Style
- Function Category Header Style
- Function List Hover Style
- Function List Active Selection Style
- Function List Inactive Selection Style
- Function List Background Color
- Function List Frame Color
- Function List Hilite Color

Miscellaneous

- URL that the logo links to.
- Header HTML shown on all reports

Note: You can customize the header HTML shown on all reports by administrator using [Reports > Set Logo \(page 287\)](#).

- HTML displayed on Agent download page.
<here> - link to package, <packageName> - display package name
- Product Title
- Nav Menu Bullet Icon
- Corporate logo image. The color depth cannot exceed 256 colors.

Agent System Tray Icons

- Agent system tray icon when Agent is online (must be .ico format)
- Agent system tray icon when Agent is offline (must be .ico format)
- Agent system tray icon when Agent is blinking (must be .ico format)
- Agent system tray icon when remote control is disabled (must be .ico format)
- Mac Agent menu bar icon when Agent is online (must be .tif format)
- Mac Agent menu bar icon when Agent is offline (must be .tif format)

- Mac Agent menu bar icon when Agent is blinking (must be .tif format)
- Mac Agent menu bar icon when remote control is disabled (must be .tif format)

Note: See [Creating Custom Agent Icons \(page 407\)](#) for more information.

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 KServer.
- `offline.ico` – By default, this is the gray K icon displayed when agent is not connected to the KServer.
- `blink.ico` – By default, this is the white K icon displayed when agent requires the user to click the icon to display a message that has been received using Remote Control > [Send Message \(page 281\)](#).
- `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 KServer.
- `macOffline.tif` - By default, this is the gray K icon displayed when agent is not connected to the KServer.
- `macNoremote.tif` - By default, this is the white K icon displayed when agent requires the user to click the icon to display a message that has been received using Remote Control > [Send Message \(page 281\)](#).
- `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.

Creating Your Own Agent Icons for Windows .ico Files

To create an icon in the Windows format, use an editor such as one in the Microsoft Visual Studio development environment.

1. Select [New > File...](#) from the [File](#) menu in Microsoft Visual Studio.
2. Select an [Icon File](#) template and click the OK button.
3. Edit a standard 32x32 size icon image and save it as one of the four *.ico names listed above.
4. Repeat this step and create four icons.

Note: The color depth must not exceed 256 colors nor be larger than 32x32 pixels.

Uploading Your Custom Agent Icons into the KServer

1. Select System > [Customize \(page 403\)](#).
2. Click the [Customize the graphical user interface](#) link.
3. Scroll to the bottom of the page and update the agent icon images for each of the following items. The agent displays the default VSA icons if any of the custom icons are omitted.
 - Agent system tray icon when agent is online (must be .ico format)
 - Agent system tray icon when agent is offline (must be .ico format)

System

- Agent system tray icon when agent is blinking (must be .ico format)
 - Agent system tray icon when remote control is disabled (must be .ico format)
4. Optionally enter four different agent icons for [Macintosh](#) machines just as you did in step 3. The agent displays the default VSA icons if any of the custom icons are omitted.

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 size cannot be larger than 32x32 pixels.
- The color depth cannot exceed 8 bit color (256 colors).

For [Macintosh](#) custom agent icons:

- The format must be .tif.
- The recommended size is 48x48 pixels and cannot be any larger.
- The color depth should be RGB 32 bit color.

Updating Existing Agents with Custom Agent Icons

Schedule an agent update using Agent > [Update Agent](#) (*page 372*). 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

The custom icons are included in install packages created using the [Create Package](#) wizard in [Deploy Agent](#) (*page 331*). If you are using a `KcsSetup.exe` file created by [Agent Deploy](#) in a domain logon script, then you must replace the `KcsSetup.exe` file on the domain server with the version updated with the new custom icons.

Chapter 13

Database Views

In This Chapter

Database Views	410
Excel Usage	411
Crystal Reporting Usage	411
Views Provided	415
fnMissingPatchCounts_UsePolicy / fnMissingPatchCounts_NoPolicy	416
fnOSCounts	417
vAdminNotesLog	417
vAgentConfiguration	418
vAgentLabel	419
vAlertLog	419
vBackupLog	420
vBaseApplicationInfo / vCurrApplicationInfo	421
vBaseCpuInfo / vCurrCpuInfo	421
vBaseDiskInfo / vCurrDiskInfo	422
vBaseDriveManufacturer / vCurrDriveManufacturer	422
vBasePciInfo / vCurrPciInfo	423
vBasePrinterInfo / vCurrPrinterInfo	423
vCollectionMember	424
vConfigLog	424
vLicenseInfo	425
vMachine	425
vMonitorAlarmAlert	427
vMonitorAlarmCounter	428
vMonitorAlarmProcess	428
vMonitorAlarmService	429
vMonitorAlarmSNMP	430
vMonitorAlarmSystemCheck	430
vNetStatsLog	431
vNtEventLog	431
vOnBoardDeviceInfo	432
vPatchApprovalStatus	432
vPatchPolicy	433
vPatchPolicyMember	434

Database Views

vPatchStatus	434
vPortInfo	436
vScriptLog	436
vScriptStatus	436
vSystemInfo	437
vTicketField	438
vTicketNote	438
vTicketSummary	438

Database Views

System > Database Views

The system exposes a set of **database views and database functions** (page 415) 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 411) and **Microsoft Excel** (page 411). 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 415).

- 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 whenever the Reapply Schema action is taken. A single database user ID, **KaseyaViews** is provided to access these views. 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. 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.

Note: If you have a problem connecting to SQL Server 2005 using the KaseyaViews user ID, see the knowledge base article <http://kb.kaseya.com/article.asp?p=11855&article=307669>
<http://kb.kaseya.com/article.asp?p=11855&article=307669>.

MSDE/SQL Server Variations

If you are using MSDE/SQL Server rather than the full SQL Server, there are a few minor variations to the steps listed above.

- The SQL server name is always [ComputerName]\KVSAMSDE for Kaseya installations before 4.7. For 4.7 Kaseya installations and later the SQL server name is [ComputerName]\KVSAEXPR05.
- Always set the authentication using a logon ID and password. This will be KaseyaViews with the password you have defined.

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).

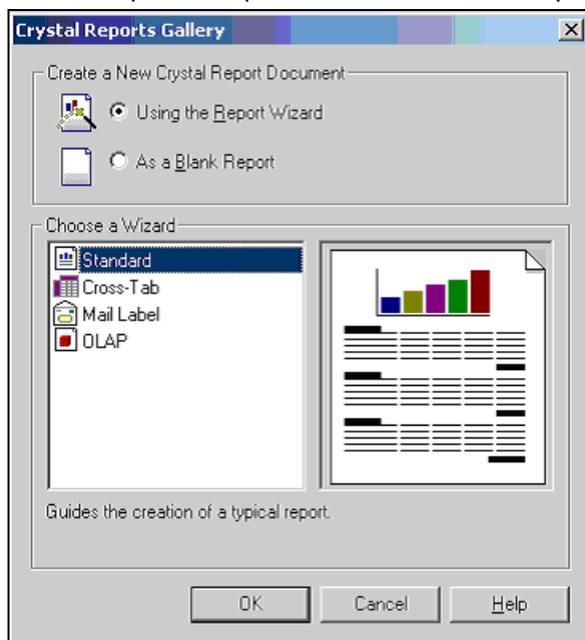
Selecting the Data Source in Excel

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

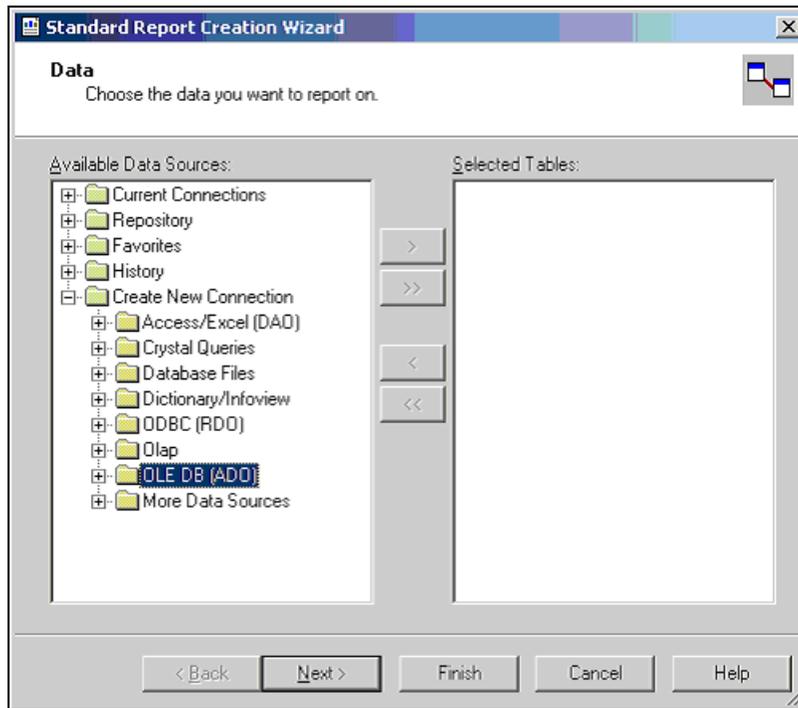
Crystal Reporting can be used to create client specified reports. Crystal 9 and 10 can be used to produce various output formats include PDF, Word and Excel. To set up a report the Crystal Report Wizard can be used. This process begins with the following dialog.

1. The client picks a report format. For this example standard will be used.

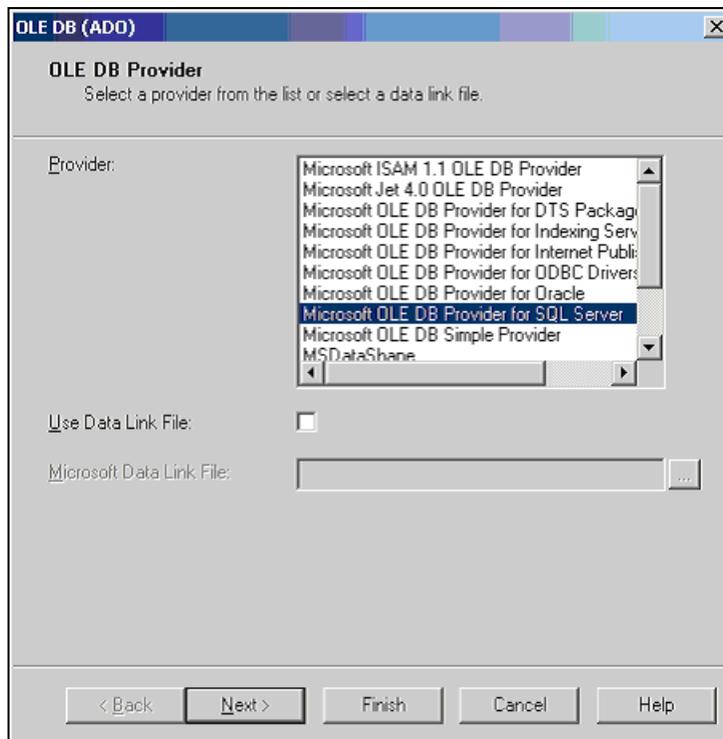


Database Views

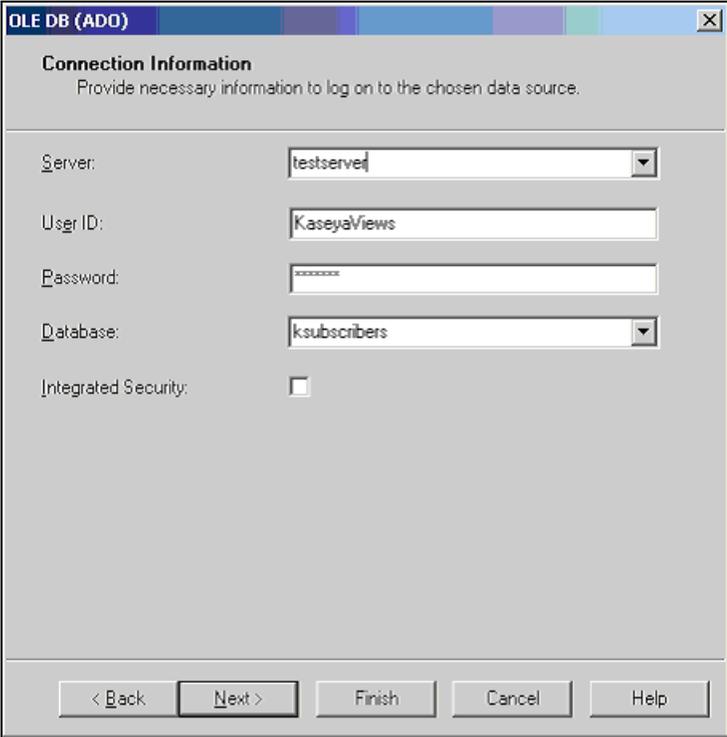
2. Next the data source is selected. This begins by picking an access method. ADO should be selected.



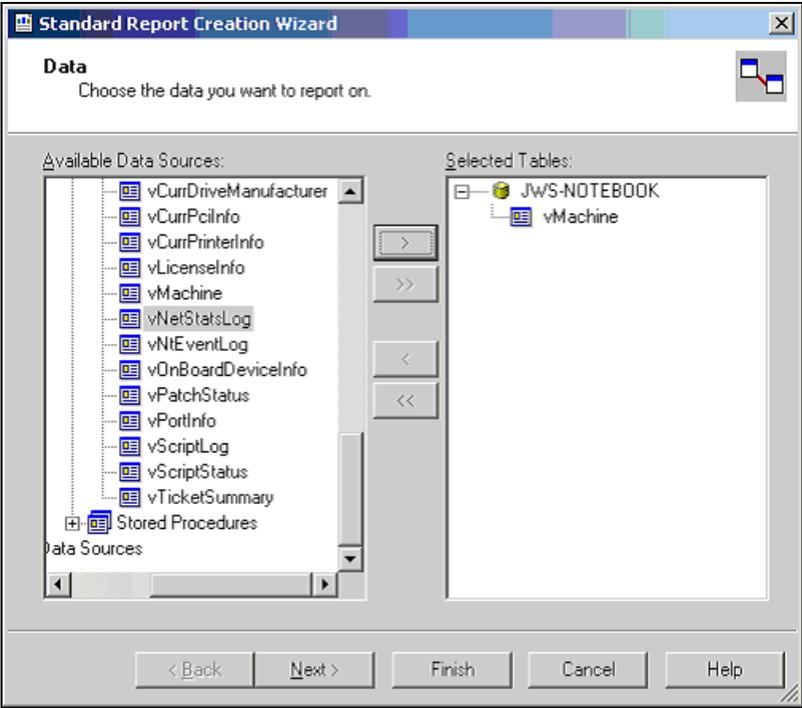
3. Once ADO is selected the SQL Server driver can be selected. This is the correct selection to access the Kaseya database.



- 4. 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.

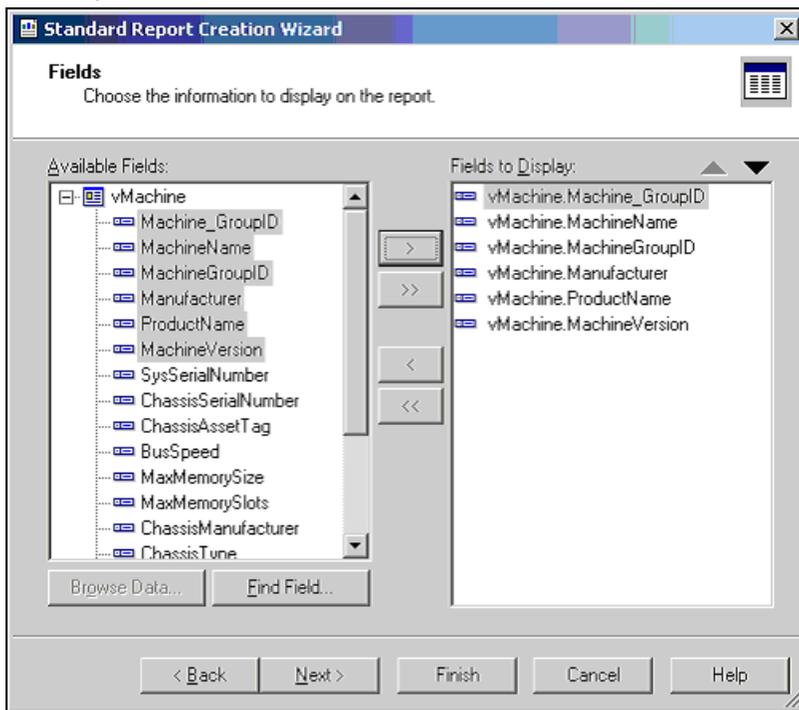


- 5. Once the credentials are provide all the available views are displayed. Pick one or more for the report desired.

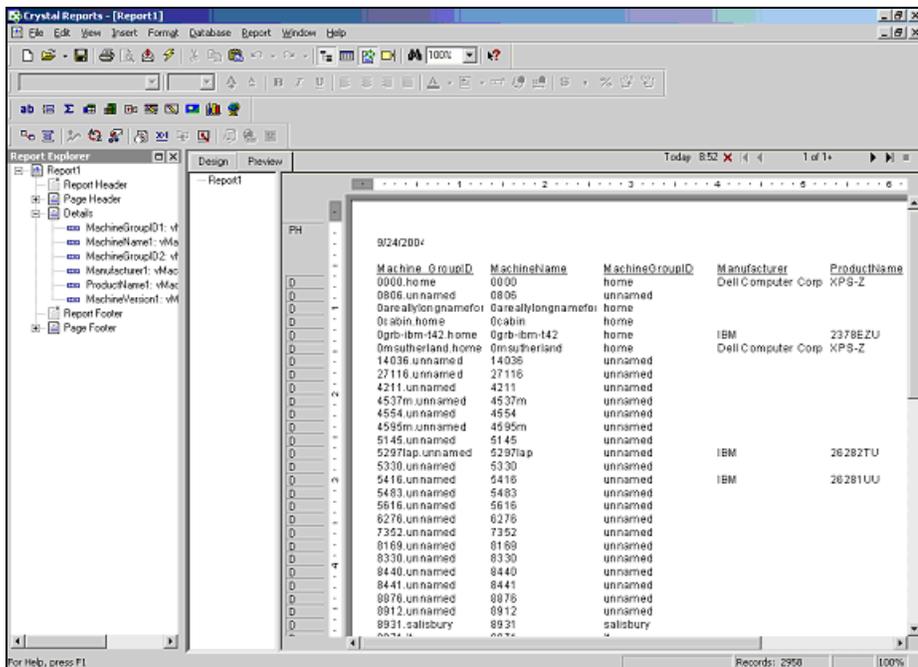


Database Views

- 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.



- 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 Provided

Machines Group	
vBaseApplicationInfo (page 421)	The baseline list of applications on a client desktop machine.
vBaseCpuInfo (page 421)	The baseline list of the CPUs in a client desktop machine.
vBaseDiskInfo (page 422)	The baseline list of the disks in a client desktop machine.
vBaseDriveManufacturer (page 422)	The baseline list of the manufacturers of the disks in a client desktop machine.
vBasePciInfo (page 423)	The baseline list of the PCI cards in a client desktop machine.
vBasePrinterInfo (page 423)	The baseline list of printers in a client desktop machine.
vCollectionMember (page 424)	List the collections each machine ID belongs to (if any)
vCurrApplicationInfo (page 421)	The current list of applications on a client desktop machine.
vCurrCpuInfo (page 421)	The current list of the CPUs in a client desktop machine.
vCurrDiskInfo (page 422)	The current list of the disks in a client desktop machine.
vCurrDriveManufacturer (page 422)	The current list of the manufacturers of the disks in a client desktop machine.
vCurrPciInfo (page 423)	The current list of the PCI cards in a client desktop machine.
vCurrPrinterInfo (page 423)	The current list of printers in a client desktop machine.
vLicenseInfo (page 425)	The licenses of applications on this machine.
vMachine (page 425)	The information known about each client desktop machine.
vOnBoardDeviceInfo (page 432)	The current list of on board devices in a client desktop machine.
vPortInf (page 436)	The current list of ports in a client desktop machine.
vSystemInfo (page 437)	All items collected by the Audit > System Info (page 35) function.
Activity / Status Group	
fnMissingPatchCounts_UsePolicy (page 416)	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 416)	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 417)	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 417)	Notes each admin enters manually for a machine or group of machines. Entries in this log never expire.
vAgentConfiguration (page 418)	Lists agent specific configuration data
vAgentLabel (page 419)	
vAlertLog (page 419)	Logs each alert sent out via email. Multiple rows per machine.
vBackupLog (page 420)	Logs all backup related events
vConfigLog (page 424)	Log of all configuration changes. One entry per change.
vNetStatsLog (page 431)	Network statistics log from the Agent.

Database Views

vNtEventLog (page 431)	NT Event log data collected from each managed machine.
vPatchApprovalStatus (page 431)	Show the approval status of a patch. There is one row for each active patch.
vPatchPolicy (page 433)	Show the approval status of a patch. There is one row for each active patch in each patch policy.
vPatchPolicyMember (page 434)	Lists all patch policies to which each machine ID is a member, if any.
vPatchStatus (page 434)	Information on the state of all patches on a per machine basis. There is one row per patch for each machine.
vScriptLog (page 432)	Log of script executions as viewed by the KServer.
vScriptStatus (page 436)	Script status for each client.
Ticketing Group	
vTicketSummary (page 438)	Trouble ticket summary. One row per ticket. Column names are used as the names displayed in the view summary table.
vTicketNote (page 438)	The notes associated with a ticket. Potentially multiple rows per ticket.
vTicketField (page 438)	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 427)	The current list of alarms for all alerts.
vMonitorAlarmCounter (page 428)	The current list of alarms for all monitor counters.
vMonitorAlarmProcess (page 428)	The current list of alarms for all monitor processes.
vMonitorAlarmService (page 429)	The current list of alarms for all monitor services.
vMonitorAlarmSNMP (page 430)	The current list of alarms for all monitor SNMP Get objects.
vMonitorAlarmSystemCheck (page 430)	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
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

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

vAdminNotesLog

vAdminNotesLog	Notes each admin enters manually for a machine or group of machines. Entries in this log never expire.
----------------	--

Database Views

Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
AdminLogin	varchar	Admin logon name. (note: no not name this col adminName)
EventTime	datetime	Time stamp string representing the time the action took place. Default is CURRENT_TIMESTAMP so nothing needs to be entered here.
NoteDesc	varchar	description of the action

vAgentConfiguration

Column Name	Type	Purpose
vAgentConfiguration Logs each alert sent out via email. Multiple rows per machine		
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
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	varchar	login name of the currently logged in user. Blank if no one logged in at this time
lastLoginName	varchar	login name of the last user to log into this system
workgroupDomainType	tinyint	0 (or Null) = unknown 1 = not joined to either 2 = member of workgroup 3 = member of domain 4 = domain controller
workgroupDomainName	nvarchar	The name of the workgroup or domain
lastReboot	datetime	timestamp when this system was last rebooted
agentVersion	int	version number of agent installed on this system
contactName	varchar	User contact name assigned to this agent
contactEmail	varchar	User email address assigned to this agent
contactPhone	varchar	Contact phone number assigned to this agent
contactNotes	varchar	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

loginName	varchar	Login Name assigned to this user (if any) to access the system user portal interface.
credentialName	varchar	The username of the credential set for this agent (if any)
primaryKServer	varchar	address:port agent connects to for its primary kserver connection
secondaryKServer	varchar	address:port agent connects to for its secondary kserver connection
quickCheckinSecs	int	interval in seconds between quick checkins
agentTempDir	varchar	The temp directory used by the agent on this system

vAgentLabel

vAgentLabel		
Column Name	Type	Purpose
displayName	varchar	The name of the machine ID.group name.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
agentGuidStr	varchar	A string version of agentGuid. Some languages convert the large number numeric to exponential notation. This string conversion prevents that.
online	int	0 -> Agent is offline. 1 -> Agent is online.
timezoneOffset	int	The timezone offset for the agent as compared to universal time.
currentLogin	varchar	The login name of the current user.
toolTipNotes	varchar	The tooltip text displayed for a machine ID.
showToolTip	tinyint	0 -> Do not show machine ID tool tips. 1 -> Do show tool machine ID tool tips.
agntTyp	int	0 -> windows agent 1 -> mac agent

vAlertLog

vAlertLog		
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	time stamp when the event was recorded

Database Views

AlertEmail	varchar	email address to send the alert to
AlertType	int	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 -> Script failure detected 6 -> NT Event Log error detected 7 -> KServer 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	Email subject line
EmailBody	varchar	Email body

vBackupLog

vBackupLog	Logs each alert sent out via email. Multiple rows per machine	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	time stamp when the event was recorded
description	varchar	description of the reported task
durationSec	int	number of seconds the reported task took to complete
statusType	int	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 cancelled 18: folder backup cancelled 19: volume image conversion (in BUDR 3.0) 20: volume synthetic full backup (in BUDR 3.0) 21: folder synthetic full backup (in BUDR 3.0)
result	int	0: failure 1: success 2: archive incomplete
imageSize	float	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	vchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	vchar	Machine Name used for each agent
groupName	vchar	Group Name used for each agent
ProductName	vchar	Product name (e.g. Microsoft Office 2000)
ProductVersion	vchar	Version (e.g. 9.0.3822)
ApplicationName	vchar	Application name (e.g. Winword.exe)
manufacturer	vchar	Manufacturers name (e.g. Microsoft Corporation)
ApplicationDesc	vchar	Description (e.g. Microsoft Word for Windows)
LastModifiedDate	vchar	File date (e.g. 02/24/2000 17:23:44)
ApplicationSize	int	File size in bytes (e.g. 8810548)
DirectoryPath	vchar	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

Database Views

Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
CpuDesc	varchar	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)

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	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
DriveLetter	varchar	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	varchar	Fixed = hard diskRemovable = floppy or other removable mediaCDROMNetwork = mapped network drive
VolumeName	varchar	Name assigned to the volume
FormatType	varchar	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	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
DriveManufacturer	varchar	Manufacturer name (data currently has 8 characters max)
DriveProductName	varchar	Product identification (data currently has 16 characters max)
DriveProductRevision	varchar	Product revision (data currently has 4 characters max)
DriveType	varchar	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	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
VendorName	varchar	PCI Vendor Name
productName	varchar	PCI Product Name
ProductRevision	int	Product revision
PciBaseClass	int	PCI base class number
PciSubclass	int	PCI subclass number
PciBusNumber	int	PCI bus number
PciSlotNumber	int	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 administrator.	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.

Database Views

agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
PrinterName	varchar	Name given to the printer. Same as shown in the Control Panels printer configuration window.
PortName	varchar	Name of the port to which the printer is attached. Same as shown in the Control Panels printer configuration window.
PrinterModel	varchar	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	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
collectionName	varchar	Collection Name

vConfigLog

vConfigLog	Log of all configuration changes. One entry per change.	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	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	Description of the change

vLicenseInfo

vLicenseInfo		License information collected during audit.
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
Publisher	varchar	software publisher (usually in the Publisher reg value)
ProductName	varchar	Software title (usually in DisplayName value but may be the reg key title)
LicenseCode	varchar	License code (usually in the ProductID value)
LicenseVersion	varchar	version string returned by the scanner (if any)
InstallDate	varchar	install date string returned by the scanner (if any)

vMachine

vMachine		The information known about each client desktop machine.
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	full machine name. Everything to the left of the left most decimal point is the machine name.
groupName	varchar	full group name for this account. Everything to the right of the left most decimal point is the group name.
Manufacturer	varchar	Manufacturer string (type 1)
ProductName	varchar	Product Name string (type 1)
MachineVersion	varchar	Version string (type 1)
SysSerialNumber	varchar	Serial Number string (type 1)
ChassisSerialNum	varchar	Chassis Serial Number (type 3)
ChassisAssetTag	varchar	Chassis Asset Tag number (type 3)
BusSpeed	varchar	External Bus Speed (in MHz) (type 4)
MaxMemorySize	varchar	Maximum Memory Module Size (in MB) (type 16 - Maximum Capacity or if type 16 not available, Maximum Memory Module Size type 5)
MaxMemorySlots	varchar	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	Chassis Manufacturer (type 3)
ChassisType	varchar	Chassis Type (type 3)

Database Views

ChassisVersion	varchar	Chassis Ver (type 3)
MotherboardManufacturer	varchar	Motherboard Manufacturer (type 2)
MotherboardProductCode	varchar	Motherboard Product Code (type 2)
MotherboardVersion	varchar	Motherboard Version (type 2)
MotherboardSerialNumber	varchar	Motherboard Serial Number (type 2)
ComputerName	varchar	Name of the Computer
IpAddress	varchar	IP Address of the computer in a.b.c.d notation
SubnetMask	varchar	Subnet mask in a.b.c.d notation. String is empty if data is unavailable
DefaultGateway	varchar	Default gateway IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer1	varchar	DNS server #1s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer2	varchar	DNS server #2s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer3	varchar	DNS server #3s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer4	varchar	DNS server #4s IP address in a.b.c.d notation. String is empty if data is unavailable.
DhcpEnable	int	0 -> Data is unavailable 1 -> DHCP on client computer is enabled 2 -> Disabled
DhcpServer	varchar	DHCP servers IP address in a.b.c.d notation. String is empty if data is unavailable.
WinsEnabled	int	0 -> Data is unavailable 1 -> WINS resolution on client computer is enabled 2 -> Disabled
PrimaryWinsServer	varchar	Primary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
SecondaryWinsServer	varchar	Secondary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
ConnectionGatewayIp	varchar	IP Address in a.b.c.d notation obtained by the Kserver 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	varchar	String contains OS type, such as 95, 98, NT4, 2000, NT3.51, or WIN32s. Derived from portions of MajorVersion, MinorVersion, and PlatformId.
OsInfo	varchar	String contains additional OS info, such as Build 1381 Service Pack 3. Derived from portions of BuildNumber and CsdVersion.
MajorVersion	int	Major version number from GetVersionEx() Windows function call.
MinorVersion	int	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	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	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.
--	--------------

vMonitorAlarmAlert

Column Name	Type	Purpose
vMonitorAlarmAlert Listing of all alarms created by monitor alerts.		
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar	Machine Name used for each agent
GroupName	varchar	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	tinyint	4 -> Monitor alert
EventLogType	int	Only applies to AlertType=6(NT Event Log) 0 -> Application Event Log 1 -> System Event Log 2 -> Security Event Log
AlarmType	smallint	0 -> Alarm 1 -> Trending
AlertType	int	2 -> Get File change alert 3 -> New Agent checked in for the first time 4 -> Application has been installed or deleted 5 -> Script failure detected 6 -> NT Event Log error detected 8 -> Protection violation detected 9 -> PCI configuration has been changed 10 -> Disk drive configuration change 11 -> RAM size changed 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	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
AdminName	varchar	Administrator who assigned monitor alert to machine

vMonitorAlarmCounter

vMonitorAlarmCounter		Listing of all alarms created by monitor counters.
Column Name	Type	Purpose
Machine_GroupID	vchar	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	vchar	Machine Name used for each agent
GroupName	vchar	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	tinyint	0 -> Monitor Counter
MonitorName	vchar	Name of monitor counter object
AlarmType	smallint	0 -> Alarm 1 -> Trending
Message	vchar	Message created from alarm, email message body
AlarmSubject	vchar	Subject of alarm and email subject
AlarmEmail	vchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	Value causing alarm
AdminName	vchar	Administrator who assigned monitor counter to machine

vMonitorAlarmProcess

vMonitorAlarmProcess		Listing of all alarms created by monitor processes.
Column Name	Type	Purpose
Machine_GroupID	vchar	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	vchar	Machine Name used for each agent
GroupName	vchar	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	tinyint	2 -> Monitor Process
MonitorName	vchar	Name of monitor process object
AlarmType	smallint	0 -> Alarm 1 -> Trending
Message	vchar	Message created from alarm, email message body
AlarmSubject	vchar	Subject of alarm and email subject

AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	Value causing alarm, below are process values: 0 -> Stopped 1 -> Running
AdminName	varchar	Administrator who assigned monitor process to machine

vMonitorAlarmService

vMonitorAlarmService	Listing of all of the alarms created by monitor services.	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar	Machine Name used for each agent
GroupName	varchar	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	tinyint	0 -> Monitor Service
MonitorName	varchar	Name of monitor service object
AlarmType	smallint	0 -> Alarm 1 -> Trending
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	Value causing alarm, below are service values: -1 -> Does not exist 0 -> Reserved 1 -> Stopped 2 -> Start Pending 3 -> Stop Pending 4 -> Running 5 -> Continue Pending 6 -> Pause Pending 7 -> Paused
AdminName	varchar	Administrator 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	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar	Machine Name used for each agent
GroupName	varchar	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	tinyint	3 -> Monitor SNMP Get
MonitorName	varchar	Name of monitor SNMP Get object
AlarmType	smallint	0 -> Alarm 1 -> Trending
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	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	Name returned from SNMP Device on scan
SNMPCustomName	nvarchar	Custom name for SNMP Device
AdminName	varchar	Administrator who assigned monitor SNMP Get to machine

vMonitorAlarmSystemCheck

vMonitorAlarmSystemCheck		Listing of all alarms created by monitor system checks.
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar	Machine Name used for each agent
GroupName	varchar	Group Name used for each agent
MonitorAlarmID	int	unique monitor alarm number
MonitorType	tinyint	5 -> Monitor system check
SystemCheckType	int	1 -> Web Server 2 -> DNS Server 4 -> Port Connection

		5 -> Ping 6 -> Custom
AlarmType	smallint	0 -> Alarm 1 -> Trending
Parameter1	varchar	First parameter used in system check
Parameter2	varchar	(Optional) Second parameter used by system check
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
AdminName	varchar	Administrator who assigned of monitor counter to machine

vNetStatsLog

vNetStatsLog	network statistics log from the Agent	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	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	Number of bytes received during this statistics period
BytesSent	int	Number of bytes sent during this statistics period
ApplicationName	varchar	Application name using the network

vNtEventLog

vNtEventLog	Event log data collected from each managed machine	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent

Database Views

LogType	int	1 -> Application Log 2 -> Security Log 3 -> System Log
EventType	int	1 -> Error 2 -> Warning 4 -> Informational 8 -> Success Audit 16 -> Failure Audit
EventTime	datetime	Time the event occurred
ApplicationName	varchar	event log source
EventCategory	varchar	event log category
EventID	int	event log event ID
UserName	varchar	event log user
ComputerName	varchar	event log computer name
EventMessage	varchar	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	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
DeviceType	varchar	Device Type
DeviceDesc	varchar	Device Description

vPatchApprovalStatus

vPatchApprovalStatus	Show the approval status of a patch. There is one row for each active patch.	
Column Name	Type	Purpose
patchDataId	int	Unique identifier for this patch within the database
KBArticle	varchar	Microsoft knowledge base article number
SecurityBulletin	varchar	Microsoft security bulleting number
Title	varchar	Patch title

UpdateClassificationId	smallint	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	Textual representation of the patch update classification
Product	varchar	Product this to which this patch is associated
PublishedDate	datetime	Date that this patch was last update by Microsoft, if available
Language	varchar	Language support for the patch
numApproved	int	Number of patch policies in which this patch is approved
numDenied	int	Number of patch policies in which this patch is denied
numPending	int	Number of patch policies in which this patch is pending approval
InstallationWarning	varchar	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', or an empty string.

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	Unique identifier for this patch within the database
Policy	varchar	Name of patch policy
KBArticle	varchar	Microsoft knowledge base article number
SecurityBulletin	varchar	Microsoft security bulleting number
Title	varchar	Patch title
UpdateClassificationId	smallint	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)

Database Views

UpdateClassification	varchar	Textual representation of the patch update classification
ApprovalStatusId	smallint	Numeric representation of the patch approval status; included to make filtering easier; Values are: 0 = Approved 1 = Denied 2 = Pending Approval
ApprovalStatus	varchar	Textual representation of the patch approval status
Product	varchar	Product this to which this patch is associated
PublishedDate	datetime	Date that this patch was last update by Microsoft, if available
Language	varchar	Language support for the patch
Admin	varchar	Name of administrator 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	Timestamp of most recent approval status change
StatusNotes	varchar	Notes added by Admin concerning the patch approval status
InstallationWarning	varchar	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', or an empty string.

vPatchPolicyMember

vPatchPolicyMember	Lists all patch policies to which each machine ID is a member, if any.	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id to which it is associated
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
PolicyName	varchar	Patch Policy Name

vPatchStatus

vPatchStatus	Shows the state of all patches on a per machine basis. There is one row per patch for each machine.	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
MachineName	varchar	Machine Name used for each agent
GroupName	varchar	Group Name used for each agent
KBArticle	varchar	Microsoft KB article number reported from the patch scanner.

Database Views

SecurityBulletin	varchar	bulletin ID string reported from the patch scanner
Title	varchar	Update title.
Product	varchar	Product to which patch is associated
UpdateClassification	smallint	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
ReleaseDate	datetime	Patch release date
InstallSeparate	tinyint	0 -> this can be installed together with other patches 1 -> this must be installed separately (its own reboot) from other patches
IsSuperseded	tinyint	0 -> update is not superseded 1 -> update is superseded by a subsequent update
PatchAppliedFlag	int	0 -> patch has not been applied 1 -> patch has been applied
PatchStatus	int	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
PatchIgnoreFlag	int	0 -> process this patch 1 -> ignore this patch
InstallDate	dateTime	timestamp when this patch was applied by the VSA
InstalledBy	varchar	Name of admin (if we installed the patch) or value from registry (if scanner returned the value)
InstallationWarning	varchar	Returns 'Manual Install Only', 'Windows Update Only', 'Product Upgrade Only', or an empty string.
Description	varchar	Patch description
UninstallNotes	varchar	Uninstall notes for the patch

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	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
InternalDesc	varchar	Internal Description
ExternalDesc	varchar	External Description
ConnectionType	varchar	Connection Type
PortType	varchar	Port Type

vScriptLog

vScriptLog		Log of script executions as viewed by the KServer
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	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	Name of script
ScriptDesc	varchar	Event description
AdminName	varchar	Admin name that scheduled this script.

vScriptStatus

vScriptStatus		script status for each client
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.

machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
ScriptName	varchar	Name of script
LastExecTime	datetime	Time stamp string representing the last time that the script was executed
lastExecStatus	varchar	Status of the last execution. The string will be one of the following:Script Summary: Success <ELSE or THEN>Script Summary: Failed <ELSE or THEN> in # step<ELSE or THEN> is replaced with the respective word ELSE or THEN.# is replaced by the number of steps that failed in the script (not useful unless allowing the processing to continue after a failure)step is replaced by the work steps if the script failed more than 1 step.
AdminLogin	varchar	Admin name that last scheduled this script. (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 System Info function	
Column Name	Type	Purpose
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
Manufacturer	varchar	System manufacturer string
Product Name	varchar	Name or model number of the machine supplied by the manufacturer
System Version	varchar	Machine version string
System Serial Number	varchar	Machine serial number string entered by the manufacturer
Chassis Serial Number	varchar	Serial number string supplied by the manufacturer
Chassis Asset Tag	varchar	Asset tag string supplied by the manufacturer
External Bus Speed	varchar	Motherboard bus speed
Max Memory Size	varchar	Max memory this system may be configured with
Max Memory Slots	varchar	Max number of memory slots this system has
Chassis Manufacturer	varchar	Name of manufacturer of the chassis
Chassis Type	varchar	system chassis type
Chassis Version	varchar	version string of the chassis
Motherboard Manufacturer	varchar	Name of motherboard manufacturer
Motherboard Product	varchar	Motherboard model name
Processor Family	varchar	processor family name
Processor Manufacturer	varchar	processor manufacturer name

Database Views

Processor Version	varchar	processor version string
CPU Max Speed	varchar	max speed of this processor
CPU Current Speed	varchar	configured speed of this processor

* Custom columns defined using Audit > [System Info](#) (page 35) display as additional columns at the end of this view.

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	unique trouble ticket ID number
TicketLabel	varchar	The label of the field
IntegerValue	int	The value of a integer field
NumberValue	numeric	The value of a number field
StringValue	varchar	The value of a string field
ListValue	varchar	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	unique trouble ticket ID number
Author	varchar	person who wrote this note in the ticket
TicketNoteTime	dateTime	Timestamp identifying when the note was added
TicketNote	varchar	Contents of the ticket note
HiddenNote	int	0 if the note is visible. 1 if the note is hidden.

vTicketSummary

vTicketSummary	Trouble ticket summary. One row per ticket. Column names are used as the names displayed in the view summary table.	
Column Name	Type	Purpose
TicketID	int	unique trouble ticket ID number
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.

Database Views

agentGuid	numeric	A globally unique identifier for a machine ID.group ID account and its corresponding agent.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
TicketSummary	varchar	summary string briefly describing the ticket
Assignee	varchar	Admin name this ticket is assigned to
CreatedBy	varchar	admin name (or machine ID if entered by user) of the person that created this ticket
CreationDate	datetime	timestamp when the ticket was created
DueDate	datetime	ticket due date
LastModifiedDate	datetime	Date of the most recent note entered for this ticket
ResolutionDate	datetime	timestamp when the ticket was closed
UserName	varchar	The name of the submitter
UserEmail	varchar	The email address of the submitter
UserPhone	varchar	The phone number of the submitter

Chapter 14

VSA API Web Service

In This Chapter

Overview	443
Operations	453

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

Click [here](#) for a complete list of operations.

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 394) page in the VSA.
- Check the [Enable VSA API Web Service](#) checkbox.
- Append the string `/vsaWS/KaseyaWS.asmx` to the VSA URL you are using to display the VSA API Web Service.

Special Fields

The following fields are included in the response to every request.

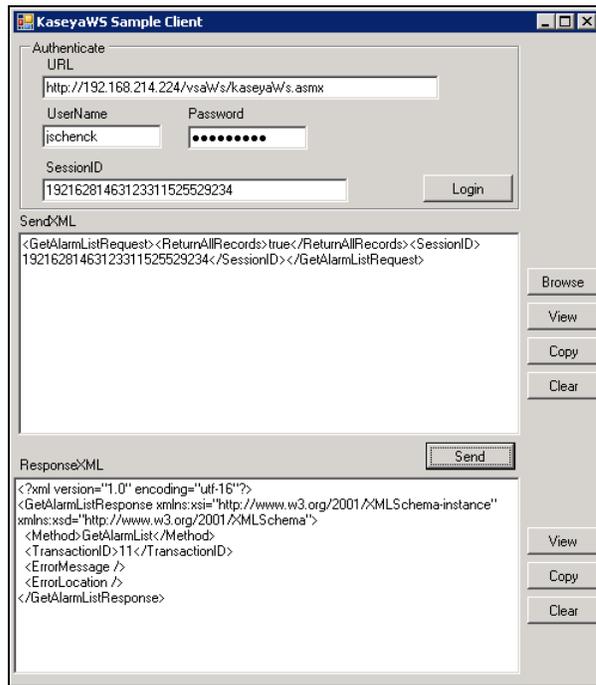
Method	string	The operation that requested this response.
TransactionID	decimal	The unique message ID for this message.
ErrorMessage	string	If blank, no error was returned.
ErrorLocation	string	If blank, no error was returned.

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.

VSA API Web Service Sample Client - C# GUI 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 VSA API Web Service [Sample Client](#) 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: An ASP page text client ([page 446](#)) is also provided.



To run the sample client:

1. Run the sample client located on your KServer:

```
<Install Dir>\vsaWs\TestClient\KaseyaWStestClient.exe
```
2. Enter the **UserName** and **Password** of a user authorized to connect with the KServer.

Note: This is the same username and password that an administrator uses to login into the KServer.

3. Click the **Login** button to display a value in the **SessionID** field.
4. 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.

5. Click the **Send** button to send the XML message to the target URL. A response XML message displays in the **ResponseXML** textbox.

VSA API Web Service Sample Client - ASP Page

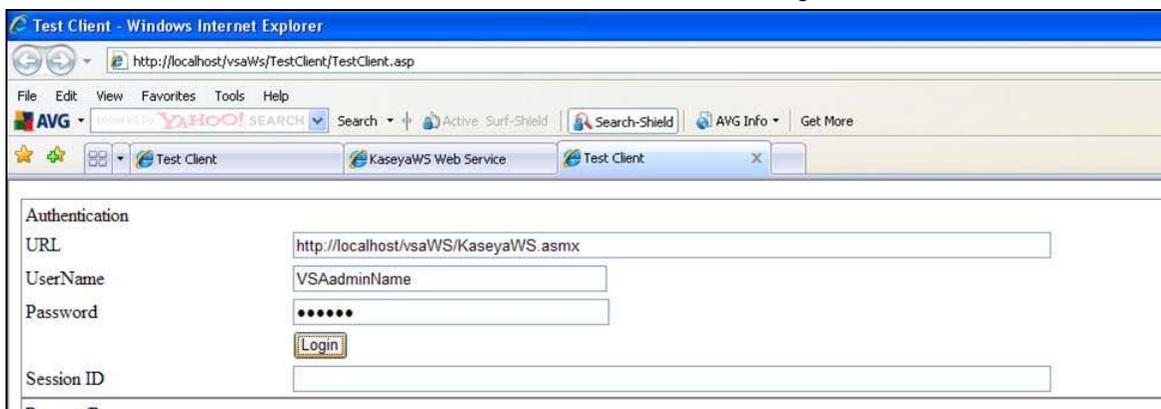
A test client ASP page is also distributed with the VSA API Web Service to help you familiarize yourself with the various API operations. You can use it to see how the ASP client was constructed and incorporate any part of its code into your own application. Users can browse to the actual `/vsaWS/KaseyaWS.asmx` page of any Kserver, 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.

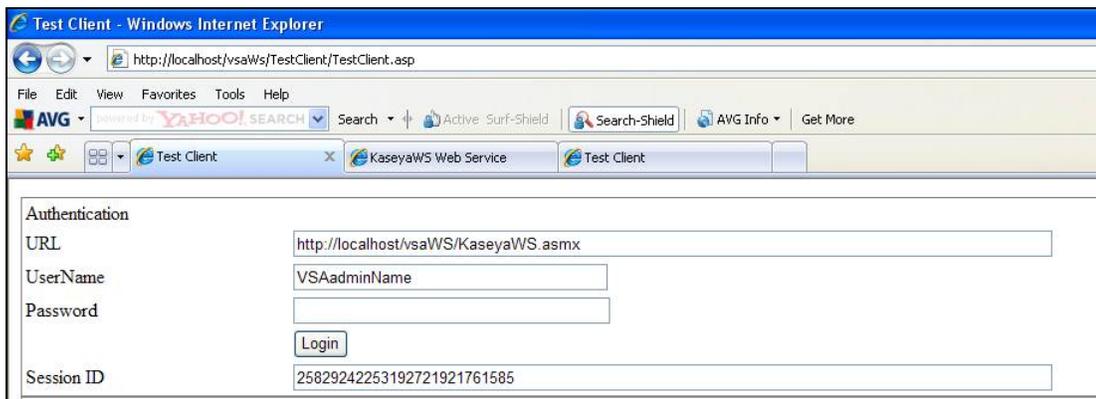
Note: This page does not automatically incorporate the displayed sessionID into subsequent request statements like the C# GUI Test Client (page 445) does.

Example 1: Authentication

1. Enter a valid VSA administrator Username and Password and click Login.

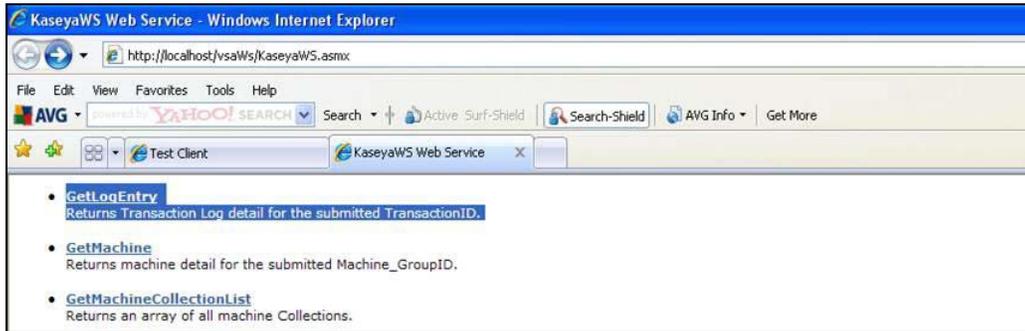


The Session ID textbox is populated with the session ID generated by your logon. You will need to copy and paste this session ID into subsequent XML requests.

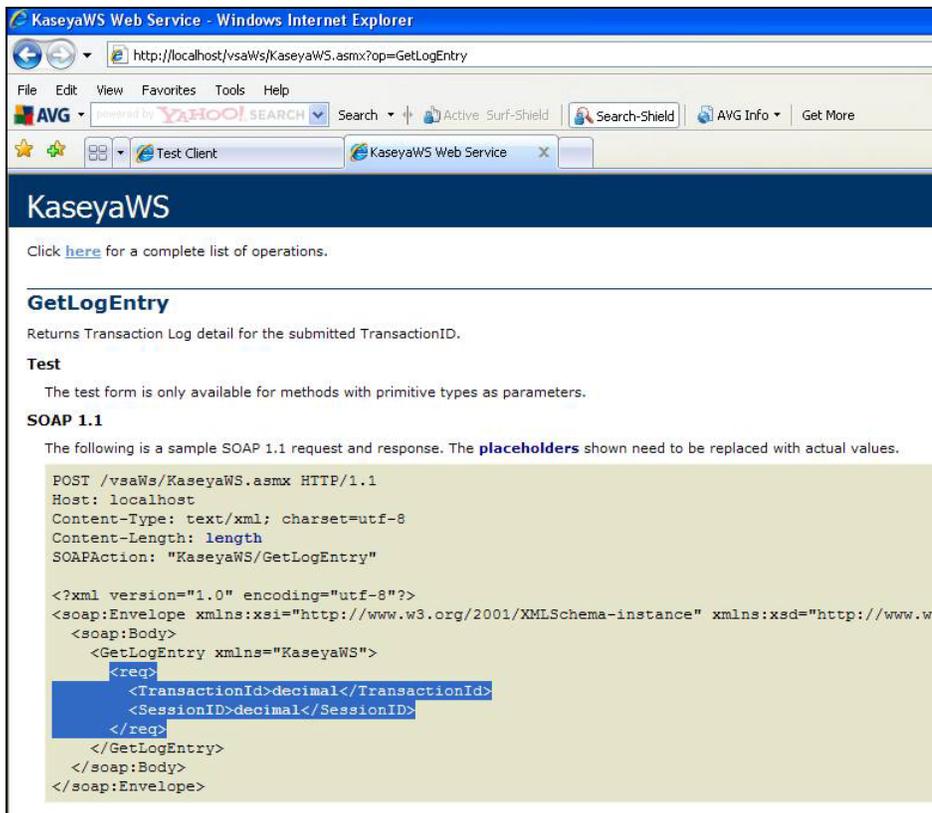


Example 2 - Creating a Get Request

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>`.



VSA API Web Service

3. Paste the request structure into the **Request** pane of the `TestClient.aspx` 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. The `<BrowserIP>` element helps to provide single-signon coordination with the VSA, and can be ignored in a testing environment where single-signon is not the focus.

The screenshot shows the Test Client application in a browser window. The URL is `http://localhost/vsaWS/TestClient/TestClient.aspx`. The application is divided into several sections:

- Authentication:** URL is `http://localhost/vsaWS/KaseyaWS.asmx`, Username is `VSAadminName`, Password is empty, and Session ID is `25829242253192721921761585`. A **Login** button is present.
- Request/Response:** Service URL is `http://localhost/vsaWS/KaseyaWS.asmx`, Web Service Name is `KaseyaWS`, and Web Method Name is `GetLogEntry`.
- Request:** The XML request is:

```
<req>
  <TransactionId>17</TransactionId>
  <SessionID>25829242253192721921761585</SessionID>
</req>
```
- Response:** The XML response is:

```
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><GetLogEntryResponse
xmlns="KaseyaWS"><GetLogEntryResult><LogTransactionId>17</LogTransactionId><Log
ErrorLocation /><LogErrorMessage /><LogMethod>GetMachineList</LogMethod><Execut
ionTimeInSeconds>0</ExecutionTimeInSeconds><SessionId>2582924225319272192176158
5</SessionId><UserName>darrel</UserName><ClientIP>127.0.0.1</ClientIP><DateSubm
itted>2009-04-29T14:39:28.517-05:00</DateSubmitted><DateUpdated>2009-04-
29T14:39:28.547-
05:00</DateUpdated><TransactionXML /><Method>GetLogEntry</Method><TransactionID
>18</TransactionID><ErrorMessage /><ErrorLocation /></GetLogEntryResult></GetLo
gEntryResponse</soap:Body></soap:Envelope>
```

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 VSA administrator 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"`

VSA API Web Service

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>
```

```
</UserMapping>
</AccessRules>
```

Web Links - Inbound and Outbound

Aside from API operations described later in the document, the KServer also supports the following inbound and outbound links:

Inbound

The URL to display the [Machine Summary](#) web page for a specific machine ID is:

`http://...?machName=<MachineID>`

For example:

<http://demo.kaseya.com?machName=jconners.acme>

The screenshot shows the Kaseya KServer interface for a machine named 'morpheus.unnamed'. The page has a navigation bar with tabs for Machine Info, Installed Applications, System Info, Disk Volumes, PCI & Disk Hardware, Printers, Pending Scripts, Agent Logs, Alerts, Patch Status, Remote Control, and Agent Settings. The main content area is divided into three sections: Computer Information, Network Information, and Time Information.

Computer Information	
Computer Name:	morpheus
OS:	XP
Version:	Professional Edition Service Pack 2 Build 2600
RAM:	1023MB
CPU:	(1) 1993 MHz Intel(R) Pentium(R) 4 CPU 2.00GHz, Model 2 Stepping 4

Network Information	
IP Address:	192.168.240.101
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.240.1
Connection Gateway:	66.218.38.45
MAC Address:	00-08-A1-03-48-5A
DHCP Server:	192.168.240.1
DNS Server:	66.51.205.100 - 66.51.206.100
Primary WINS:	WINS disabled
Secondary WINS:	

Time Information	
KServer time (local):	5:49:46 pm 25-Oct-07
Agent time (local):	5:49:46 pm 25-Oct-07

Powered by Kaseya - Copyright © 2000-2007 Kaseya. All rights reserved.

VSA API Web Service

The URL to display the **Ticket** web page for a specific ticket ID is:

Error! Hyperlink reference not valid.>

For example:

<http://demo.kaseya.com?ticaid=1234>

Ticket ID: Associate ticket with:

Summary:

Submitter Information	Assignee: <input type="text" value="< unassigned >"/>
Name: <input type="text"/>	Category: <input type="text" value="Workstation configuration"/>
Email: <input type="text"/>	Status: <input type="text" value="Open"/>
Phone: <input type="text"/>	Priority: <input type="text" value="High"/>
Date Created: 7:33:49 pm 12-Oct-07	SLA Type: <input type="text" value="None"/>
Age: 12 days 22 hrs	Dispatch Tech: <input type="text" value="Yes"/>
Date Due: 7:33:49 pm 1-Nov-07	Approval: <input type="text" value="Not required"/>
	Hours Worked: <input type="text" value="0.00"/>
	On site: <input type="text" value="Yes"/>
	Warranty Work: <input type="text" value="Yes"/>
	Billable: <input type="text" value="Yes"/>
	Phone Number: <input type="text"/>
	Contact Email: <input type="text"/>
	Hardware type: <input type="text" value="Laptop"/>
	Blood type: <input type="text" value="ab-"/>
	Number of Siblings: <input type="text" value="0"/>

Enter new note Suppress email notifications

Time/Admin	Note	Hide
7:33:49 pm 12-Oct-07	D: on mt-ws002.unnamed has 12356MB free space (10.6%) on a 115718MB disk drive "Alert"	<input type="checkbox"/>

Outbound

To customize the **New Ticket** link on the **Machine Summary** 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 KServer.

```
<?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>
```

Operations

The following operations can be performed using the [VSA API Web Service](#).

Admin Group Access

Assigns a machine group to an administrator 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.

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. So, if the application developer needs to redirect to a VSA page, he can now get directly to a page 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 403) page, and has a system default value of 30 minutes.

CloseAlarm

Closes the alarm for the submitted MonitorAlarmID.

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 standard administrator. 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.

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.

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 an administrator 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 administrator.

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.

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.

DeleteRole

Deletes the specified administrator 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.

DisableAdmin

Disables a specified administrator.

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.

VSA API Web Service

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.
------------	--------	--

EnableAdmin

Enables a specified administrator.

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 globally 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 5=System Check 6=EPS
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	Administrator who assigned monitor counter to machine
MonitorName	string	Name of monitor SNMP Get object
LogType		1 -> Application Log 2 -> Security Log 3 -> System Log
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
SNMPCustomerName	string	Custom name for SNMP Device
SystemCheckParam1	string	First parameter used in system check
SystemCheckParam2	string	(Optional) Second parameter used by system check
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 globally unique identifier for a machine ID.group ID account and its corresponding agent.
MonitorAlarmID	int	unique monitor alarm number

VSA API Web Service

AlertType	int	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 -> Script failure detected 6 -> NT Event Log error detected 7 -> KServer 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

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.

Machine_GroupID	string	A concatenated representation of the machine id and the group id it is associated with.
agentGuid	decimal	A globally 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)
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)
ChassisType	string	Chassis Type (type 3)
ChassisVersion	string	Chassis Ver (type 3)
MotherboardManufacturer	string	Motherboard Manufacturer (type 2)
MotherboardProductCode	string	Motherboard Product Code (type 2)

VSA API Web Service

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 Kserver 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 95, 98, 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 kserver connection
secondaryKServer	string	address:port agent connects to for its secondary kserver connection
quickCheckinSecs	int	the time to wait, in secs, before performing another agent quick check-in
agentTempDir	string	The temp 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 diskRemovable = floppy or other removable mediaCDROMNetwork = 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.

GetNotesList

Returns an array of new ticket notes added since last request.

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.

GetMachineList

Returns an array of all the machines that the authenticated administrator 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 globally 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.

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.

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.

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 globally 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

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 globally 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.

LockFunctionAccess

Locks function access of the submitted administrator role to the submitted base administrator 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.

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
PrimitiveAuthenticate	PrimitiveAuthenticateResult	string
PrimitiveCloseAlarm	PrimitiveCloseAlarmResult	string
PrimitiveDeleteMachineGroup	PrimitiveDeleteMachineGroupResult	string
PrimitiveGetAlarmList	PrimitiveGetAlarmResult	string
PrimitiveGetLogEntry	PrimitiveGetLogEntryResult	string
PrimitiveGetMachine	PrimitiveGetMachineResult	string
PrimitiveGetMachineCollectionList	PrimitiveGetMachineCollectionListResult	string
PrimitiveGetMachineGroupList	PrimitiveGetMachineGroupListResult	string
PrimitiveGetMachineList	PrimitiveGetMachineListResult	string
PrimitiveGetNotesList	PrimitiveGetNotesListResult	string
PrimitiveGetTicket	PrimitiveGetTicketResult	string
PrimitiveGetTicketList	PrimitiveGetTicketListResult	string
PrimitiveGetTicketNotes	PrimitiveGetTicketNotesResult	string
PrimitiveUpdateTicket	PrimitiveUpdateTicketResult	string

RoleMembership

Assigns an administrator to an administrator 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 an administrator.

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 administrator.

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.

UpdateTicket

Updates one or more fields of a ticket. Only fields listed on the Ticketing > [Email Reader](#) (page 208) 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 administrators are aware of this integration constraint before changes are made to Email Reader 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	Email Phone
Current Tier	List	Manually Entered Web Site
Resolution	List	< Edit List > <not resolved>

Update New

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.

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.

VSA API Web Service

Ticket Attachments

The VSA 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 KServer. API developers are responsible for writing code to place attachment files in this directory before making Web Service API calls that reference these attachments.

Glossary of Terms

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. e-mail) and users (user accounts and groups). The AD provides information on the objects, organizes the objects, controls access and sets security.

The VSA can reference information stored in Active Directory during a [LAN Watch](#) (page 476). Subsequently, agents can be automatically installed on machines using [View AD Computers](#) (page 354). Using [View AD Users](#) (page 355), agents can be automatically installed on each machine a AD user logs onto. Also the latest user contact information can be extracted from Active Directory and applied to the machine ID an AD user is currently logged onto. This provides VSA administrators with up-to-date contact information automatically.

Administrator Roles

[Administrators](#) (page 469) can belong to none, one, or more administrator roles. If an administrator is assigned to multiple roles, and any one of those assigned roles provides access to a function, then the administrator has access to that function. The following policies are assigned by administrator role:

- Access to machine group IDs using System > [Group Access](#) (page 385)
- Access to VSA modules and functions using System > [Function Access](#) (page 387)
- Access to the entire VSA by weekday and hour using System > [Logon Hours](#) (page 388)
- Remote control user notification using Remote Control > [Admin Role Policy](#) (page 274)

In addition, scripts and agent installation packages can be shared by administrator role. Standard administrators can only see other administrators who are members of the same roles.

Administrators

Administrators use the VSA application to maintain the KServer and oversee the monitoring of [managed machines](#) (page 477) by the KServer and its [agents](#) (page 470). KServer management configuration and other [specialized functions](#) (page 387) can only be performed by [master administrators](#). [Standard administrators](#) are typically restricted to the administration and monitoring of managed machines. A background of two alternating shades of *beige* designates master administrators. A background of two alternating shades of *grey* designates standard administrators. Access to functions, machine groups and other policies are assigned by [administrator role](#) (page 469). Standard administrators can only see other administrators who are members of the same roles.

Agent Menu

The set of options that display when the user right-clicks the [agent](#) (page 470) icon  in the [system tray](#) (on page 483) of the managed machine. The agent menu can be [customized](#) (page 361).

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 371)
- [Agent Menu](#) (page 361)

Glossary of Terms

- [Check-in Control](#) (page 363)
- [Temp Directory](#) (page 366)
- [Logs](#) (page 328)
- [User Profile](#) - Refers to settings in Audit > [Edit Profile](#) (page 210) or Ticketing > [User Profiles](#) (page 210).
- [View Collections](#)
- [User Access](#) (page 212)
- [Remote Control Policy](#) (page 269)
- [Patch Settings](#) (page 478)
- [Patch File Source](#) (page 248)
- [Patch Policy Memberships](#) (page 236)
- [Fixed Alerts](#) (page 100) - These all the alert types on the Monitor > [Alerts](#) (page 100) page except for Event Log alerts and System alerts.
- [Event Log Alerts](#) (page 100)
- [Monitor Sets](#) (page 140)
- [Distribute Files](#) (page 60)
- [Protection](#)
- [Script Schedules](#) (page 61)

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 in for it to function and it does not require a reboot for it 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 IT administrator. Once installed:

- A K icon  displays in the icon tray of the remote machine. This can be a custom image or removed altogether.
- Each installed agent is assigned a unique VSA [machine ID / group ID](#) (page 476). 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 licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > [Deploy Agents](#) (page 331) inside the VSA.

Agents - Macintosh

Agents can be installed on Mac OS X version 10.3.9 and up. Both Intel and PowerPC platforms are supported. For Macintosh machines, the VSA supports:

- Hardware & Software Audit
- Scripts
- Remote Control via K-VNC
- FTP
- Reset Password
- Task Manager

See [Deploying Macintosh Agents using Apple Remote Desktop](#) (page 337).

Alarm

In graphical displays throughout the VSA, when an [alarm condition](#) (page 471) exists, the VSA displays, by default, a red traffic light  icon. If no alarm condition exists, a green traffic light icon  displays. These icons can be customized.

Alarms, and [other types of responses](#) (page 472), are enabled using the following pages:

- Monitor > [Alerts](#) (page 100)
- Monitor > [Assign Monitoring](#) (page 147)

- Monitor > [Assign SNMP](#) (page 168)
- Monitor > [System Checks](#) (page 154)
- Monitor > [Parser Summary](#) (page 179)
- Monitor > [Assign Parser Sets](#) (page 187)
- Patch Mgmt > [Patch Alerts](#) (page 250)
- Remote Cntl > Offsite Alerts
- Backup > Backup Alerts
- Security > Apply Alarm Sets
- Agent > [LAN Watch](#) (page 348)

Alarm Condition

An alarm condition exists when a machine's performance succeeds or fails to meet a pre-defined criteria.

Alarms - Suspending

The [Suspend Alarms](#) page suppresses [alarms](#) (page 470) 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 [alarm conditions](#) (page 471). This differs from an [audit](#) (page 472), 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 alarm condition:

- Create [Alarm](#)
- Create [Ticket](#)
- Run [Script](#)
- [Email Recipients](#)

Defining an alert sets the [ATSE response code](#) (page 472) for that machine ID or SNMP device.

Alerts are defined using:

- Monitor > [Alerts](#) (page 100)
- Monitor > [Assign Monitoring](#) (page 147)
- Monitor > [Assign SNMP](#) (page 168)
- Monitor > [System Checks](#) (page 154)
- Monitor > [Parser Summary](#) (page 179)
- Monitor > [Assign Parser Sets](#) (page 187)
- Patch Mgmt > [Patch Alerts](#) (page 250)
- Remote Cntl > Offsite Alerts
- Backup > Backup Alerts
- Security > Apply Alarm Sets
- Agent > [LAN Watch](#) (page 348)

Specific Alerts

The [Alerts](#) page enables you to quickly define alerts for typical [alarm conditions](#) (page 471) found in an IT environment. For example, low disk space is frequently a problem on managed machines. Selecting the [Low Disk](#) type of alarm displays a single additional field that lets you define the % free space threshold. Once defined, you can apply this alarm immediately to any machine ID displayed on the [Alerts](#) page and specify the response to the alarm.

Glossary of Terms

ATSE Response Code

[Creating an alarm](#) represents one of three ways to notify administrators of an alarm condition. The other two ways are to [send an email](#) or to [create a ticket](#). In addition, alarm conditions can [run a script](#) to automatically respond to the alarm condition. These four types of response are called the [ATSE response code](#). Whether assigned to a machine ID, a group ID, or an SNMP device, the designation indicates which types of responses are active for the alarm condition defined.

- A = Create [Alarm](#)
- T = Create [Ticket](#)
- S = Run [Script](#)
- E = [Email Recipients](#)

None of the ATSE responses are required. The alarm condition and the ATSE responses, including no response, is reported to the Reports > [Monitor](#) (page 314) > Monitor Action Log.

The same ATSE design applies to all methods of monitoring provided by the VSA.

Audit

[Agents](#) (page 470) 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 KServer 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 [Reports](#) (page 286) are based on the latest audit. The [Machine Changes](#) report compares a machine ID's latest audit to a baseline audit. Two [alert](#) (page 100) 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](#).

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 KServer primarily to provide immediate technical support. Administrator's can chat with users of managed machines and/or chat with other administrators currently logged on the same Kserver. Administrators can enable or disable the user's ability to initiate chat sessions with administrators. Since Kaseya chats are relayed through the KServer, 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:

-  Agent has checked in
-  Agent has checked in and user is logged on. Tool tip lists the logon name.
-  Agent is currently offline
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is 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 KServer. These tasks can include processing a script, posting cached log data, or refreshing the agent configuration file. A full checkin 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 KServer that the machine ID 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 380).

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 administrator is authorized to have access to those groups. This enables the administrator 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 18). 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.

Copy Settings and Templates

[Machine ID templates](#) (page 477) 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.

Credential

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. See Agent > [Set Credentials](#) (page 371).

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 477). Navigation: Home > [View Dashboard](#) (page 28).

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 477). Navigation: Home >

Glossary of Terms

[Dashboard List](#) (page 88) 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 473). 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 script execution. Use it in conjunction with recurring scripts 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 KServer database, serve as the basis of alerts and reports, and be archived.

Depending on the operating system, the [event logs types](#) available include but are not limited to:

- Application log
- Security log
- System log
- Directory service log
- File Replication service log
- DNS server log

The list of event types available to select can be updated using Monitoring > [Update Lists by Scan](#) (page 140).

Windows events are further classified by the following [event log categories](#):

- Error
- Warning
- Information
- Success Audit
- Failure Audit
- Critical - Applies only to Vista.
- Verbose - Applies only to Vista.

Event logs are used or referenced by the following VSA pages:

- Monitor > [Agent Logs](#) (page 327)
- Monitor > Alerts > [Event Logs](#) (page 115)
- Monitor > Alerts > [Edit Event Sets](#) (page 120)
- Monitor > [Update Lists by Scan](#) (page 140)
- Agent > [Log History](#) (page 328)
- Agent > [Event Log Settings](#) (page 329)
- Agent > [Agent Logs](#) (page 327)
- Reports > [Logs](#) (page 476)
- System > Database Views > [vNtEventLog](#) (page 431)

Events Sets

Because the number of events in Windows based events logs is enormous the VSA uses a record type called an [event set](#) to filter the triggering of alerts.

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 474) 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 triggers an alert on any machine that event set is applied to.

For details on how to configure event sets, see Monitor > Alerts > Event Logs > [Edit Event Sets](#) (page 120).

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 administrator's 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 KServer 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 KServer, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.

Flood Detection

If 1000 events—not counting [black list events](#) (page 475)—are uploaded to the KServer 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 log to record that collection has been suspended. 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 KServer. 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

Alert, system check, and log monitoring alarms are automatically assigned to a [group alarm](#) category. If an alert alarm is triggered, 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 93) dashlet of the Monitor > [Dashboard List](#) page. You can create new groups using the Group Alarm Column Names tab in Monitor > [Monitor Lists](#) (page 138).

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. Host names are only available from computers. Hubs, switches, routers, or other network appliances do not return a host name.

Hotfix

Kaseya frequently posts hotfixes to correct small problems in the latest release. If the [Enable automatic check](#) box is checked in System > [Configure](#) (page 394), your VSA periodically checks for *new only* hotfixes at <http://vsupdate.kaseya.net>. If any new hotfixes are available, the KServer automatically downloads and applies the hotfixes without any user interaction.

The hotfix mechanism addresses minor issues only, typically either cosmetic typos, or ASP page errors. The KServer, agents, or database schema are never updated via hotfixes. Any changes affecting system operation go into full product updates that you approve before installing. Hotfixes just correct minor issues without having to wait for the release cycle.

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

Glossary of Terms

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 uses an existing [agent](#) (page 470) on a managed machine to periodically scan the 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 or [SNMP devices](#) (page 481). Optionally, the VSA can send an [alert](#) (page 471) 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 476). [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 483) files created for Unix, Linux, and Macintosh operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the KServer database, Log Monitoring uses a [parser definitions and parser sets](#) (page 478) 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 the [Machine Summary](#) (page 21) page or by generating a report using the Agent > [Logs](#) (page 309) page. Administrators can optionally trigger alerts when a Log Monitoring record is generated, as defined using [Assign Parsing Sets](#) (page 187) or [Parser Summary](#) (page 179).

Logs

Logs collect event information about multiple systems, including the KServer. The different types of logs that can be generated are:

- [Alarm Log](#) - List out all triggered alarms issued against the selected machine.
- [Admin Notes](#) - Lists administrator notes, sorted by administrator.
- [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.
- [Configuration Changes](#) - Shows a log of changes made by a master or standard administrator to an managed machine's agent configuration.
- [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.
- [Event Logs](#) - Shows the [event log](#) (page 474) data collected by Windows. (Not available with Win9x)
- [Remote Control Log](#) - Lists successful remote controls sessions.
- [Script Log](#) - Shows a list of scripts executed on the selected agent machine. The date and time of each script execution is also noted, as well as whether it completed successfully or not.

Note: [Log Monitoring](#) (page 476) enables you to monitor the data generated by any text-based log.

MAC address

The unique [media access control \(MAC\)](#) identifier assigned to network adapter cards (NICs).

Machine ID / Group ID

Each [agent](#) (page 470) installed on a managed machine is assigned a unique machine ID/group ID name. All machine IDs are associated with a group ID and optionally a subgroup ID. Typically a group ID represents a single customer account. Subgroup IDs typically represent a location or network within a group ID. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.acme.chicago`. In this case `chicago` is a subgroup ID defined within the group ID called `acme`. Only a master administrator, or administrators authorized by a [master administrator](#) (page 469), can create group IDs. Any administrator can create subgroup IDs. Group IDs

and subgroup IDs are created using the System > Machine Groups > [Create/Delete](#) (page 379) page.

Machine ID / Group ID filter

The Machine ID / Group ID filter is available on all tabs and functions. It allows you to limit the machines displayed on *all* function pages. The [View Definitions](#) window lets you further refine a Machine ID / Group ID filter based on attributes contained on each machine—for example, the

operating system type. Once filter parameters are specified, click the green arrow icon  to apply filter settings to *all* function pages. By default, the Machine ID / Group ID filter displays all machine IDs in <All Groups> managed by the currently logged in administrator.

Note: Even if an administrator selects <All Groups>, only groups the administrator is granted access to using System > Group Access (page 385) 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 copied from a selected machine ID template. Typically machine ID templates are 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 341).
- Import a machine ID template using Agent > [Import/Export](#) (page 360). Sample templates can be downloaded from the Kaseya Support Forum and imported.
- Base an agent install package on machine ID template using Agent > [Deploy Agents](#) (page 331).
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > [Copy Settings](#) (page 358).
- Identify the total number of machine ID template accounts in your VSA using System > [Statistics](#) (page 401).
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the [machine ID / group ID](#) (page 476) and the [agent](#) (page 470). The machine ID / group ID is the VSA's [user account name](#) for a managed machine in its 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 machine ID / group ID account name on the VSA. Tasks assigned to a machine ID by a VSA administrator direct the agent's actions on the managed machine.

Managed Machine

A monitored machine with an installed [agent](#) (page 470) and active [machine ID/group ID](#) (page 477) account on the KServer. Each managed machine uses up one [agent license](#) (page 399).

Migrating the KServer

For the latest instructions on migrating an existing KServer to a new machine see the article [How do I move my Kaseya Server to a new computer? \(270436\)](#) in the [Kaseya Support Knowledge Base Portal](#).

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, 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

Glossary of Terms

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 by source machine ID using Monitor > [Update Lists by Scan](#) (page 140).
2. Optionally update monitor set counter objects, instances and counters manually and review them using [Monitor Lists](#) (page 138).
3. Optionally update predefined *sample* monitor sets using System > [Configure](#) (page 394).
4. Create and maintain monitor sets using Monitor > [Monitor Sets](#) (page 140).
5. Assign monitor sets to machine IDs using Monitor > [Assign Monitoring](#) (page 147).
6. Optionally customize standard monitor sets as *individualized monitor sets*.
7. Optionally customize standard monitor sets using *Auto Learn*.
8. Review monitor set results using:
 - Monitor > [Live Connect](#) (page 99)
 - Monitor > [Monitor Log](#) (page 153)
 - Monitor > Dashboard > [Network Status](#) (page 92)
 - Monitor > Dashboard > [Group Alarm Status](#) (page 93)
 - Monitor > Dashboard > [Monitoring Set Status](#) (page 93)
 - Reports > [Monitor](#) (page 314) > Monitor Set Report
 - Reports > [Monitor](#) (page 314) > Monitor Action Log

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 scripts to any managed machine. Distribute a package any way you choose. You can email it, or store it on a server where a [custom script](#) (page 63) can perform a silent installation on any managed machine.

Parser Definitions and Parser Sets

When configuring [Log Monitoring](#) (page 476) 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, and
- Populate parameters with log data values.

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 KServer 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 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 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](#) (page 224) and [Automatic Update](#) (page 227) require patches be approved before these patches are installed.
- [Approval by Policy](#) (page 238) approves or denies patch by *policy*.
- [Approval by Patch](#) (page 240) approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- [KB Override](#) (page 242) 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](#) (page 231) and [Machine Update](#) (page 229) can install denied patches.
- Standard administrators can only see patch policies they have created or patch policies that have machine IDs the administrator is authorized to see based on the administrator roles they are assigned.

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 upgrade, 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, 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.

Primary Domain Controller

Primary domain controllers have full access to the accounts databases stored on their machines.

Glossary of Terms

Only primary domain controllers run [Active Directory](#) (page 469).

Private, Shared or Public

Administrators can define many types of records within the VSA, then decide whether these records are [private](#), [shared](#) or [public](#). These types of records include scripts, reports, files, [managed variables](#) (page 484), and [log file parser definitions](#) (page 184). Private is the default and means only a single administrator has access to the record. Shared means selected administrators or administrator roles have access to the record. When a record is public, all administrators have access to the record. In some cases an administrator must "take ownership" of a public record to edit the record.

PSEXEC.EXE

PSEXEC.EXE is a light-weight telnet-replacement that lets you execute processes on other systems without having to manually install client software. It used by Agent > [Install Agents](#) (page 351) to install agents *on remote systems* after a [LAN Watch](#) (page 476).

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 93), then clicking the [Quick Status](#) link or the Quick Status icon .

Sample Templates

The easiest method of assigning monitoring sets and event sets to machine IDs is to use the sample [templates](#) (page 477) provided by Kaseya. Each sample template is an XML file defined for a certain type of machine, for example, `Windows Server Basic.xml` and `Workstation XP.xml`. Each sample template contains references to the appropriate set of sample monitor sets, sample event sets and sample scripts for that type of machine. These sample monitor sets, sample event sets and sample scripts, are loaded and updated automatically when you install the VSA, if enabled using System > Configure. Sample templates can be downloaded from the Kaseya Support Forum. Use [Copy Settings](#) to assign a set of sample monitor sets, sample event sets and sample scripts from a sample template to machine IDs.

To update monitoring of machine IDs using sample templates:

1. Ensure sample monitor sets, sample events and sample scripts are enabled using System > [Configure](#) (page 394).
2. Import the sample template using Agent > [Import/Export](#) (page 360).
3. Copy monitor set assignments and event log alert assignments from the template to selected machine IDs using Agent > [Copy Settings](#) (page 358).
 - Set [Monitor Sets](#) and [Event Log Alert](#) options to [Add](#). This adds the assignments to selected machine IDs without removing any existing assignments.
 - Set all other [Copy Settings](#) options to [Do Not Copy](#) unless you have a specific reason for copying them.
4. Review sample monitor set assignments on target machine IDs using Monitor > [Assign Monitoring](#) (page 147).
5. Review sample event log alert assignments on target machine IDs using Monitor > Alerts > [Event Logs](#) (page 115).

To customize monitoring using templates:

- If you create a customized monitor set, or event set or script, you can apply it to a new or imported template, then perform the same procedure above, starting with step 3.

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, administrators can use [Packager](#) ([page 478](#)) to create a custom installation package. See [Creating Silent Installs](#) ([page 57](#)).

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 470](#)). 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 \(SNMP\)](#). Read/write instructions are communicated using a set of object variables. Collectively, the set of object variables made available by a device is called its [Management Information Base](#) or [MIB](#). The objects within a MIB are therefore referred to as [MIB objects](#).

Vendors typically provide a specific data file for each device called a [MIB file](#). MIB files are used by monitoring systems such as the VSA to identify the MIB objects available on a device and the typical read or write values for each MIB object. The MIB file includes the "friendly name" associated with an object's ID number or [OID number](#), enabling you to easily identify the object in SNMP sets.

SNMP Quick Sets

The [SNMP Info](#) link page displays a list of SNMP objects provided by the specific SNMP device you selected. These objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a [LAN Watch](#) ([page 165](#)) is performed. You can subsequently define device-specific SNMP sets called [quick sets](#) and associate alerts with these quick sets. Quick sets can be *individualized* for a single device. The *standard* version of the quick set can be shared with other administrators and applied to similar devices throughout the VSA. The prefix (QS) is used to distinguish quick set names from other kinds of SNMP sets.

1. Discover SNMP devices using Monitor > [LAN Watch](#) ([page 165](#)).
2. Assign SNMP sets to discovered devices using Monitor > [Assign SNMP](#) ([page 168](#)).
3. Click the [SNMP info](#) ([page 172](#)) link in the [Assign SNMP](#) page to display a list of SNMP objects that apply to the specific SNMP device you selected.
4. Display SNMP alarms using Monitor > [SNMP Log](#) ([page 175](#)) or [Dashboard List](#) ([page 88](#)).

SNMP Sets

A SNMP set is a set of MIB objects used to monitor the performance of [SNMP enabled network devices](#) ([page 481](#)). 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 an device-specific SNMP set based on the objects discovered on that device during a LAN Watch. [SNMP quick sets](#) ([page 481](#)) 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.

Glossary of Terms

- **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 482) determined during a LAN Watch.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Monitor > **LAN Watch** (page 165).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** (page 168). This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** (page 175) or **Dashboard List** (page 88).

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 138).
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** (page 158).
- Optionally add an SNMP object using Monitor > **Add SNMP Object** (page 163).
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **SNMP Type** (page 178).
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** (page 177).

SNMP Types

You can assign **SNMP sets** (page 481) to **devices** (page 481) *by type* automatically as follows:

1. Add or edit SNMP types using the **SNMP Device** tab in Monitor > **Monitor Lists** (page 138).
2. Add or edit the `sysServicesNumber` associated with SNMP types using the **SNMP Services** tab in Monitor > Monitor Lists. Broad categories of SNMP devices share the same `sysServiceNumber`.
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 159).
4. Perform a **LAN Watch** (page 165). During a LAN Watch 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.
5. Manually assign a SNMP type to an SNMP device using Monitor > **SNMP Type** (page 178). Doing so causes SNMP sets using that same type to start monitoring the SNMP device.

Synthetic Backups

A synthetic full backup is created by consolidating existing incremental or differential backups with the previous full backup image. This is sometimes called an 'Incremental Forever Backup'. Unlike traditional full backups, synthetic full backups are not transferred from the local server to the offsite server. Instead, after the *first* full backup is transferred, only the incremental or differential files are transferred to the offsite server. A synthetic backup component on the offsite server recreates the next full synthetic backup in parallel with the local server. This eliminates the need to transfer full backups between the local server and offsite server. With synthetic backups, bandwidth requirements for transferring full backups are eliminated, but the offsite server's access to its own file server may need to be enhanced to handle the processing of its synthetic backups.

Configuring synthetic backups involves the following steps:

Note: The first three steps are required even if synthetic backups are not enabled on the offsite server.

1. Install an agent on a local server. Typically the backup image locations of machine IDs being backed up point to the local server.
2. Install an agent on the offsite server.
3. Define a machine ID as an offsite server using Backup > Offsite Servers.

Note: You do not have to install the backup client to a local server or an offsite server.

4. Click the [Schedule Install](#) hyperlink on the Backup > [Offsite Servers](#) page for the machine ID you want to schedule synthetic support on. A dialog box displays. Schedule the installation of synthetic support components to the offsite server.
5. Schedule volume backups for machine IDs, ensure the [Synthetic Full](#) checkbox is checked. These are machine IDs that store backups on local servers that transfer backups to the offsite server you defined above.

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 Macintosh operating systems and hardware devices such as Cisco routers. [Log Monitoring](#) (page 476) 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 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 Scripts

System scripts are basic functions that are exposed by the VSA. You can schedule system scripts to run automatically. They cannot be edited nor can they accept parameters. A list of available system scripts displays in any Script Search popup window. System scripts can be run from:

- Within a parent script using the [Execute Script](#) or [Schedule Script](#) commands of an [IF-THEN-ELSE](#) (page 72) statement.
- Any alerts page using the [Run Script](#) checkbox.
- The [Pending Scripts](#) tab of the [Machine Summary](#) (page 21) page.

Because a system script can be run using an alert or parent script associated with a specific machine ID account, the scheduling of a system script can be copied, typically from a machine ID template to a machine using Agent > [Copy Settings](#) (page 358).

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.

Update Classification

Microsoft updates are organized as follows:

Update Classification	Classification Type (Non-Vista / Vista)	Included in WSUSSCN2.CAB*
Security Updates	High Priority / Important Includes critical, important, moderate, low, and non-rated security updates.	Yes
Critical Updates	High Priority / Important	Yes

Glossary of Terms

Update Rollups	High Priority / Important	Yes
Service Packs	Optional – Software / Recommended	Yes
Updates	Optional – Software / Recommended	No
Feature Packs	Optional – Software / Recommended	No
Tools	Optional – Software / Recommended	No

In those cases where a machine does not have Internet connectivity at the time of a machine patch scan, Kaseya uses Microsoft's WSUSSCN2.CAB data file. Microsoft publishes this CAB file as needed. It contains a sub-set of the Microsoft Update Catalog. As seen in the table above, scan data for only the high priority updates and service packs are included in the CAB file. The KServer automatically downloads the CAB file on a daily basis to make it available for those machines needing this type of scan. See [Windows Automatic Update](#) (page 486).

URL to Display "Create/View" Page

The following URL displays the [Create/View](#) (page 197) web page for a specific ticket ID

Error! Hyperlink reference not valid.>

For example:

<http://demo.kaseya.com?ticaid=1234>

URL to Display Machine Summary Page

The following URL displays the [Machine Summary](#) (page 21) web page for a specific machine ID:

`http://...?machName=<MachineID>`

For example:

<http://demo.kaseya.com?machName=jconners.acme>

User Access Welcome Page

The [User Access Welcome Page](#) is the page the user sees when the agent icon  on the system tray of a managed machine is double-clicked. The User Access Welcome Page contains user options such as changing the user's contact information, creating or tracking trouble tickets, chatting with administrators or remote controlling their own machine from another machine. Some of these options are enabled by an administrator using Agent > [User Access](#) (page 212). The function list the user sees on the User Access Welcome Page can be customized using System > [Customize](#) (page 403).

User Account

See [Machine IDs vs. Agents](#) (page 477)

Variables

Use variables to store values that can be referenced in multiple script steps. Variables are passed automatically to nested scripts.

- [Two Methods for Creating Variables](#):
 - [Script Variables](#) - Use the [Get Variable](#) command within a script to create a new variable name without any special characters. Example: `VariableName`. In subsequent steps, including steps in nested scripts, reference the variable by bracketing the variable name with the # character. Example: `#VariableName#`. Scripts variables cannot be referenced outside of the script or nested scripts that use them.
 - [Managed Variables](#) - Use the [Variable Manager](#) (page 70) to define variables that can be used repeatedly in different scripts. 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 script. Within a script, reference a managed variable by bracketing the variable name with the < and > character. Example: `<VariableName>`.
- [Where Used](#) - Once variables are created you can include them, in their bracketed format, *in any text entry field* displayed by an IF-THEN-ELSE 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 script runtime as `c:\dir > filelist.txt`.
- **Types of Variable Values Possible** - The following are the types of variable values typically obtained by using the **Get Variable** parameter.
 - **Registry Value** - Data from the specified registry value on the managed machine.
 - **File Content** - Data from a specified file on the managed machine.
 - **Constant Value** - Specified constant as typed in the script editor.
 - **Expression Value** - Specify an expression that consists of script variables and six mathematical operators +, -, *, /, (, and) that are evaluated and assigned to a new script variable. For example, $((\#variable1\# + \#variable2\#) + 17.4) / (\#variable3\# * 4)$. The script variables must contain numeric values.
 - **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 Temp Directory Path** - Temporary directory on the managed machine as specified on the **Temp Directory** function on the agent tab.
 - **User Temp Directory Path** - The temporary directory for the user currently logged in on the managed machine. This path is the expansion of the `%TEMP%` environment variable for the currently logged in user. If no user is logged in, it is the default Windows temporary directory.
 - **Machine.Group ID** - Machine ID of the agent executing the script.
 - **File Version Number** - Version number from the property of the specified file on the managed machine.
 - **File Size** - Size in bytes of the specified file on the managed machine.
 - **File Last Modified Date** - Date of the specified file on the managed machine in the format of `yyyy/mm/dd hh:mm:ss`.
 - **SQL View Data** - Use the **GetVariable** command with the **SQL View Data** option to create a new script 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 script is retrieved. If `ColumnName` contains a space, surround it with square brackets. Example: `vSystemInfo/[Product Name]`. See **System > Database Views** (*page 410*) for a list of the SQL views and columns that are available.

Note: - Automatic SQL View Data Variables - SQL view parameters are available as automatically declared script variables. Automatic variables enable you to skip using the **GetVariable** command with the **SQL View Data** option. Use the format `#SqlViewName.ColumnName#` in a script to return the value of a `dbo.SqlView.Column` for the agent executing the script.

- **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`.

View Definitions

The **View Definitions** (*page 18*) 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 administrators flexibility for machine management and reporting. View filtering is applied to *all*

Glossary of Terms

function pages by selecting a view from the [Select View](#) drop-down list on the [Machine ID / Group ID Filter](#) (page 17) panel and clicking the green arrow  icon. Any number of views can be created and shared with other administrators. 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 KServer 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 target machine that shares its screen. The [VNC client \(or viewer\)](#) is the program on the administrator's machine that watches and interacts with the target machine. The VNC client machine requires user access rights to the VNC server machine. Since Kaseya VNC sessions are relayed through the KServer, 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 476), 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, and Windows 2000 SP3 or later. While Windows Millennium Edition (Me) has an Automatic Updates capability, it cannot be managed as the above operating systems can. Patch Mgmt > [Windows Auto Update](#) (page 243) can enable or disable this feature on managed machines.

Index

A

Access Policy • 204
 Active Directory • 469
 Add SNMP Object • 163
 Add/Remove • 37
 Admin Group Access • 453
 Admin History • 393
 Admin Role Policy • 274
 Administrator Notes • 24
 Administrator Roles • 469
 Administrators • 469
 Advanced Filtering • 295
 Agent • 323
 Agent Icons • 11
 Agent Install Command Line Switches • 335
 Agent Logs • 327
 Agent Menu • 361, 469
 Agent Settings • 469
 Agent Status • 325
 Agent Tab • 324
 Agents • 10, 470
 Agents - Macintosh • 470
 Aggregate Table • 294
 Alarm • 470
 Alarm Condition • 471
 Alarm Network Status • 90
 Alarm Rotator • 92
 Alarm Summary • 90, 96
 Alarm Summary Window • 90
 Alarm Ticker • 92
 Alarms • 86
 Alarms - Suspending • 471
 Alert • 471
 Alerts • 100
 Alerts - Agent Status • 103
 Alerts - Application Changes • 106
 Alerts - Backup Alert • 133
 Alerts - Event Logs • 115
 Alerts - Get Files • 108
 Alerts - Hardware Changes • 110
 Alerts - LAN Watch • 121
 Alerts - Low Disk • 113
 Alerts - New Agent Installed • 128
 Alerts - Patch Alert • 130
 Alerts - Protection Violation • 126
 Alerts - Script Failure • 124
 Alerts - Summary • 101
 Alerts - System • 136
 API • 443
 Application Blocker • 50

Application Deploy • 56
 Approval by Patch • 240
 Approval by Policy • 238
 Assign Monitoring • 147
 Assign Parser Sets • 187
 Assign SNMP • 168
 Assignee Policy • 205
 ATSE Response Code • 472
 Audit • 31, 472
 Audit Tab • 32
 Authenticate • 453
 Auto Learn - Monitor Sets • 152
 Auto Learn - SNMP Sets • 174
 Auto Learn Monitor Sets • 472
 Automatic Update • 227

B

Backup • 312
 Backup Sets • 472

C

Cancel Script • 21
 Cancel Updates • 234
 Canonical Name • 472
 Change Group • 347
 Chat • 279, 472
 Check-in
 Full vs. Quick • 473
 Check-In Control • 363
 Check-in Policy • 382
 Check-in Status • 473
 CloseAlarm • 453
 Collection • 473
 Command Line • 256
 Configuration • 9
 Configure • 394
 Configuring Patch Management • 217
 Configuring the Server • 10
 Control Machine • 263
 Copy Settings • 358
 Copy Settings and Templates • 473
 Counter Thresholds • 143
 CPU/RAM • 42
 Create • 341
 Create / Delete
 Admin Accounts • 388
 Admin Roles • 383
 Machine Groups • 379
 Create/Delete
 Patch Policy • 235
 Create/View • 197

Index

CreateAdmin • 454
CreateAgentInstallPackage • 454
CreateMachineGroup • 454
CreateRole • 454
Creating Custom Agent Icons • 407
Creating Silent Installs • 57
Credential • 473
Crystal Reporting Usage • 411
Customize • 403

D

Dashboard • 473
Dashboard List • 88, 473
Database Views • 409, 410
Define Monitor Sets • 142
Define SNMP Set • 159
Define SNMP Set Details • 161
Delete • 344
Delete/Archive • 200
DeleteAdmin • 455
DeleteAgent • 455
DeleteMachineGroup • 455
DeleteRole • 455
Deploy Agents • 331
Deploying Macintosh Agents using Apple Remote Desktop • 337
Device Status • 95
DisableAdmin • 455
Disk Utilization • 305
Disk Volumes • 40
Distribute File • 60, 474
Distribution • 62
DNS/DHCP • 39
Documents • 44
Domain Logon • 355, 377
Due Date Policy • 205

E

Echo • 456
Edit Event Sets • 120
Edit Fields • 207
Edit Profile / User Profiles • 210, 367
Email Mapping • 210
Email Reader • 208
Enable / Disable • 390
EnableAdmin • 456
Enabling VSA API Web Service • 444
Event Log Settings • 329
Event Logs • 474
Events Sets • 474
Excel Usage • 411
Executive Summary • 289

F

File Access • 47
File Source • 248
File Transfer Protocol (FTP) • 475
Filter Aggregate Table • 20
Flood Detection • 475
fnMissingPatchCounts_UsePolicy /
fnMissingPatchCounts_NoPolicy • 416

fnOSCounts • 417
FTP • 277
Function Access • 387

G

Get File • 59
GetAlarm • 456
GetAlarmList • 457
GetGroupLicenseInfo • 458
GetLogEntry • 458
GetMachine • 459
GetMachineCollectionList • 462
GetMachineGroupList • 462
GetMachineList • 462
GetNotesList • 462
GetPackageURLs • 463
GetTicket • 463
GetTicketList • 464
GetTicketNotes • 464
Getting Started • 15
Global Event Log Black Lists • 475
Group Access • 385
Group Alarm Status • 93
Group Alarms • 475

H

Home • 27
Home Tab • 28
Host name • 475
Hotfix • 475

I

IF-THEN-ELSE Commands • 72
Import / Export • 360
Initial Update • 224
Install Agents • 351
Install Issues and Failures • 340
Installed Apps • 36
Inventory • 301
IP Info • 38
ISO Image • 475

K

KB Override • 242
KES Status • 95
KES Threats • 96

L

LAN Watch • 165, 348, 476
Layout Dashboard • 29
License Manager • 399
Live Connect • 99
LockFunctionAccess • 465
Log File Parser Definition • 184
Log File Set Definition • 191
Log History • 328
Log Monitoring • 476
Log Parser • 182
Logoff • 25
Logon and Browser Settings • 16

Logon Hours • 388
 Logon Policy • 403
 Logs • 309, 476

M

MAC address • 476
 Machine Changes • 298
 Machine History • 228
 Machine ID / Group ID • 476
 Machine ID / Group ID filter • 477
 Machine ID / Group ID Filter • 17
 Machine ID Template • 477
 Machine IDs vs. Agents • 477
 Machine Policy • 276
 Machine Status • 95
 Machine Summary • 21, 44, 296
 Machine Update • 229
 Machines Online • 95
 Macintosh • 337, 366, 407, 470
 Manage Files Stored on Server • 69
 Managed Machine • 477
 Membership
 Admin Roles • 384
 Patch Policy • 236
 Methods of Updating Patches • 217
 Migrate • 10, 360, 363, 394, 477
 Migrating the KServer • 477
 Minimum System Requirements • 13
 Monitor • 83, 314
 Monitor Icons • 147
 Monitor Lists • 138
 Monitor Log • 153
 Monitor Sets • 140, 477
 Monitor Status • 95
 Monitor Tab • 84
 Monitoring Set Status • 93

N

Name/OS Info • 38
 Naming Policy • 380
 Network Access • 48
 Network Health Score • 291
 Network Statistics • 306
 Network Status • 92
 Notify Policy • 202

O

Office Source • 254
 Operations • 453
 Overview • 443

P

Packager • 58, 478
 Parser Definitions and Parser Sets • 478
 Parser Summary • 179
 Patch Alert • 250
 Patch Deploy • 55
 Patch Failure • 219
 Patch Location • 258
 Patch Management • 215, 299
 Patch Mgmt Tab • 216

Patch Policy • 478
 Patch Processing • 218
 Patch Status • 222
 Patch Update • 231
 Patch Update Order • 479
 PCI & Disk H/W • 41
 Performance Objects, Instances and Counters • 479
 Power Mgmt • 268
 Power Savings • 319
 Pre/Post Script
 Patch Management • 226
 Preferences • 377
 Preinstall RC • 272
 Primary Domain Controller • 479
 Primitives • 465
 Printers • 43
 Private, Shared or Public • 480
 Process Status • 146
 PSEXEC.EXE • 480

Q

Quick Status • 480

R

Reboot Action • 245
 Remote Cntl Tab • 262
 Remote Control • 261
 Rename • 346
 Rename Group • 380
 Reports • 285
 Reports Tab • 286
 Request Support • 394
 Reset Master Admin Password • 393
 Reset Password • 267
 RoleMembership • 465
 Rollback • 234
 Run Audit • 33

S

Sample Templates • 480
 Scan Machine • 221
 Schedule Reports • 287
 Script Browser and Script Toolbar • 63
 Script Editor • 67
 Script Manager • 64
 Script Scheduler • 65
 Script, Cancel • 21
 Scripts • 53
 Scripts Status • 61
 Scripts Tab • 54
 Security • 316
 Select Type • 269
 Send Message • 281
 SendAdminMessage • 466
 Services Check • 145
 Set Credential • 371
 Set Logo • 287
 Set Parameters • 271
 Set Password • 391
 Set SNMP Values • 177
 SetAdminPassword • 466

Index

- SetGroupLicenseInfo • 466
 - Settings • 96
 - Silent Install • 481
 - SNMP Community • 481
 - SNMP Devices • 481
 - SNMP Icons • 164
 - SNMP Log • 175
 - SNMP Quick Sets • 172, 481
 - SNMP Sets • 158, 481
 - SNMP Type • 178
 - SNMP Types • 482
 - Software • 303
 - Special Fields • 444
 - Statistics • 401
 - Status Monitor • 24
 - Superseded Patches • 218
 - Suspend • 360
 - Suspend Alarms • 98
 - SW Licenses • 37
 - Synthetic Backups • 482
 - syslog • 483
 - System • 375
 - System Activity • 293
 - System Check • 154
 - System Checks • 483
 - System Info • 35
 - System Log • 400
 - System Scripts • 483
 - System Security • 12
 - System Tab • 376
 - System Tray • 483
- ### T
- Task Manager • 283
 - Temp Directory • 366
 - Ticketing • 193, 311
 - Ticketing Tab • 194
 - Toolbox • 23
 - Top N - Monitor Alarm Chart • 95
- ### U
- Uninstall RC • 273
 - Update Agent • 372
 - Update Classification • 219, 483
 - Update Lists By Scan • 140
 - UpdateTicket • 466
 - Updating the VSA • 13
 - Uptime History • 308
 - URL to Display • 484
 - URL to Display Machine Summary Page • 484
 - User Access • 212, 369
 - User Access Welcome Page • 484
 - User Account • 484
 - User State • 318
- ### V
- vAdminNotesLog • 417
 - vAgentConfiguration • 418
 - vAgentLabel • 419
 - vAlertLog • 419
 - Variable Manager • 70
 - Variables • 484
 - vBackupLog • 420
 - vBaseApplicationInfo / vCurrApplicationInfo • 421
 - vBaseCpuInfo / vCurrCpuInfo • 421
 - vBaseDiskInfo / vCurrDiskInfo • 422
 - vBaseDriveManufacturer / vCurrDriveManufacturer • 422
 - vBasePciInfo / vCurrPciInfo • 423
 - vBasePrinterInfo / vCurrPrinterInfo • 423
 - vCollectionMember • 424
 - vConfigLog • 424
 - Video Streaming • 265
 - View AD Computers • 354
 - View AD Users • 355
 - View Dashboard • 28
 - View Definitions • 18, 485
 - View LAN • 354
 - View Summary • 194
 - View vPro • 358
 - Views Provided • 415
 - Virtual Machine • 486
 - Virtual Network Computing (VNC) • 486
 - vLicenseInfo • 425
 - vMachine • 425
 - vMonitorAlarmAlert • 427
 - vMonitorAlarmCounter • 428
 - vMonitorAlarmProcess • 428
 - vMonitorAlarmService • 429
 - vMonitorAlarmSNMP • 430
 - vMonitorAlarmSystemCheck • 430
 - vNetStatsLog • 431
 - vNtEventLog • 431
 - vOnBoardDeviceInfo • 432
 - vPatchApprovalStatus • 432
 - vPatchPolicy • 433
 - vPatchPolicyMember • 434
 - vPatchStatus • 434
 - vPortInfo • 436
 - vPro • 486
 - VSA API Web Service • 441
 - VSA API Web Service Sample Client - ASP Page • 446
 - VSA API Web Service Sample Client - C# GUI application • 445
 - VSA API Web Service Security • 449
 - VSA Tabs • 17
 - vScriptLog • 436
 - vScriptStatus • 436
 - vSystemInfo • 437
 - vTicketField • 438
 - vTicketNote • 438
 - vTicketSummary • 438
- ### W
- Web Links - Inbound and Outbound • 451
 - Windows Auto Update • 243
 - Windows Automatic Update • 486