VSA Glossary

User Guide

Version R95

English

July 22, 2019

Copyright Agreement

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

Contents

Glossary

Active Directory

Active Directory is a directory service used to store information about the network resources across a domain. Its main purpose is to provide central authentication and authorization services for Windows based computers. An Active Directory structure is a hierarchical framework of objects. The objects fall into three broad categories: resources (e.g. printers), services (e.g. email) and users (user accounts and groups). The AD provides information on the objects, organizes the objects, controls access and sets security.

The VSA can manage computers, contacts and users by referencing information stored in Active Directory. See Domain Watch in the **Discovery** module for more information.

Agent Menu

The set of options that display when the user right-clicks the **agent** *(page 3)* icon in the **system tray** *(on page 20)* of the managed machine. The agent menu can be customized.

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:

- **Agent Credential** *(page 8)*
- Agent Menu
- Check-in Control
- Working Directory
- Logs
- Machine Profile - Refers to settings in Audit > Edit Profile.
- **View Collections** *(page 8)*
- Portal Access
- Remote Control Policy
- **Patch Settings** *(page 15)*
- Patch File Source
- Patch Policy Memberships
- Fixed Alerts - These all the alert types on the Monitor > Alerts page except for Event Log alerts and System alerts.
- Event Log Alerts
- Monitor Sets
- Distribute Files
- Protection
- Agent Procedure Schedules

Agent Time Scheduling

With **agent time scheduling**, the system clock used by the agent machine determines when that scheduled task occurs. Scheduling the same task for 10 machines all on Tuesday, at 2:00 PM, will occur whenever 2:00 PM on Tuesday, local time, occurs for each machine, as determined each machine's system clock. A global default to use either server time or agent time scheduling is provided using the new System > Server Management > Default Settings page.

Agents

The VSA manages machines by installing a software client called an **agent** on a managed machine. The agent is a system service that does not require the user to be logged on for the agent to function

and does not require a reboot for the agent to be installed. The agent is configurable and can be totally invisible to the user. The sole purpose of the agent is to carry out the tasks requested by the VSA user. Once installed:

- An agent icon—for example the ⬈ agent icon—displays in the system tray of the managed machine. Agent icons can be custom images or removed altogether.
- Each installed agent is assigned a unique VSA **machine ID / group ID / organization ID** *(page 12)*. Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available agent licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > Deploy Agents inside the VSA.
- Multiple agents can be installed on the same machine, each pointing to a different server.
- A check-in icon displays next to each machine ID in the VSA, displaying the overall status of the managed machine. For example, the 🔵 check-in icon indicates an agent is online and the user is currently logged on.
- Clicking a check-in icon displays a single machine interface for the managed machine called Live Connect. **Live Connect** provides instant access to comprehensive data and tools you need to work on that one machine.
- Hovering the cursor over a check-in icon displays an agent Quick View window immediately. You can view agent properties, quick launch selected agent procedures, or launch **Live Connect** from the agent **Quick View** window.

Agents - Apple

Apple agents support the following functions:

- Audits - selected hardware and software attributes
- Agent procedures
- Remote Control
- FTP
- SSH
- Reset Password
- Task Manager
- Live Connect
- Kaseya Remote Control
- Live Connect (Classic)
- Network scan via Discovery

> **Note:** OS X is not currently supported for Probe Machine, but devices running OS X are discovered by the Network Discovery.

- Supported monitoring:
  - ➢ SNMP monitoring
  - ➢ Process monitoring in monitor sets
  - ➢ System Check
  - ➢ Log Parser

See **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/index.asp#home.htm)*.

Agents - Linux

Linux agents support the following functions:

- 'Headless' agent procedures

- Latest audits, baselines audits and system audits
- The SSH page in the legacy Remote Control module
- Selected alerts
- Monitoring of Processes
- Monitoring of SNMP
- Log Parser
- Site Customization - The **Agent Icons** tab includes a set of icons for Linux agents you can customize.

See **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/index.asp#home.htm)*.

Alarms - Suspending

The **Suspend Alarms** page suppresses **alarms** *(page 6)* 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 and will show alarm state in the dashboard, but does not generate assigned alarm actions.*

Alert

Alerts are responses to **alert conditions** *(page 7)*. This differs from an **audit** *(page 7)*, which simply collects selected data for reference purposes without regard to any criteria.

Alerts have two meanings, generic and specific:

Generic Alerts

Typically there are four types of alert responses to an alert condition:

- Create **A**larm
- Create **T**icket
- Run Procedure
- **E**mail Recipients

Defining an alert sets the **ATSE response code** *(page 5)* for that machine ID or SNMP device.

Alerts are defined using:

- Monitor > Alerts
- Monitor >   Assign Monitoring
- Monitor > Assign SNMP
- Monitor > System Checks
- Monitor > Parser Summary
- Monitor > Assign Parser Sets
- Patch Management > Patch Alerts
- Remote Control > Offsite Alerts
- Backup > Backup Alerts
- Security > Apply Alarm Sets
- Discovery > By Network or **By Agent**
  (http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#1944.htm)

Specific Alerts

The **Alerts** page enables you to quickly define alerts for typical **alert conditions** *(page 7)* found in an IT environment.   For example, low disk space is frequently a problem on managed machines. Selecting the `Low Disk` type of alert displays a single additional field that lets you define the `% free space` threshold. Once defined, you can apply this alert immediately to any machine ID displayed on the **Alerts** page and specify actions to take in response to the alert.

Alert Actions

Creating an alarm represents only one *type of action* that can be taken when an alert occurs. Two other types of actions are notifications. They include **send an email** or **create a ticket**. A fourth type of action is to **run an agent procedure** to automatically respond to the alert. These four types of actions are called the **ATSE code**. Whether assigned to a machine ID, a group ID, or an SNMP device, the ATSE code indicates which types of actions will be taken for the alert defined.

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

None of the ATSE actions are required to be set when configuring an alert. Both the alert and the ATSE action, including no action, are reported in the Info Center > Monitor - Monitor Action Log report.

Alert Types

Types of alerts include:

- Discovery > By Network or By Agent
- Backup > Backup Alerts
- Monitor > Alerts - These are specialized "fixed" alerts that are ready to apply to a machine.
- Monitor >   Assign Monitoring
- Monitor > SNMP Traps Alert
- Monitor > Assign SNMP
- Monitor > System Checks
- Monitor > Parser Summary
- Monitor > Assign Parser Sets
- Patch Management > Patch Alerts
- Remote Control > Offsite Alerts
- Security > Apply Alarm Sets

Other add-on modules have alerts not listed here.

Alert Types

Alerts are one of several **monitor types** *(page 14)*.
1 - Admin account disabled
2 - Get File change alert
3 - New Agent checked in for the first time
4 - Application has been installed or deleted
5 - Agent Procedure failure detected
6 - NT Event Log error detected
7 - Kaseya Server stopped
8 - Protection violation detected.
9 - PCI configuration has been changed
10 - Disk drive configuration change
11 - RAM size changed.
12 - Test email sent by serverInfo.asp
13 - Scheduled report completed
14 - Network scan 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

Alerts

An alert is created when the performance of a machine or device matches a pre-defined criteria or "alert condition".

Audit

Agents *(page 3)* can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the Kaseya Server so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per week is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machines's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > Reporting > Reports are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two alert 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 Kaseya Server primarily to provide immediate technical support. VSA users can chat with machine users and/or chat with other VSA users currently logged on the same Kaseya Server. VSA users can enable or disable the machine user's ability to initiate chat sessions with VSA users. Since Kaseya chats are relayed through the Kaseya Server, all chats are protected by 56 bit rolling encryption protocol.

Check-in Status

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

- Online but waiting for first audit to complete
- Agent online

🔵   Agent online and user currently logged on.

🟡   Agent online and user currently logged on, but user not active for 10 minutes

⚫   Agent is currently offline

🔲   Agent has never checked in

🔴   Agent is online but remote control has been disabled

✋   The agent has been suspended

Check-in: Full vs. Quick

A **full check-in** occurs when an agent completes the processing of any and all outstanding tasks assigned to it by the Kaseya Server. These tasks can include processing an agent procedure, posting cached log data, or refreshing the agent configuration file. A full check-in occurs if 24 hours elapses without a specific task requiring it. A **quick check-in** occurs when an account checks in at the configured check-in interval, indicating to the Kaseya Server that the managed machine is still online. This doesn't require the completion of all outstanding tasks. Some functions require a full check-in before an agent can begin processing a new task. For example, System > Naming Policy. You can force a full check-in by right-clicking the agent icon in the system tray of a managed machine and clicking the **Refresh** option.

Collection

Collections are a free-form selection of *individual machine IDs within a view*. It doesn't matter which groups the machine IDs belong to, so long as the VSA user is authorized to have access to those groups. This enables the VSA user to view and report on logical collections of related machine IDs, such as laptops, workstations, servers, MS Exchange Servers, etc. Collections are created using the **Only show selected machine IDs** checkbox in View Definitions. Save a view first before selecting machines IDs using this option. Once the view is saved, a **<N> machines selected** link displays to the right of this option. Click this link to display a **Define Collection** window, which allows you to create a view using a free-form selection of individual machine IDs.

> **Note:** The Filter Aggregate Table provides an alternate method of selecting machine IDs for a view definition, based on standard and user defined attributes.

Copy Settings and Templates

Machine ID templates *(page 13)* are initially used to create an agent install package using the template as the source to copy settings from. But even after agents are installed on managed machines, you'll need to update settings on existing machine ID accounts as your customer requirements change and your knowledge of the VSA grows. In this case use Agent > **Copy Settings** to copy these changes to any number of machines IDs you are authorized to access. Be sure to select `Do Not Copy` for any settings you do not want to overwrite. Use `Add` to copy settings without removing existing settings. Kaseya recommends making changes to a selected template first, then using that template as the source machine ID to copy changes from. This ensures that your machine ID templates remain the "master repositories" of all your agent settings and are ready to serve as the source of agent install packages and existing machine ID accounts.

Credentials

A credential is a username and password used to authenticate a user or process's access to a machine or network or some other resource.

Agent Credentials

The VSA maintains a single *agent credential* with administrator privileges for an agent to use, using the Agent > Manage Agents page.

- Patch Management - If an agent credential is defined for a machine ID, then Patch Management installs all new patches using this agent credential. Therefore, the agent credential should always be a user with administrator rights.

- Patch Status - Patch Status resets test results every time a machine ID's agent credential changes.
- File Source - File Source may require an agent credential be defined for the machine ID acting as the file share.
- Patch Alert - Set up an alert to notify you if a machine ID's agent credential is missing or invalid.
- Office Source - A machine ID must have an agent 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 - The `useCredential()` command in the agent procedure editor requires a an agent credential to run successfully.
- **Backup** > **Image Location** *(http://help.kaseya.com/webhelp/EN/KSD/9050000/index.asp#7948.htm)* - If a UNC path is specified in **Image Location**, an agent credential must be defined to provide access to this UNC path. Without the agent credential, the machine will *not* have access to the image location and the backup will fail. When specifying a UNC path to a share accessed by an agent machine—for example \\machinename\share—ensure the share's permissions allow read/write access using the agent credential.
- View Definitions - Includes a **Machines with Credential status** option that allows you to filter the display of machine IDs on any agent page by their agent credential status.
- Desktop Management - Installing the client for this module requires an agent credential be defined.

Blank Credentials

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.

Managed Credentials

The VSA maintaines *additional* credentials at three different levels: by organization, by machine group and by individual machine or device. They are managed using three navigation items in the **Audit** module:

- View Assets - Use this page to create multiple credentials for an *individual* machine or device.
- Manage Credentials - Use this page to create multiple credentials for *organizations* and *machine groups* within organizations.
- Credential Log - This page logs the creation, display and deletion of managed credentials.

Once created, use managed credentials:

- To instantly lookup all the credentials that apply to a machine you're working on. The Quick View (Classic) popup window includes a **View Credentials** option. Access is controlled by role and by scope. You can add a description for each credential.
- As the *source credential* for an agent credential in a policy. Check the **Use organization defaults** checkbox in the **Credential** setting of the Policy Management > Policies page to establish the link.

> **Note:** A managed credential can not overwrite the agent credential maintained using the Agent > Manage Agents directly. The managed credential must be applied to a policy and the policy applied to the machine.

If multiple credentials are defined for a machine, then the most local level defined has precedence: by individual machine, by machine group, or by organization. At any one level, only one managed credential can be designated the *source credential* for an agent credential for Policy Management

Current VSA Time

The current time used by the Kaseya Server is displayed in System > Preferences.

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 13)*. Navigation: Info Center > View Dashboard.

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 13)*. Navigation: Info Center > Dashboard List 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 8)*. If the file is ever deleted, corrupted, or an updated version is available on the VSA, the VSA sends down a new copy prior to any procedure execution. Use it in conjunction with recurring procedures to run batch commands on managed machines.

Event Logs

An **event log service** runs on Windows operating systems (Not available with Win9x). The event log service enables event log messages to be issued by Window based programs and components. These events are stored in event logs located on each machine. The event logs of managed machines can be stored in the Kaseya Server database, serve as the basis of alerts and reports, and be archived.

Depending on the operating system, the **event log types** available include but are not limited to:

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

Windows events are further classified by the following **event log categories**:

- Error
- Warning
- Information
- Success Audit
- Failure Audit
- Critical - Applies only to Vista, Windows 7 and Windows Server 2008
- Verbose - Applies only to Vista, Windows 7 and Windows Server 2008

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

- Monitor > Agent Logs
- Monitor > Event Log Alerts
- Monitor > Event Log Alerts > Edit Event Sets
- Monitor > Update Lists by Scan
- Agent > Log History
- Agent > Event Log Settings
- Agent > Agent Logs
- Reports > **Logs** *(page 12)*
- Live Connect > Events
- Live Connect (Classic) > Event Viewer
- Quick View (Classic) > Event Viewer

- System > Database Views > vNtEventLog

Events Sets

Because the number of events in Windows **events logs** *(page 10)* is enormous the VSA uses a record type called an **event set** to filter an alert condition. Event sets contain one or more **conditions**. Each condition contains filters for different fields in an **event log entry**. The fields are **source**, **category**, **event ID**, **user**, and **description**. An **event log** *(page 10)* entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to. For details on how to configure event sets, see Monitor > Event Log Alerts > Edit Event Sets.

Feature Set

A feature set provides advanced, specialized functionality that is typically hidden in the basic module. The basic module must be installed and the feature licensed separately to display feature set options.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. The **FTP server** is the program on the target machine that listens on the network for connection requests from other computers. The **FTP client** is the program on the VSA user's local machine that initiates a connection to the server. The FTP client machine requires user access rights to the FTP server machine. It is included with the Kaseya Server primarily to provide immediate technical support. Once connected, the client can upload files to the server, download files from the server, rename or delete files on the server and so on. Any software company or individual programmer is able to create FTP server or client software because the protocol is an open standard. Virtually every computer platform supports the FTP protocol. Since Kaseya FTP sessions are relayed through the Kaseya Server, all FTP sessions are protected by 256 bit rolling encryption protocol.

Flood Detection

If 1000 events—not counting **black list events** *(page 11)*—are uploaded to the Kaseya Server by an agent *within one hour*, further collection of events of that log type are stopped for the remainder of that hour. A new event is inserted into the event log to record that collection was suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your Kaseya Server. Alarm detection and processing operates regardless of whether collection is suspended.

Global Event Log Black Lists

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

Group Alarms

Alarms for alerts, event log alerts, system check, and log monitoring are automatically assigned to a **group alarm** category. If an alarm is created, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the Group Alarm Status dashlet of the Monitor > **Dashboard List** page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > Monitor Lists. Group alarm column names are assigned to monitor sets using Define Monitor Set.

Host name

The text equivalent of an IP address. For example, the IP address `89.234.7.197` should resolve to the host name of `www.kaseya.com`.

ISO Image

An **ISO image (.iso)** is a disk image of an ISO 9660 file system. ISO 9660 is an international standard originally devised for storing data on CD-ROM. In addition to the data files that are contained in the ISO image, the ISO image also contains all the filesystem metadata, including *boot code*, structures, and attributes. All of this information is contained in a single file. CD writers typically provide the option of writing an ISO file *as an image* when writing to a CD.

Log Monitoring

The VSA is capable of monitoring data collected from many **standard log files** *(page 12)*. **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 20)* files created for Unix, Linux, and Apple operating systems, and network devices such as Cisco routers. To avoid uploading all the data contained in these logs to the Kaseya Server database, **Log Monitoring** uses **parser definitions and parser sets** *(page 15)* to parse each log file and select only the data you're interested in. Parsed messages are displayed in Log Monitoring, which can be accessed using the Agent Logs tab of Live Connect (Classic) > Agent Data or the Machine Summary page or by generating a report using the Agent > Logs - Log Monitoring page. Users can optionally trigger alerts when a **Log Monitoring** record is generated, as defined using Assign Parsing Sets or Parser Summary.

Logs

Logs collect event information about multiple systems, including the Kaseya Server. The different types of logs that can be generated are:

- **Admin Notes** - Lists user notes, sorted by user.
- **Agent Log** - Shows a list of activity associated with the Agent machine Agent. Start and stop times, `.ini` file changes, and other information is captured. The date and time of each activity is also noted.
- **Agent Procedure Log** - Shows a list of procedures executed on the selected agent machine. The date and time of each procedure execution is also noted, as well as whether it completed successfully or not.
- **Alarm Log** - List out all triggered alarms issued against the selected machine.
- **Configuration Changes** - Shows a log of changes made by a user to a managed machine's agent configuration.
- **Event Logs** - Shows the **event log** *(page 10)* data collected by Windows. (Not available with Win9x)
- **Log Monitoring** - enables you to monitor the data generated by any text-based log.
- **Monitor Action Log** - The log of **alert conditions** *(page 7)* that have occurred and the corresponding actions, if any, that have been taken in response to them.
- **Network Statistics** - Shows a list of applications that have accessed the network and the packet size of the information exchanged during the network access session. The time of the exchange is also listed.
- **Remote Control Log** - Lists successful remote controls sessions.

MAC address

The unique **media access control (MAC)** identifier assigned to network adapter cards (NICs).

Machine ID / Group ID / Organization ID

Each **agent** *(page 3)* installed on a managed machine is assigned a unique **machine ID / group ID / organization ID**. All machine IDs belong to a machine group ID and optionally a subgroup ID. All machine group IDs belong to an organization ID. An organization typically represents a single customer account. If an organization is small, it may have only one machine group containing all the machine IDs in that organization. A larger organization may have many machine groups and subgroups, usually organized by location or network. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.sales.chicago.acme`. In this case `sales` is a subgroup ID within the `chicago` group ID within the organization ID called `acme`. In some places in the VSA, this

hierarchy is displayed in reverse order. Each organization ID has a single default machine group ID called `root`. Group IDs and subgroup IDs are created using the System > Orgs/Group/Depts/Staff > Manage > Machine Groups page.

Machine ID / Group ID filter

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

> **Note:** Even if a VSA user selects `<All Groups>`, only groups the VSA user is granted access to using System > User Security > Scopes are displayed.

Machine ID Template

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

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

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the **machine ID / group ID / organization ID** *(page 12)* and the **agent** *(page 3)*. The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

Machine Roles

The **Machine Roles** page creates and deletes machine roles. Machine roles determine what *machine users* see when they use Kaseya User Portal or Portal Access (Classic) from a machine with an agent. The user access window displays when a *machine user double-clicks the agent icon in the system tray of their managed machine.*

> **Note:** The **User Roles** page determines what *VSA users* see when they use Live Connect or Live Connect (Classic) from within the VSA.

Within the **Machine Roles** page you can select:

- Members - Assign or remove machines for a machine role.
- Access Rights - Select the access rights for a machine role. Access rights determine the functions a *machine user* can access.
- Role Types - Assign or remove role types for a machine role. Currently there is only one machine role type provided and no access rights are restricted.

Managed Machine

A monitored machine with an installed **agent** *(page 3)* and active **machine ID / group ID** *(page 13)* account on the Kaseya Server. Each managed machine uses up one agent license.

Master User / Standard User

A master user is a VSA **user** *(page 20)* that uses a `Master` user role and a `Master` scope. The `Master` user role provides user access to all functions throughout the VSA. The `Master` scope provides access to all scope data objects throughout the VSA. A `Master` user role can be used with a non-`Master` scope, but a `Master` scope cannot be used with a non-`Master` role. Kaseya Server management configuration and other specialized functions can only be performed by `Master` role users. The term *standard user* is sometimes used to indicate a user that does not use a `Master` user role and a `Master` scope.

Migrating the Kaseya Server

For the latest instructions on migrating an existing Kaseya Server to a new machine see *Moving the Kaseya Server* section in the latest **Kaseya Server installation instructions** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/Install/index.asp#home.htm)*.

Monitor Sets

A monitor set is a set of **counter objects**, **counters**, **counter instances**, **services** and **processes** used to monitor the performances of machines. Typically, a threshold is assigned to each **object/instance/counter** *(page 16)*, service, or process in a monitor set. Alarms can be set to trigger if any of the thresholds in the monitor set are exceeded. A monitor set should be used as a logical set of things to monitor. A logical grouping, for example, could be to monitor all counters and services integral to running an Exchange Server. You can assign a monitor set to any machine that has an operating system of Windows 2000 or newer.

The general procedure for working with monitor sets is as follows:

1. Optionally update monitor set counter objects, instances and counters manually and review them using Monitor Lists.
2. Create and maintain monitor sets using Monitor > Monitor Sets.
3. Assign monitor sets to machine IDs using Monitor > Assign Monitoring.
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.
6. Review monitor set results using:
   - Monitor > Monitor Log
   - Monitor > Live Counter
   - Monitor > Dashboard > Network Status
   - Monitor > Dashboard > Group Alarm Status
   - Monitor > Dashboard > Monitoring Set Status
   - Info Center > Reporting > Reports > Monitor > Monitor Set Report
   - Info Center > Reporting > Reports > Monitor > Monitor Action Log

Monitor Types

0 - Counter
1 - Service

    2 - Process
    3 - SNMP
    4 - Alert - Alerts are further classified using **alert types** *(page 6)*.
    5 - System Check
    6 - EPS
    7 - Log Monitoring

myOrg

`myOrg` is the **organization** *(page 15)* of the service provider using the VSA. All other organizations in the VSA are second party organizations doing business with `myOrg`. The default name of `myOrg`, called `My Organization`, should be renamed to match the service provider's company or organization name. *This name displays at the top of various reports to brand the report.* Agents installed to internally managed machines can be assigned to this organization. *VSA user logons are typically associated with staff records in the* `myOrg` *organization.* `myOrg` cannot be assigned a parent organization.

On Premises

An **on premises** hardware/software installation of the VSA is a maintained by a service provider and typically used only by the service provider. See **Software as a Service (SaaS)** *(page 19)*.

Org

The VSA supports three different kinds of business relationships:

- **Organizations** - Supports machine groups and manages machines using agents.
- **Customers** - Supports the billing of customers using **Service Billing**.
- **Vendors** - Supports the procurement of materials using **Service Billing**.

The `Org` table is a support table shared by *organizations*, *customers* and *vendors*. Each record in the `Org` table is identified by a unique `orgID`. The `Org` table contains basic information you'd generally need to maintain about any kind of business relationship: mailing address, primary phone number, duns number, yearly revenue, etc. Because the `Org` table is shared, you can easily convert:

- A customer into an organization or vendor.
- A vendor into an organization or customer.
- An organization into a customer or vendor.

> **Note:** `myOrg` (page 15) is the organization of the service provider using the VSA.

Parser Definitions and Parser Sets

When configuring **Log Monitoring** *(page 12)* it's helpful to distinguish between two kinds of configuration records: **parser definitions** and **parser sets**.

A **parser definition** is used to:

- Locate the log file being parsed.
- Select log data based on the log data's *format*, as specified by a template.
- Populate parameters with log data values.
- Optionally format the log entry in **Log Monitoring**.

A **parser set** subsequently *filters* the selected data. Based on the *values* of populated parameters and the criteria you define, a parser set can generate log monitoring entries and optionally trigger alerts.

Without the filtering performed by the parser set, the Kaseya Server database would quickly expand. For example a log file parameter called $FileServerCapacity$ might be repeatedly updated with the latest percentage of free space on a file server. Until the free space is less than 20% you may not need to make a record of it in **Log Monitoring**, nor trigger an alert based on this threshold. Each parser set applies only to the parser definition it was created to filter. Multiple parser sets can be created for each parser definition. Each parser set can trigger a separate alert on each machine ID it is assigned to.

Patch Policy

Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named `servers` and assign all your servers to be members of this patch policy and another patch policy named `workstations` and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- Initial Update and Automatic Update require patches be approved before these patches are installed.
- Approval by Policy approves or denies patch by *policy*.
- Approval by Patch approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- KB Override overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- Patch Update and Machine Update can install denied patches.
- Non-`Master` role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

Patch Update Order

Service packs and patches are installed in the following order:

1. Windows Installer
2. OS related service packs
3. OS update rollups
4. OS critical updates
5. OS non-critical updates
6. OS security updates
7. Office service packs
8. Office update rollups
9. All remaining Office updates

> **Note:** Reboots are forced after each service pack and at the end of each patch group **without warning**. This is necessary to permit the re-scan and installation of the subsequent groups of patches.

Performance Objects, Instances and Counters

When setting up counter thresholds in **monitor sets** *(page 14)*, it's helpful to keep in mind exactly how both Windows and the VSA identify the components you can monitor:

- **Performance Object** - A logical collection of counters that is associated with a resource or service that can be monitored. For example: processors, memory, physical disks, servers each have their own sets of predefined counters.

- **Performance Object Instance** - A term used to distinguish between multiple performance objects of the same type on a computer. For example: multiple processors or multiple physical disks. The VSA lets you skip this field if there is only one instance of an object.
- **Performance Counter** - A data item that is associated with a performance object, and if necessary, the instance. Each selected counter presents a value corresponding to a particular aspect of the performance that is defined for the performance object and instance.

Portal Access (Classic)

> **Note:** Portal Access in R95 only works using Live Connect (Classic). Even if the **Use new Live Connect when clicking the Live Connect button in Quickview** option is set to Yes in System > Default Settings, Live Connect (Classic) will still be used when logging into the VSA using Portal Access credentials.

Portal Access (Classic) is a Live Connect (Classic) session initiated by the machine user. The machine user displays the **Portal Access** page by clicking the agent icon on the system tray of a managed machine. **Portal Access** contains machine user options such as changing the user's contact information, creating or tracking trouble tickets, chatting with VSA users or remote controlling their own machine from another machine. **Portal Access** logons are defined using Agent > Portal Access. The function list the user sees during a **Portal Access** session is determined by the System > Machine Roles page. You can customize **Portal Access** sessions using the System > Customize > Live Connect page.

Primary Domain Controller

Primary domain controllers have full access to the accounts databases stored on their machines. Only primary domain controllers run **Active Directory** *(page 3)*.

Private Folders

Private Folders

Objects you create—such as reports, procedures, or monitor sets—are initially saved in a folder with your user name underneath a **Private** cabinet. This means only you, the creator of the objects in that folder, can view those objects, edit them, run them, delete them or rename them.

To share a private object with others you first have to drag and drop it into a folder underneath the **Shared** cabinet.

> **Note:** A master role user can check the **Show shared and private folder contents from all users** checkbox in System > Preferences to see all shared and private folders. For Private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.

Quick Status

A **Quick Status** feature enables you to select *any* monitor set counter, service or process from *any* machine ID and add it to the same single display window. Using **Quick Status**, you can quickly compare the performance of the same counter, service or process on different machines, or display selected counters, services and processes from different monitor sets all within a single view. SNMP sets provide a similar **Quick Status** view for selected SNMP objects. *Any Quick Status view you create exists only for the current session.* The **Quick Status** window is accessed using Monitor > Dashboard > Monitoring Set Status, then clicking the **Quick Status** link or the **Quick Status** icon .

Scanning Networks

The **Discovery** module uses an existing VSA **agent** *(page 3)* on a managed machine to scan a local area network for any and all new devices connected to that network since the last time a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#10627.htm)* ran. These new devices can be workstations and servers without agents, **SNMP devices** *(page 18)* and vPro machines. Optionally, the VSA can send an **alert** *(page 5)* when a scanning discovers any new device. **Discovery** effectively uses the agent as a proxy to scan a network behind a firewall that might not be accessible from a remote

server.

Silent Install

Silent installs, also called **silent deploys**, do not prompt the user for input. Silent installs may not require user input or else provide a typical configuration that serves the purposes of most users, or else provide command line parameters that enable users to configure the installation at execution. If an install does not support a silent install but still needs to be distributed automatically, users can use Packager to create a custom installation package. See Creating Silent Installs.

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 communiity 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 3)*. But a VSA agent installed on a managed machine on the same network as the device can read or write to that device using **simple network management protocol (SNMP).**

SNMP Quick Sets

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **network is scanned** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#1944.htm)* is performed. You can use the list of discover MIB objects to instantly create a device-specific SNMP set—called a **quick set**—and apply it to the device. Once created, quick sets are the same as any standard set. They display in your private folder in Monitor > **SNMP Sets** and in the drop-down list in Monitor > **Assign SNMP**. A (QS)prefix reminds you how the quick set was created. Like any other standard set, quick sets can be *individualized* for a single device, used with Auto Learn, shared with other users, and applied to similar devices throughout the VSA.

1. Discover SNMP devices using Discovery > By Network or **By Agent** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#1944.htm)*.
2. Assign SNMP sets to discovered devices using Monitor > Assign SNMP.
3. Click the hyperlink underneath the name of the device, called the SNMP info link, in the **Assign SNMP** page to display a dialog.
   - ➢ Click **Discovered MIB Objects** and select one or more of the MIB objects that were discovered on the SNMP device you just selected.
   - ➢ Click **Quick Set Items** and, if necessary, edit the alarm thresholds for selected MIB objects.
   - ➢ Enter a name after the **(QS)** prefix in the header of the dialog.
   - ➢ Click the **Apply** button to apply the quickset to the device.
4. Display SNMP monitoring data returned by the quick set using Monitor > SNMP Log, the same as you would for any other standard SNMP set.
5. Optionally maintain your new quick set using Monitor > **SNMP Sets** *(page 18)*.

SNMP Sets

A SNMP set is a set of MIB objects used to monitor the performance of **SNMP enabled network devices** *(page 18)*. The SNMP protocol is used because an agent cannot be installed on the device. You can assign alarm thresholds to any performance object in a SNMP set. If you apply the SNMP set to a device, you can be notified if the alarm threshold is exceeded. The following methods can be used to configure and assign SNMP sets to machine IDs.

- **SNMP quick sets** - Creates and assigns a device-specific SNMP set based on the objects discovered on that device during a network scan. **SNMP quick sets** *(page 18)* 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 19)* determined during a network scan.

Typically the following procedure is used to configure and apply SNMP sets to devices.

1. Discover SNMP devices using Discovery > By Network or **By Agent** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#1944.htm)*.
2. Assign SNMP sets to discovered devices using Monitor > Assign SNMP. This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using   Monitor > SNMP Log or Dashboard List.

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.
- Optionally maintain SNMP sets using Monitor > SNMP Sets.
- Optionally add an SNMP object using Monitor > Add SNMP Object.
- Optionally assign a SNMP type to an SNMP device manually using Monitor > Set SNMP Type.
- Optionally write values to SNMP devices using Monitor > Set SNMP Values.

SNMP Types

Most SNMP devices are classified as a certain type of SNMP device using the MIB object `system.sysServices.0`. For example, some routers identify themselves as routers generically by returning the value `77` for the `system.sysServices.0` MIB object. You can use the value returned by the `system.sysServices.0` MIB object to auto assign SNMP sets to devices, as soon as they are discovered by a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#10627.htm)*.

> **Note:** The entire OID for `system.sysServices.0` is `.1.3.6.1.2.1.1.7.0` or `.iso.org.dod.internet.mgmt.mib-2.system.sysServices`.

You can assign **SNMP sets** *(page 18)* to **devices** *(page 18)* *by type automatically* as follows:

1. Add or edit SNMP *types* using the **SNMP Device** tab in Monitor > Monitor Lists.
2. Add or edit the value returned by the MIB object `system.sysServices.0` *and associated with each SNMP type* using the **SNMP Services** tab in Monitor > **Monitor Lists**.
3. Associate a SNMP *type* with a SNMP *set* using the **Automatic Deployment to** drop-down list in Monitor > SNMP Sets > Define SNMP Set.
4. Perform a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#1944.htm)*. During the scan SNMP devices are automatically assigned to be monitored by SNMP sets if the SNMP device returns a value for the `system.sysServices.0` MIB object that matches the SNMP type associated with those SNMP sets.

You can also assign **SNMP sets** *(page 18)* to **devices** *(page 18)* *manually* as follows:

- Assign a SNMP type to an SNMP device using Monitor > Set SNMP Type. Doing so causes SNMP sets using that same type to start monitoring the SNMP device.

Software as a Service (SaaS)

Sharing the capabilities of a single instance of the VSA is oftentimes called "Software as a Service". Service providers contract to access a VSA hosted and maintained by a VSA *tenant manager*. Service

providers are allocated a unique *tenant partition* of a shared Kaseya Server and database. Within their assigned partition, service providers can only see their own organizations, machine groups, agents, procedures, reports, tickets, and any other types of user-defined data. Service providers in a tenant partition have full access to most functions of the VSA except system maintenance, which is the responsibility of the VSA tenant manager.

syslog

Syslog is a standard for forwarding log messages in an IP network to a syslog server. A syslog server collects the messages broadcast by various devices on the network and integrates them into a centralized repository of syslog files. Syslog is commonly used by Unix, Linux and Apple operating systems and hardware devices such as Cisco routers. **Log Monitoring** *(page 12)* enables you to monitor syslog files.

A typical format for a syslog file entry is:

```
<time> <hostname> <tag>:<message>
```

For example:

```
Oct 15 19:11:12 Georges-Dev-Computer kernel[0]: vmnet: bridge-en1: interface en is
going DOWN
```

System Agent Procedures

System agent procedures are basic functions that are exposed by the VSA. You can schedule system agent procedures to run automatically. They cannot be edited nor can they accept parameters. A list of available system agent procedures displays in any Agent Procedure Search popup window. System agent procedures can be run from:

- Within a parent procedure using the **execute**Procedure() or **schedule**Procedure() commands of an IF-ELSE-STEP statement.
- Any alerts page using the **Run Agent Procedure** checkbox.
- The **Pending Procedures** tab in Live Connect or the Machine Summary page.

Because a system agent procedure can be run using an alert or parent agent procedure associated with a specific machine ID account, the scheduling of a system agent procedure can be copied, typically from a machine ID template to a machine using Agent > Copy Settings.

System Checks

The VSA can monitor machines that *don't have an agent installed on them*. This function is performed entirely within a single page called **System Check**. Machines without an agent are called **external systems.** A machine with an agent is assigned the task of performing the system check on the external system. A system check typically determines whether an external system is available or not. Types of system checks include: web server, DNS server, port connection, ping, and custom.

System Tray

The system tray is located, by default, in the lower right-hand corner of the Windows desktop, in the Taskbar. It contains the system clock, and other system icons.

User Account

See **Machine IDs vs. Agents** *(page 13)*

Users

VSA users use the VSA application to maintain the Kaseya Server and oversee the monitoring of **managed machines** *(page 14)* by the Kaseya Server and its **agents** *(page 3)*. VSA users are created using System > Users. Users also refers to machine users, who use the computers managed by the VSA. **Master users** *(page 14)* have special privileges throughout the VSA.

View Definitions

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. Views provide users flexibility for machine management and reporting. View filtering is applied to *all* function pages by selecting a view from the **Select View** drop-down list on the machine ID / group filter panel and clicking the Apply icon 🔍 . Any number of views can be created and shared with other users. Views are created by clicking the **Edit** button to the right of the **Views** drop-down list.

Virtual Machine

A virtual machine (VM) is a software implementation of a physical computer (machine) that executes programs like a physical computer. Virtual machines are capable of virtualizing a full set of hardware resources, including a processor (or processors), memory and storage resources and peripheral devices. The **Backup** module can convert a backup image into a VM. See Backup > Image to VM.

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 **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#10627.htm)*, list the hardware assets of vPro machines, access hardware-based security use the power management and remote booting of ISO images capabilities provided by vPro.

Windows Automatic Update

Windows Automatic Updates is a Microsoft tool that automatically delivers updates to a computer. Windows Automatic Updates is supported in the following operating systems: Windows 2003, Windows XP, Windows 2000 SP3 or later, and all operating systems released after these. Patch Management > Windows Auto Update can enable or disable this feature on managed machines. While Windows Millennium Edition (Me) has an Automatic Updates capability, it cannot be managed as the above operating systems can.

Work Types

Work types determine how time entries are integrated with other functions in the VSA. The work type options displayed in your VSA depend on the modules installed.

- **Admin Tasks** - A recurring operational activity not associated with any project.
- **Work Orders** - Only displays if the **Service Billing** is installed.
- **Service Desk Tickets** - Only displays if **Service Desk** 1.3 or later is installed.

Index

U

V

W