Kaseya

Monitor

User Guide

Version R94

English

July 20, 2017

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 Kseya 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

Monitor Overview

Monitor

The **Monitoring** module in **Virtual System Administrator™** provides six methods of monitoring machines and log files:

- **Alerts -** Monitors events on *agent* machines.
- **Event Log Alerts** - Monitors events in the event logs of *agent* machines.
- **Monitor Sets** - Monitors the performance state on *agent* machines.
- **SNMP Sets** - Monitors the performance state on *non-agent devices*.
- **System Check** - Monitors events on *non-agent* machines.
- **Log Monitoring** - Monitors events in *log files*.

You can monitor the health in real time of managed machines   and SNMP devices and be notified immediately if any problems arise. When programmable alarms are triggered, **Monitor** executes email notifications, procedures and job ticketing, for such problems and state changes as:

- When any critical server or desktop computer goes off-line.
- When a machine user disables remote control.
- When any software application is added or removed.
- When the hardware configuration changes.
- When the computer is running low on disk space.
- When a specific event or any event log entry is generated.
- When any protection policy violation occurs.
- When any agent procedure fails execution.
- When an unapproved application attempts to access the network.
- When an unapproved application attempts to access a protected file.
- When a new device appears on the local area network.
- When an external log records a specific log entry.

In addition to generating alert notifications when **event log entries** are generated, event log entries collected from your managed machines are stored on the VSA. The event log data is always available, even if the managed machine goes offline or suffers a hard failure. Event log data is presented in a familiar and concise form using the Agent > Agent Logs page, as well as Info Center > Reporting > Reports > Logs.

> **Note:** You can download a **Monitoring Configuration** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/EN_monitoringconfiguration_R94.pdf#zoom=70&navpanes=0)* PDF from the first topic of online user assistance.
>
> **Note:** You can download a **Configuring Log Parsers Step-by-Step** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/EN_logparsers_R94.pdf#zoom=70&navpanes=0)* PDF from the first topic of online user assistance.
>
> **Note: Kaseya IT Services** *(http://www.kaseya.com/customer-success/services)* extends monitoring past nine-to-five. By out-tasking systems management and monitoring during off-hours, MSPs can offer customers 24/7/365 "Always-On" monitoring.
>
> **Note:** Any agent used for monitoring must be updated using the Agent > Manage Agents page.

Function	Description
Dashboard List *(page 6)*	Provides multiple monitoring views.

Dashboard Settings *(page 14)*	Users can customize the Dashboard List page.
Alarm Summary *(page 14)*	Lists alarms for monitored machines.
Suspend Alarms *(page 16)*	Suspends alarm notifications for specific machine IDs.
Live Counter *(page 17)*	Displays live performance counter data for a selected machine ID.
Monitor Lists *(page 18)*	Configures the monitor list objects for monitoring.
Update Lists By Scan *(page 20)*	Scans machines for monitor counters and services.
Monitor Sets *(page 21)*	Configures monitor sets.
SNMP Sets *(page 28)*	Configures SNMP monitor sets.
Add SNMP Object *(page 33)*	Manages SNMP MIB objects.
Alerts *(page 35)*	Configures monitor alerts for machines.
Event Log Alerts *(page 64)*	Triggers an alert for an event log entry.
SNMP Traps Alert *(page 70)*	Configures alerts for SNMP Trap event log entries created on selected managed machines.
Assign Monitoring *(page 73)*	Assigns, removes and manages alarms of monitor sets on machines.
Monitor Log *(page 79)*	Views monitor log data in chart and table format.
System Check *(page 81)*	Assigns, removes and manages alarms for system checks on machines.
Assign SNMP *(page 84)*	Assigns, removes and manages alarms of SNMP monitor sets on devices.
SNMP Log *(page 93)*	Views SNMP log data in chart and table format.
Set SNMP Values *(page 94)*	Sets SNMP values on the specified device.
Set SNMP Type *(page 95)*	Assigns SNMP types to SNMP devices.
Parser Summary *(page 97)*	Defines alerts for parser sets and copy parser set assignments to multiple machine IDs.
Log Parser *(page 100)*	Defines log parsers and assigns them to machine IDs.
Assign Parser Sets *(page 105)*	Creates and assigns parsers sets to machine IDs and creates alerts on parser set assignments.

Monitor Terms and Concepts

The same alert management terms and concepts apply to all methods of monitoring.

Alerts and Alarms

- **Alerts** - An alert is created when the performance of a machine or device matches a pre-defined criteria or "alert condition".
- **Alarms** - *Alarms* are a graphical way of notifying the user that an *alert* has occurred. In many graphical displays throughout the VSA, when an alert exists, the VSA displays by default a red traffic light ⬤ icon. If no alert exists, a green traffic light icon ⬤ displays. These icons can be customized.
- **Logs** - Two logs distinguish between alerts and alarms.
  - ➢ **Alarm Log** - Tracks any *alarm that was created by an alert.*
  - ➢ **Monitor Action Log** - Tracks any *alert that was created*, whether or not an alarm or any other type of action was taken in response to the alert.

Actions

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

- A = Create **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.

Types of Alerts

Types of alerts include:

- Discovery > By Network or By Agent
- Backup > Backup Alerts
- Monitor > **Alerts** *(page 35)* - These are specialized "fixed" alerts that are ready to apply to a machine.
- Monitor > **Assign Monitoring** *(page 73)*
- Monitor > **SNMP Traps Alert** *(page 70)*
- Monitor > **Assign SNMP** *(page 84)*
- Monitor > **System Checks** *(page 81)*
- Monitor > **Parser Summary** *(page 97)*
- Monitor > **Assign Parser Sets** *(page 105)*
- Patch Management > Patch Alerts
- Remote Control > Offsite Alerts
- Security > Apply Alarm Sets

Other add-on modules have alerts not listed here.

Six Methods of Monitoring

Each of the six methods of monitoring in **Virtual System Administrator™** is either *event-based* or

state-based.

- Event-based
    - **Alerts** - monitors events on *agent* machines
    - **Event Log Alerts** - monitors events in the event logs of *agent-installed* machines
    - **System Check** - monitors events on *non-agent* machines
    - **Log Monitoring** - monitors events in *log files*
- State-based
    - **Monitor Sets** - monitors the performance state on *agent* machines
    - **SNMP Sets** - monitors the performance state on *non-agent devices*

Event-Based Alerts

Alerts *(page 35)*, **System Check** *(page 81)*, Event Log Alerts and **Log Monitoring** *(page 100)* represent **event-based alert** that occur perhaps once. For example a backup may fail. Even if the backup succeeds later, the failure of the backup is a historical event in the alarm log. If an alarm is created for this type of event, then *the alarm remains "open" in the alarm log even if the alert condition recovers.* Typically you use the **Alarm Summary** *(page 14)* page to review alarms created by event-based alerts. When the issue is resolved you "close' the alarm.

Event-based alerts are usually easier to configure, since the possibilities are reduced to whether one or more of the events happened or did not happen within a specified time period.

State-Based Alerts

Monitor set *(page 21)* counters, services, and processes and **SNMP set** *(page 28)* objects are either currently within their expected state range or outside of it and display as red or green alarm icons *dynamically* in monitoring dashlets. These are known as **state-based alerts**.

- *If an alert condition currently exists, monitor dashlets (page 6) show a red alarm icon.*
- *If an alert condition does not currently exist, monitor dashlets show a green alarm icon.*

If you create an alarm for state-based alerts, they'll create alarm entries in the alarm log just like event-based alarms, which you can then choose to close. But because state-based alerts typically go in and out of an alert condition dynamically, you may want to avoid creating an alarm each time this happens. Instead use the **Network Status** *(page 10)* dashlet to identify the *current status* of state-based alerts. Once the issue is corrected on the machine or device, the status of the alert automatically returns to a green icon. You don't have to manually "close" the alert in this dashlet.

> Note: If you do decide to create traditional alarms for monitor sets and off-line alerts specifically, these two types of alerts can be closed automatically when they recover. See the **Enable auto close of alarms and tickets** checkbox on the System > Configure page.

Typically state-based alarms require more thought to configure then event-based alarms, because the intent is to measure the level of performance rather than outright failure.

Dashboards and Dashlets

The **Dashboard List** page is the VSA's primary method of visually displaying monitoring data, including alerts and alarms. The **Dashboard List** page maintains configurable monitoring windows called **Dashboard Views**. Each dashboard contains one or more panes of monitoring data called **Dashlets**. Each VSA user can create their own customized dashboards. Types of dashlets include:

- **Alarm List** *(page 7)*
- **Alarm Network Status** *(page 8)*
- **Alarm Rotator** *(page 10)*
- **Alarm Ticker** *(page 10)*
- **Network Status** *(page 10)*
- **Group Alarm Status** *(page 10)*

- **Monitoring Set Status** *(page 11)*
- **Monitor Status** *(page 13)*
- **Machines Online** *(page 13)*
- **Top N - Monitor Alarm Chart** *(page 13)*

Reviewing Alarms

All alert conditions that have the **Create Alarm** checkbox checked—both state-based alarms and event-based alarms—are recorded in the **alarm log**. An alarm listed in the alarm log does not represent the *current status* of a machine or device, rather it is a *record* of an alarm that has occurred *in the past*. An alarm log record remains `Open` until you close it.

Created alarms can be, reviewed, `Closed` or **Deleted...** using:

- Monitor > **Alarm Summary** *(page 14)*
- Monitor > Dashboard List > any **Alarm Summary Window** *(page 8)* within a dashlet
- Agent > Agent Logs > Alarm Log
- Live Connect (Classic) > Agent Data > Agent Logs > Alarm Log

Created alarms can also be reviewed using:

- Monitor > Dashboard List > **Alarm List** *(page 7)*
- Monitor > Dashboard List > **Alarm Network Status** *(page 8)*
- Monitor > Dashboard List > **Alarm Rotator** *(page 10)*
- Monitor > Dashboard List > **Alarm Ticker** *(page 10)*
- Monitor > Dashboard List > **Group Alarm Status** *(page 10)*
- Monitor > Dashboard List > **Monitor Set Status** *(page 11)*
- Monitor > Dashboard List > **Monitor Status** *(page 13)*
- Monitor > Dashboard List > **Top N - Monitor Alarm Count** *(page 13)*
- Monitor > Dashboard List > **KES Status** *(page 13)*
- Monitor > Dashboard List > **KES Threats** *(page 14)*
- Info Center > Reporting > Reports > Monitoring > Logs > Alarm Log
- Info Center > Reporting > Reports > Monitoring > Monitor Action Log
- Live Connect > Asset > Log Viewer > Alarm

Reviewing Performance (with or without Creating Alarms)

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

- Monitor > **Live Counter** *(page 17)*
- Monitor > **Monitor Log** *(page 79)*
- Monitor > **SNMP Log** *(page 93)*
- Monitor > Dashboard > **Network Status** *(page 10)*
- Monitor > Dashboard > **Group Alarm Status** *(page 10)*
- Monitor > Dashboard > **Monitoring Set Status** *(page 11)*
- Info Center > Reporting > Reports > Monitoring > Logs

Suspending Alarms

The triggering of alarms can be suspended. The **Suspend Alarms** page suppresses alarms for specified time periods, including recurring time periods. This allows upgrade and maintenance activity to take place without generating alarms. When alarms are suspended for a machine ID, *the agent still collects data, but does not generate corresponding alarms.*

Group Alarms

Alarms for alerts, event log alerts, system check, and log monitoring are automatically assigned to a **group alarm** category. If an alarm is created, the group alarm it belongs to is triggered as well. The group

alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display in the **Group Alarm Status** *(page 10)* dashlet of the Monitor > Dashboard List page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > **Monitor Lists** *(page 18)*. Group alarm column names are assigned to monitor sets using **Define Monitor Set** *(page 23)*.

Dashboard List

Info Center > Dashboard > Dashboard List
Monitor > Dashboard > Dashboard List

- Similar information is provided using Monitor > *Alarm Summary (page 14)* and Info Center > Reporting > Reports > Monitor Alarm Summary.

The Dashboard List page is the VSA's primary method of visually displaying monitoring data, including alerts and alarms. The Dashboard List page maintains configurable monitoring windows called **Dashboard Views**. Each dashboard contains one or more panes of monitoring data called **Dashlets**. Each VSA user can create their own customized dashboards.

Adding Dashboard Views and Dashlets

To add a new dashboard:

1. Click to create a new Dashboard View. The new dashboard displays in a popup window.
2. Enter a Title and Description for your new dashboard.
3. Click the Add Dashlets tab. A side panel displays a list of dashlets. These choices include:
   - ➢ **Alarm List** *(page 7)*
   - ➢ **Alarm Network Status** *(page 8)*
   - ➢ **Alarm Rotator** *(page 10)*
   - ➢ **Alarm Ticker** *(page 10)*
   - ➢ **Network Status** *(page 10)*
   - ➢ **Group Alarm Status** *(page 10)*
   - ➢ **Monitoring Set Status** *(page 11)*
   - ➢ **Monitor Status** *(page 13)*
   - ➢ **Machines Online** *(page 13)*
   - ➢ **Top N - Monitor Alarm Chart** *(page 13)*
   - ➢ **KES Status** *(page 13)*
   - ➢ **KES Threats** *(page 14)*
4. Check as many checkboxes as you like, then click the Add button. The side panel closes and the Dashlets display in the Dashboard View.
5. Move and resize the Dashlets within the Dashboard View.
6. Click the Delete tab to delete dashlets already displayed in the Dashboard View.
7. Click to save the Dashboard View. Click to save the Dashboard View using a different title and description.
8. Click Share to share this Dashboard View with other users, user roles or to make it public for all users to use and edit.

Configuring Dashlet Options

You can size and position each dashlet within the Dashboard View. You can also access additional configuration options for each dashlet by clicking the configure icon located in the upper left hand corner of the dashlet. Common configuration options include:

- **Show Title Bar** - If checked, displays the dashlet with a title bar.
- **Title** - Specifies the title of the dashlet.
- **Refresh Rate** - Specifies how often the data in the dashlet is refreshed.
- **Machine** - Filters the dashlet by machine ID. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Machine Group** - Filters the dashlets by group ID. Select `<All Groups>` to see all groups you are authorized to see.

> **Note:** *Dashlets are unaffected by the* main *machine ID / machine group filter at the top of the VSA page.*

Add Dashboard

Click [icon] 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 [icon] to filter the list of dashboards listed in the paging area. Include an asterisk (*) wildcard with the text you enter to match multiple records. Enter a different title to rename the dashboard.

My Dashboards

If checked, only the dashboards you are the owner of display.

View

Displays the view icons available for each dashboard.

[icon] - Click to view this dashboard.

[icon] - Click to configure this dashboard.

[icon] - Click to delete this dashboard.

Owner

The owner of the dashboard.

Title

The name of the dashboard.

Description

The description of the dashboard.

Load on Startup

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

Alarm List

Dashboard > Dashboard List > Alarm List

The **Alarm List** dashlet displays all alarms for all machine IDs matching the dashlet's machine ID/group ID filter. The display lists the most recent alarms first.

Alarm Network Status

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 8)* of `Open` alarms for that machine.

Alarm Summary Window

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 status* of a machine or device, rather it is a *record* of an alarm that has occurred *in the past*. An alarm log record remains `Open` until you close it.

> **Note:** Within a dashlet, the Alarm Summary window displays *only* `Open` *alarm log records.* If you attempt to filter alarms using the `Closed` status within a dashlet, the dashlet will reset your selection to `Open`. Closing an alarm makes it disappear from this dashlet's alarm summary list. You can review both `Open` and `Closed` alarms using the **Alarm Summary** *(page 14)* page.

Filtering Alarms

Select or enter values in one or more of the following Alarm Filter fields. The filtering takes effect as soon as you select or enter a value.

- Alarm ID - A specific alarm ID.
- Monitor Type - `Counter`, `Process`, `Service`, `SNMP`, `Alert`, `System Check`, `Security` or `Log Monitoring`.
- Alarm State - `Open` or `Closed`. You can only select the `Open` status for an alarm listed in a dashlet Alarm Summary Window.
- Alarm Type - `Alarm` or `Trending`.
- Alarm Text - Text contained in the alarm. Bracket text with asterisks, for example: `*memory*`
- Filter Alarm Count - The number of alarms displayed using the current filter criteria.

Closing Alarms

You can close alarm log records in one of two ways:

- Click the `Open` link in the State column of the Alarm Summary window.

Or:

1. Set the Alarm State drop-down list to `Closed`.
2. Select one or more alarms listed in the paging area.
3. Click the Update button.

Deleting Alarms

1. Select one or more alarms listed in the paging area.
2. Click the Delete... button.

Adding Notes

1. Enter a note in the Notes field.

2. Select one or more alarms listed in the paging area.
3. Click the Update button.

Select Page

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

Select All/Unselect All

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

Alarm ID

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- 🕒 An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes. Each dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Alarm Date

The date and time the alarm was created.

Type

The type of monitor object: `Counter`, `Process`, `Service`, `SNMP`, `Alert`, `System Check,` `Security` and `Log Monitoring`.

Ticket

If a ticket has been generated for an alarm a Ticket ID link displays. Clicking this link displays the ticket in the Ticketing > View Ticket page. If no ticket has been generated for an alarm a New Ticket... link displays. Click this link to create a ticket for this alarm.

Name

The name of the monitoring object.

Alarm Rotator

Dashboard > Dashboard List > Alarm Rotator

The Alarm Rotator dashlet displays current alarms that have occurred within the last 10 minutes. Each alarm displays one at a time, in a rotating fashion, for 10 seconds. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Alarm Ticker

Dashboard > Dashboard List > Alarm Ticker

The Alarm Ticker dashlet displays current alarms that have occurred within a specified period. Each alarm displays one at a time, in a "ticker-tape" fashion, for 10 seconds. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Network Status

Dashboard > Dashboard List > Network Status

The Network Status dashlet is specific for machines assigned *monitor sets* or devices assigned *SNMP sets*. This dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

The value of this dashlet is that you can see the *current state* of monitor sets on machines or SNMP sets on devices *dynamically*.

Initially the Network Status dashlet displays each machine group as an icon. You can click any group icon to display the machines and SNMP devices within that group. If even a single monitor set or SNMP set is in an alarm state, then the icon for that machine or device displays a red exclamation point. Click any machine icon or device icon to display a list of monitor set alarms or SNMP set alarms that are *currently* outside their alarm thresholds. Alarms in this list are automatically removed as soon as the monitor set or SNMP set returns to a "no alarm" state.

Dismissed

You can manually force an alarm to return to a "no alarm" state by clicking the Dismiss link for that alarm. The "alarm" state will reappear again if the monitor set or SNMP set crosses its alarm threshold again. The timing of the reappearance depends on the alarm interval criteria defined for that monitor set or SNMP set.

> Note: Dismissing an alarm *state* should not be confused with the Open or Closed status of an alarm *record* entered in the alarm log, which is displayed, for example, using the **Alarm Summary Window** *(page 8)*. Alarm log entries can remain Open indefinitely, long after the alarm state has returned to "no alarm".

# Group Alarm Status

Dashboard > Dashboard List > Group Alarm Status

The Group Alarm Status dashlet summarizes the alarm status of all group alarm categories, for all machine IDs matching the *dashlet's* unique machine ID/group ID filter. Alarms for alerts, event log alerts, system check, and log monitoring are automatically assigned to a group alarm category. If an alarm is created, the group alarm it belongs to is triggered as well. The group alarm categories for monitor sets and SNMP sets are manually assigned when the sets are defined. Group alarms display

in the **Group Alarm Status** *(page 10)* dashlet of the Monitor > **Dashboard List** page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > **Monitor Lists** *(page 18)*. Group alarm column names are assigned to monitor sets using **Define Monitor Set** *(page 23)*.

> **Note:** Do not confuse *group alarm categories* with *machine group IDs*.

- Click the **machine group ID** link to display the group alarm status of all machine IDs and SNMP device IDs included in that machine group ID.
- Click the **Machine ID/SNMP Device ID** link to display a **Monitor Set Status** *(page 11)* 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 8)* for that combination of *group alarm category and machine group ID* or *group alarm category and machine ID*.
- Click **Filter...** to filter a dashlet by group alarm category or by machine group ID. Click **Reset** to return a filtered dashlet back to its default. You can also re-order the display of group alarm categories.

Monitoring Set Status

Dashboard > Dashboard List > Monitoring Set Status

- You can also display a Monitoring Set Status dashlet using a Group Alarm Status dashlet, by clicking a machine group ID link, then a machine ID link.

The **Monitoring Set Status** dashlet displays all alarms assigned to a machine ID, whether created by monitor set, alert, system check, **SNMP set** *(page 28)*, or Log Monitoring. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Display only alarmed monitor objects

If checked, only alarmed monitor objects are displayed in the list.

Display only alarmed machines

If checked, only alarmed machines are displayed in the list.

First Row of Information

The first row of information displays:

- The check-in status icon - Click to display the Live Connect window.
- The machine status icon 🔲 - Click to display the **Machine Status** *(page 13)* 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.

Monitor Sets

If a monitoring set is assigned to a machine ID, the following displays below the name of the monitor set:

- The triggered alarm 🔴 or no-alarm 🟢 status of the monitoring set.
- The expand icon ⊞ - Click to display collection and threshold information.
- The **Quick Status** link or the quick chart icon 📊 - Click to display a **Quick Status Monitor** popup window. This feature enables you to select *any* monitor set counter, service or process from *any*

machine ID and add it to the same single display window. Using Quick Status, you can quickly compare the performance of the same counter, service or process on different machines, or display selected counters, services and processes from different monitor sets all within a single view. SNMP sets provide a similar Quick Status view for selected SNMP objects. *Any Quick Status view you create exists only for the current session.* Use the **Machine Status** *(page 13)* icon to permanently save chart display selections.

- The monitoring log icon - Click to display the **monitoring log** *(page 79)* for this single alarm counter in a popup window.
- The live monitoring log icon - Click to display current, ongoing counter log information in a popup window.
- The monitor set object name.
- For triggered alarms, the Alarm hyperlink displays. Click to display the **Alarm Summary Window** *(page 8)*. 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 8)*. 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 8)*. 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 13)* popup window.
- The IP address of the SNMP device.
- The name of the SNMP device.
- The name of the SNMP set assigned to the SNMP device. The following displays with each SNMP set:
  - ➢ The triggered or no-alarm status of the SNMP set.
  - ➢ The expand icon - Click to display collection and threshold information.
  - ➢ The monitoring log icon - Click to display the **SNMP log** *(page 93)* 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 8)*. The Alarm Summary Window is restricted to just Open alarms for the selected SNMP set object and SNMP device.

Machine Status

Dashboard > Dashboard List > Monitor Set Status > Machine Status icon ▦

The **Machine Status** popup window selects and displays charts or tables for monitor set objects. The setup is specific for each machine ID and can be saved permanently. Applies to monitor set objects only. Monitor sets must be assigned to a machine ID before using this window.

- Click the **Setup...** button to select monitoring objects to display and to set the chart or table format.
- Click the **Save Position** button to save the selection and format of monitoring objects on the **Monitor Set Status** popup window.

Device Status

Dashboard > Dashboard List > Monitor Set Status > Machine Status icon ▦

The **Device Status** popup window selects and displays charts or tables for SNMP devices. The setup is specific for each SNMP device and can be saved permanently.

- Click the **Setup...** button to select monitoring objects to display and to set the chart or table format.
- Click the **Save Position** button to save the selection and format of monitoring objects on the **Monitor Set Status** popup window.

Monitor Status

Dashboard > Dashboard List > Monitor Status

The **Monitor Status** dashlet displays a bar chart showing the number of alarms created for the selected time interval. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. This dashlet can be customized using Monitor > **Dashboard Settings** *(page 14)*.

Machines Online

Dashboard > Dashboard List > Machines Online

The **Machines Online** chart shows the percentage of servers and workstations online. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. This dashlet can be customized using Monitor > **Dashboard Settings** *(page 14)*.

Top N - Monitor Alarm Chart

Dashboard > Dashboard List > Top N - Monitor Alarm Chart

The **Top N - Monitor Alarm Chart** dashlet displays a bar chart showing which machines have the *most* alarms for the selected time interval. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID filter. The chart shows up to 10 machines. This dashlet can be customized using Monitor > **Dashboard Settings** *(page 14)*.

KES Status

Dashboard > Dashboard List > KES Status

The **KES Status** dashlet displays different views of the security status of machine IDs using Endpoint Security protection. Applies to all machine IDs matching the *dashlet's* unique machine ID/group ID

filter. The three views of security status are:

- **Machine Configuration**
- **Scan Details**
- **Profile Chart**

> **Note:** This dashlet does not display unless the Endpoint Security add-on module is installed for the VSA.

KES Threats

`Dashboard > Dashboard List > KES Threats`

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

- **Most Recent**
- **Most Common**
- **Profile Chart**

> **Note:** This dashlet does not display unless the Endpoint Security add-on module is installed for the VSA.

Dashboard Settings

`Info Center > Dashboard > Settings`
`Monitor > Dashboard > Dashboard Settings`

The **Settings** page enables you to customize controls for dashlets.

- **Turn notification sounds on or off for all popup monitoring windows** - Applies only to the **Monitor Set Status** *(page 11)* dashlet.
- The **Chart Total Monitor Alarms** and **Chart Top N Monitor Alarms** title and background colors are customizable. Each chart parameter is customizable, this includes the chart time interval and the number of machines referenced by the **Chart Top N Monitor Alarms**.
- The **Customize machines online chart zone** specifies two percentages to create three zones of machines online:
  - ➢ The percentage of machines online, below which represents an alert condition.
  - ➢ The additional percentage of machines online, below which represents a warning condition.
- **Show refresh time**
- **Custom Dashboard Skin** - Select the border and titlebar style you want dashlets to display.

Alarm Summary

`Monitor > Status > Alarm Summary`
  - `Similar information is provided using Monitor > `Dashboard Lists` (page 6) and Info Center > Reporting > Reports > Monitor.`

The **Alarm Summary** page displays alarms for all machine IDs that match the current machine ID / group ID filter. You can include additional filtering for listed alarms using fields in the **Alarm Filters** panel. You can also close alarms or re-open them and add notes to alarms.

Filtering Alarms

Select or enter values in one or more of the following **Alarm Filter** fields. The filtering takes effect as soon as you select or enter a value.

- **Alarm ID** - A specific alarm ID.
- **Monitor Type** - `Counter`, `Process`, `Service`, `SNMP`, `Alert`, `System Check`, `Security` or `Log Monitoring`.
- **Alarm State** - `Open` or `Closed`. You can only select the `Open` status for an alarm listed in a dashlet **Alarm Summary Window**.
- **Alarm Type** - `Alarm` or `Trending`.
- **Alarm Text** - Text contained in the alarm. Bracket text with asterisks, for example: `*memory*`
- **Filter Alarm Count** - The number of alarms displayed using the current filter criteria.

Closing Alarms

You can close alarm log records in one of two ways:

- Click the `Open` link in the **State** column of the **Alarm Summary** window.

Or:

1. Set the **Alarm State** drop-down list to `Closed`.
2. Select one or more alarms listed in the paging area.
3. Click the **Update** button.

Deleting Alarms

1. Select one or more alarms listed in the paging area.
2. Click the **Delete...** button.

Adding Notes

1. Enter a note in the **Notes** field.
2. Select one or more alarms listed in the paging area.
3. Click the **Update** button.

Select Page

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

Select All/Unselect All

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

Alarm ID

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

Check-in status

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

🕐 An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes. Each dashlet displays all machine groups and machine IDs matching the *dashlet's* unique machine ID/group ID filter.

Alarm Date

The date and time the alarm was created.

Type

The type of monitor object: `Counter`, `Process`, `Service`, `SNMP`, `Alert`, `System Check`, `Security` and `Log Monitoring`.

Ticket

If a ticket has been generated for an alarm a Ticket ID link displays. Clicking this link displays the ticket in the Ticketing > View Ticket page. If no ticket has been generated for an alarm a New Ticket... link displays. Click this link to create a ticket for this alarm.

Name

The name of the monitoring object.

Suspend Alarm

Monitor > Status > Suspend Alarm

The Suspend Alarms page suppresses alarms 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 and the scope you are using.

Clear All

Clears all time periods scheduled for suspending alarms for all selected machine IDs.

Add / Replace

Click Add to add a schedule time period when alarms will be suspended for selected machine IDs. Click Replace to remove suspend alarm time periods currently assigned to selected machine IDs and assign them a new single time period to suspend alarms.

Schedule

Click Schedule to schedule this task on selected machine IDs using the schedule options previously selected.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Clears a time period matching the date/time parameters for suspending alarms on selected machine

IDs.

Run recurring

Check the box to make this task a recurring task. Enter the number of periods to wait before running this task again.

Suspend alarms

Select the duration of time during which alarms will be suspended.

Select All/Unselect All

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

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

Next Suspend

Lists the start times when machine ID alarms are scheduled to be suspended.

Duration

Lists the duration of the time periods alarms are scheduled to be suspended.

Recur

If recurring, displays the interval to wait before running the task again.

Live Counter

Monitor > Status > Live Counter

The Live Counter page displays live performance counter data for a selected machine ID. Only machines IDs assigned one or more monitor sets using **Assign Monitoring** *(page 73)* are listed on this page. The list of machine IDs you can select depends on the machine ID / group ID filter and the scope you are using.

Each specific Live Counter displays in a new window. Each window displays a bar chart with 75 data points containing the value of the counter object for the Refresh Rate specified. The chart refresh rate can be set between 3 and 60 seconds. The new data displays on the far right of the chart and the data moves from right to left as it ages.

Each bar within the chart displays in a specific color, which is determined by the alarm and warning thresholds of the monitor set counter object.

- **Red** - if alarming
- **Yellow** - if within warning threshold
- **Green** - if not alarming or not in warning threshold

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- An agent icon adorned with a red clock badge is a temporary agent.

(Machine.Group ID)

Lists the Machine.Group IDs currently matching the Machine ID / Group ID filter and that has been assigned one or more monitor sets. Click a machine ID to select a monitor set, refresh rate and one or more counters.

Select Monitor Set

Select a monitor set.

Refresh Rate

Enter a value from 3 to 60. This is the interval **Live Counter** uses to gather data.

Select Counter

Lists the counters included in a selected monitor set. Click a counter link to display a **Live Counter** window for that counter.

Monitor Lists

Monitor > Edit > Monitor Lists

The **Monitor Lists** page maintains the complete list of all objects, services and processes loaded on the Kaseya Server that are used to create **Monitor Sets** *(page 21)* and **SNMP Sets** *(page 28)*. The **Monitor List** page also maintains user-defined group alarms.

> **Note:** The **Counter Objects**, **Counters**, **Instances** and **Services** lists are populated by **Update Lists by Scan** *(page 20)*. For most Windows machines **Update Lists by Scan** is run automatically. Additionally these lists, as well as **Services** and **Processes**, can be populated with the import of a **Monitor Set** *(page 21)*. MIB OIDs can be populated by using the **Add SNMP Object** *(page 33)* page or by the import of a **SNMP Set** *(page 28)*.

Counter Objects

This tab lists **counter objects** you can include in a **Monitor Set** *(page 21)*. 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** you can include in a **Monitor Set** *(page 21)*. Monitor Set uses the **PerfMon** combination of object/counter/instance to collect counter information.

Counter Instances

This tab lists **counter instances** you can include in a **Monitor Set** *(page 21)*. Monitor Set uses the **PerfMon** combination of object/counter/instance to collect counter information.

> **Note:** Windows **PerfMon** requires that a counter object have at least one counter, but does not require an instance be available.

Services

This tab lists Windows **services** you can include in a **Monitor Set** *(page 21)* to monitor the activity of Windows Services. This list can also be populated by **Update Lists By Scan** *(page 20)* *or* the import of a **Monitor Set** *(page 21)*.

Processes

This tab lists Windows **processes** you can include in a **Monitor Set** *(page 21)* to to monitor the transition of a process to or from a running state. A process is equivalent to an application. The processes list is *not* populated via **Update Lists by Scan** *(page 20)*. This list can be populated by the import of a **Monitor Set** *(page 21)*.

CMIB OIDs

This tab lists SNMP **MIB objects** you can include in **SNMP Sets** *(page 28)*. SNMP sets monitor the activity of SNMP devices. This list can be populated with the import of a **SNMP Set** *(page 28)* *or* the execution of the **Add SNMP Object** *(page 33)* page. MIB objects are references to values that can be monitored on SNMP devices. Example: the MIB object `sysUptime` returns how much time has passed since the device was powered-up.

SNMP Devices

This tab defines broad categories of SNMP devices called **Set SNMP Types** *(page 95)*. 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 30)*. When scanning a network 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 21)* and **Define Monitor Sets** *(page 23)* to assign a monitor set to any group alarm column name. Group alarms are displayed using the **Dashboard List** *(page 6)* page.

Page Select

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

each page of data.

Edit Icon

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

Delete Icon

Click the delete icon ✖ to delete a list item.

Update Lists By Scan

Monitor > Edit > Update Lists By Scan

The **Update Lists by Scan** page scans one or more machine IDs and returns lists of counter objects, counters, instances and services to select from when creating or editing a monitor set. A consolidated list of all scanned objects displays on the Monitor > **Monitor Lists** *(page 18)* page. Typically only a handful of machines of each operating system type needs to be scanned to provide a set of comprehensive lists on the **Monitor Lists** page. **Update Lists by Scan** also updates the list of event types available for monitoring using Monitoring > **Event Log Alerts** *(page 64)*. You can see the list of event types available by displaying the Agent > Event Log Settings page. For newer Windows machines **Update Lists by Scan** need not be run more than once.

- **For Windows Machines Later than Windows 2000** - The discovery of new counter instances is managed entirely by the agent. For example, removable disks may be added to a machine. A new counter instance for a new removable disk will be discovered by the agent within a few hours. If a monitor set specifies the monitoring of that disk—either by specifying the letter of that drive or by using the *ALL counter instance—then data will start to be returned for that newly added disk. Any counters being monitored that stop are automatically restarted within the same discovery time period. All of this occurs independently of **Update Lists by Scan**.
- **For Windows 2000 and Earlier Windows Machines** - Users may elect to run **Update Lists by Scan** to discover new counter objects on those machines. This and **Enable Matching** *(page 26)* are the only reasons to run **Update Lists by Scan**.

Run Now

Runs a scan immediately.

Cancel

Click **Cancel** to cancel execution of this task on selected managed machines.

Select All/Unselect All

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

Check-in status

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

🕐 An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

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

Last Scan

This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

Next Scan

This timestamp shows the next scheduled scan. Overdue date/time stamps display as red text with yellow highlight. A green ✔ checkmark indicates the scan is recurring.

Monitor Sets

Monitor > Edit > Monitor Sets

The **Monitor Sets** page adds, imports or modifies monitor sets. Sample monitor sets are provided.

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

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

1. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** *(page 18)*.
2. Create and maintain monitor sets using Monitor > **Monitor Sets** *(page 21)*.
3. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** *(page 73)*.
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.
6. Review monitor set results using:
    - ➢ Monitor > **Monitor Log** *(page 79)*
    - ➢ Monitor > **Live Counter** *(page 17)*
    - ➢ Monitor > Dashboard > **Network Status** *(page 10)*
    - ➢ Monitor > Dashboard > **Group Alarm Status** *(page 10)*
    - ➢ Monitor > Dashboard > **Monitoring Set Status** *(page 11)*
    - ➢ Info Center > Reporting > Reports > Monitor > Monitor Set Report
    - ➢ Info Center > Reporting > Reports > Monitor > Monitor Action Log

Sample Monitor Sets

The VSA provides a growing list of sample monitor sets. The names of sample monitor sets begin with ZC. You can modify sample monitor sets, but its better practice to copy a sample monitor set and customize the copy. Sample monitor sets are subject to being overwritten every time the sample sets are updated during a maintenance cycle.

Monitoring using Apple OS X

Apple OS X supports process monitoring only. See **System Requirements**
(http://help.kaseya.com/WebHelp/EN/VSA/9040000/reqs/index.asp#home.htm).

Folder Trees

Monitor sets are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

Always Available

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon ▼ to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

When a Folder is Selected

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

  > **Note:** See guidelines for share rights to objects within folder trees in the Folder Rights topic.

- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.
- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **New Monitor Set** - Opens the **Define Monitor Set** *(page 23)* window to create a new monitor set in the selected folder of the folder tree.
- **Import Monitor Set** - Imports a monitor set.

When a Monitor Set is Selected

- **Copy Monitor Set** - Copies the selected monitor set.
- **Export Monitor Set** - Exports the selected procedure.
- **Delete Monitor Set** - Deletes the selected procedure.

Creating Monitor Sets

1. Select a folder in the middle pane.
2. Click the **New Monitor Set** button.
3. Enter a name.
4. Enter a description.
5. Select a group alarm category from the **Group Alarm Column Name** drop-down list. User defined group alarm column names are maintained using the **Monitor Lists** *(page 18)* page. Group alarms display on the **Dashboard List** *(page 6)* page.
6. Click **Save**. The **Define Monitor Sets** *(page 23)* window displays.

> **Note:** Sample monitor sets do not display in the **Assign Monitoring** *(page 73)* > **Select Monitor Set** drop-down list. Create a copy of a sample monitor set by selecting the sample set in **Monitor Sets** *(page 21)* and clicking the **Save As** button. Your copy of the sample monitor set will display in the drop-down list. In a SaaS-based VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

Define Monitor Sets

Monitor > Edit > Monitor Sets
- Select a monitor set in a folder.

The **Define Monitor Sets** window maintains a set of counter objects, counters, counter instances, services and processes included in a monitor set. This collection is drawn from a "master list" maintained using **Monitor Lists** *(page 18)*. Sample monitor sets are provided.

Monitor Sets

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

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

1. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** *(page 18)*.
2. Create and maintain monitor sets using Monitor > **Monitor Sets** *(page 21)*.
3. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** *(page 73)*.
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.
6. Review monitor set results using:
   - Monitor > **Monitor Log** *(page 79)*
   - Monitor > **Live Counter** *(page 17)*
   - Monitor > Dashboard > **Network Status** *(page 10)*
   - Monitor > Dashboard > **Group Alarm Status** *(page 10)*
   - Monitor > Dashboard > **Monitoring Set Status** *(page 11)*
   - Info Center > Reporting > Reports > Monitor > Monitor Set Report
   - Info Center > Reporting > Reports > Monitor > Monitor Action Log

Click the following tabs to define monitor set details.
- **Counter Thresholds** *(page 24)*
- **Services Check** *(page 26)*
- **Process Status** *(page 27)*

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 10)* pane of the Monitor > **Dashboard List** page.

> **Note:** The **Enable Matching** *(page 26)* option applies to counters, services and processes.

Save

Saves changes to a record.

Save As

Saves a record using a new name.

Export Monitor Set...

Click the **Export Monitor Set...** link to display the procedure in XML format in the **Export Monitor Sets** popup window. You can copy it to the clipboard or download it to a text file.

Counter Thresholds

Monitor > Edit > Monitor Sets
- Select a monitor set in a folder, then Counter Thresholds

The **Counter Thresholds** tab defines alert conditions for all performance objects/instances/counters associated with a monitor set. These are the same performance objects, instances and counters displayed when you run `PerfMon.exe` on a Windows machine.

> Note: The **Enable Matching** *(page 26)* option applies to counters, services and processes.

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.

Select Page

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

Edit icon

Click the edit icon next to row to edit the row.

Delete Icon

Click the delete icon ✗ to delete this record.

Add / Edit

Click **Add** or the edit icon to use a wizard that leads you through the six steps required to add or edit a performance counter.
1. Select a **Object**, **Counter** and, if necessary, an **Instance** using their respective drop-down lists.
   - If only one instance of a performance object exists, the **Instance** field can usually be skipped.

➢ The drop-down lists used to select performance objects, counters, and instances are based on the "master list" maintained using the **Monitor Lists** *(page 18)* page. If an object/instance/counter does not display in its respective drop-down list, you can add it manually using **Add Object**, **Add Counter**, and **Add Instance**.

➢ Whatever the range of counter instances specified by a monitor set, the **Monitor Log** *(page 79)* page only displays instances that exist on a specific machine. Newly added counter instances—for example, adding a removable disk to a machine—will start being displayed on the **Monitor Log** page soon after they are discovered, if included in the range specified for monitoring by a monitor set.

➢ When multiple instances exist, you can add an instance called `_Total`. The `_Total` instance means you want to monitor the *combined* value of all the other instances of a performance object *as a single counter*.

➢ When multiple instances exist, you can add a counter instance called `*ALL` to the list of instances supported using the **Monitor Lists** *(page 18)* > **Counter Instance** tab. Once added to the counter you want to work with, the `*ALL` value will display in the drop-down list of instances associated with that counter. The `*ALL` instance means you want to monitor all instances for the same performance object *using individual counters*.

2. Optionally change the default counter object **Name** and **Description**.

3. Select the log data collected. If the returned value is numeric, you can minimize unwanted log data by setting a collection operator just over or just under the collection threshold.

   ➢ **Collection Operator** - For character string return values, the options are `Changed`, `Equal` or `NotEqual`. For numeric return values, the options are `Equal`, `NotEqual`, `Over`, or `Under`.

   ➢ **Collection Threshold** - Set a fixed value that the returned value is compared to, using the selected **Collection Operator**, to determine what log data is collected.

   ➢ **Sample Interval** - Defines how frequently the data is sent by the agent to the Kaseya Server.

4. Specify when an alert condition is encountered.

   ➢ **Alarm Operator** - For character string return values, the options are `Changed`, `Equal` or `NotEqual`. For numeric return values, the options are `Equal`, `NotEqual`, `Over` or `Under`.

   ➢ **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alert condition is encountered.

   ➢ **Duration** - Specify the time the returned values must continuously exceed the alarm threshold to generate the alert condition. Many alert conditions are only alarming if the level is sustained over a long period of time.

   ➢ **Ignore additional alarms for** - Suppress additional alert conditions for this same issue for this time period. This reduces the confusion of many alert conditions for the same issue.

5. **Warn when within X% of alarm threshold** - Optionally display a warning alert condition when the returned value is within a specified percentage of the **Alarm Threshold**. The warning icon is a yellow traffic light icon 🟡.

6. Optionally activate a **trending alarm**. Trending alarms use historical data to predict when the next alert condition will occur.

   ➢ **Trending Activated?** - If yes, a linear regression trendline is calculated based on the last 2500 data points logged.

   ➢ **Trending Window** - The time period used to extend the calculated trendline into the future. If the predicted trendline exceeds the alarm threshold within the future time period specified, a trending alert condition is generated. Typically a trending window should be set to the amount of time you need to prepare for an alert condition, if it occurs. Example: a user may want 10 days notice before a hard drive reaches the alert condition, to accommodate ordering, shipping and installing a larger hard drive.

   ➢ **Ignore additional trending alarms for** - Suppress additional trending alert conditions for this same issue for this time period.

   ➢ Trending alarms display as an orange icon 🟠.

Warning status alert conditions and trending status alert conditions don't create alarm entries in the alarm log, but they change the image of the alarm icon in various display windows. You can generate a trending alarm report using Reports > Monitor.

Next

Moves to the next wizard page.

Previous

Moves back to the previous wizard page.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Enable Matching

The **Enable Matching** checkbox applies to services, counters and processes as follows:

- **Services** *(page 24)* - If checked, no alarms are created if a service specified in the monitor set does not exist on an assigned machine. If unchecked, creates a `Service Does Not Exist` alarm.
  - ➤ Specifying a range of services using the * wildcard character requires **Enable Matching** *(page 26)* be checked.
- **Counters** *(page 24)* - If checked, no alarms are created if a counter specified in the monitor set does not exist on an assigned machine. If unchecked, the counter displays on the **Monitor Log** *(page 79)* page with a **Last Value** of `Not Responding`. No alarm is created.
- **Processes** *(page 27)* - If checked, no alarms are created if a process specified in the monitor set does not exist on an assigned machine. If unchecked, creates a `Process Does Not Exist` alarm.
  - ➤ This change does not take effect on machines already assigned the monitor set until the monitor set is reassigned.

> **Note:** When **Enabled Matching** is used, **Update Lists by Scan** *(page 20)* should be run on at least one machine matching the characteristics of the machines being monitored, to ensure reliable comparisons.

Services Check

Monitor > Edit > Monitor Sets
- Select a monitor set in a folder, then Services Check

The **Services Check** tab defines alarms conditions for a service if the service on a machine ID has stopped, and optionally attempts to restart the stopped service. *The service must be set to automatic to be restarted by a monitor set.*

Select Pages

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

Edit icon

Click the edit icon 📝 next to row to edit the row.

Delete Icon

Click the delete icon ✗ to delete this record.

Add / Edit

Click **Add** or the edit icon 🗒 to maintain a **Services Check** record.

1. **Service** - Selects the service to be monitored from the drop-down list.

   ➢ The drop-down list is based on the "master list" maintained using the **Monitor Lists** *(page 18)* page. If a service does not display in the drop-down list, you can add it manually using **Add Service**.

   ➢ You can add an asterisk (*) wildcard service to the **Name** or **Description** columns in the list of services supported using the **Monitor Lists** *(page 18)* > **Service** tab. Once added, the wildcard service will display in the drop-down list of services. For example specifying the service `*SQL SERVER*` will monitor all services that include the string `SQL SERVER` in the name of the service.

   ➢ You can add a service called `*ALL` to the **Name** or **Description** columns in the list of services supported using the **Monitor Lists** *(page 18)* > **Service** tab. Once added, the `*ALL` value will display in the drop-down list of services. Selecting the `*ALL` service means you want to monitor all services.

   > **Note:** Specifying a range of services using the * wildcard character requires **Enable Matching** *(page 26)* be checked.

2. **Description** - Describes the service and the reason for monitoring.
3. **Restart Attempts** - The number of times the system should attempt to restart the service.
4. **Restart Interval** - The time period to wait between restart attempts. Certain services need more time.
5. **Ignore additional alarms for** - Suppresses additional alert conditions for the specified time period.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Process Status

Monitor > Edit > Monitor Sets
- Select a monitor set in a folder, then Process Status

The **Process Status** tab defines alert conditions based on whether a process has started or stopped on a machine ID.

> **Note:** The **Enable Matching** *(page 26)* option applies to services, counters and processes.

Select Pages

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

Edit icon

Click the edit icon 🗒 next to row to edit the row.

Delete Icon

Click the delete icon ✕ to delete this record.

Add / Edit

Click **Add** or the edit icon 📝 to maintain a **Process Status** record.

1. **Process** - Selects the process to be monitored from the drop-down list. The drop-down list is based on the "master list" maintained using the **Monitor Lists** *(page 18)* page. If a process does not display in the drop-down list, you can add it manually using **Add Process**.
2. **Description** - Describes the process and the reason for monitoring.
3. **Alarm on Transition** - Triggers an alert condition when a process (application) is started or stopped.
4. **Ignore additional alarms for** - Suppresses additional alert conditions for the specified time period.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Monitor Icons

Monitor > Edit > Monitor Sets

- **Select a monitor set in a folder, then Monitor Icons**

The **Monitor Icons** tab selects the monitor icons that display in the **Monitor Log** *(page 79)* 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 a orange traffic light 🟠.
- **Select the Image for Not Deployed Status** - The default icon is a grey traffic light ⚪.

Save

Saves changes to a record.

Upload additional monitoring icons

Select the **Upload additional monitoring icons** link to upload your own icons to the status icon drop-down lists.

Restore

Sets all monitor icons back to their defaults.

SNMP Sets

Monitor > Edit > SNMP Sets

SNMP Sets adds, imports or modifies a SNMP set. A SNMP set is a set of MIB objects used to monitor the performance of SNMP enabled network devices. 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 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 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/9040000/index.asp#1944.htm)*.
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** *(page 84)*. This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using Monitor > **SNMP Log** *(page 93)* or **Dashboard List** *(page 6)*.

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 18)*.
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** *(page 28)*.
- Optionally add an SNMP object using Monitor > **Add SNMP Object** *(page 33)*.
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** *(page 95)*.
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** *(page 94)*.

> **Note:** Certain command line functions from the Net-SNMP suite of applications are used to implement SNMP v1 and SNMP v2c retrieval of information from SNMP capable devices in accordance with all pertinent copyright requirements.

Monitoring using Apple OS X

Apple OS X supports SNMP monitoring. See **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9040000/reqs/index.asp#home.htm)*.

Folder Trees

SNMP sets are organized using two folder trees in the middle pane, underneath **Private** and **Shared** cabinets. Use the following options to manage objects in these folder trees:

Always Available

- **Folder Properties** - Display the name, description, and owner of a folder, and your access rights to the a folder.
- **(Apply Filter)** - Enter text in the filter edit box, then click the funnel icon ▼ to apply filtering to the folder trees. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the folder trees.

When a Folder is Selected

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

  > **Note:** See guidelines for share rights to objects within folder trees in the Folder Rights topic.

- **Add Folder** - Creates a new folder underneath the selected cabinet or folder.

- **Delete Folder** - Deletes a selected folder.
- **Rename Folder** - Renames a selected folder.
- **New SNMP Set** - Opens the **Define SNMP Set** *(page 30)* window to create a new monitor set in the selected folder of the folder tree.
- **Import SNMP Set** - Imports a monitor set.

When a Monitor Set is Selected

- **Delete Monitor Set** - Deletes the selected procedure.

Creating SNMP Sets

1. Select a folder in the middle pane.
2. Click the **New SNMP Set** button.
3. Enter a name.
4. Enter a description.
5. Select an **SNMP type** *(page 95)* from the **Automatic deployment to** drop-down list. If a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/index.asp#10627.htm)* detects this type of SNMP device the system automatically begins monitoring the SNMP device using this SNMP set.
6. Select a group alarm category from the **Group Alarm Column Name** drop-down list. User defined group alarm column names are maintained using the **Monitor Lists** *(page 18)* page. Group alarms display on the **Dashboard List** *(page 6)* page.
7. Click **Save**. The **Define SNMP Set** *(page 30)* window displays.

> **Note:** Sample SNMP sets do not display in the **Assign SNMP** *(page 84)* > **Select SNMP Set** drop-down list. Create a copy of a sample SNMP set by selecting the sample set in **SNMP Sets** *(page 28)* and clicking the **Save As** button. Your copy of the sample SNMP set will display in the drop-down list. In a SaaS-based VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

Define SNMP Set

Monitor > Edit > SNMP Sets > Define SNMP Set
- Select a SNMP set in a folder.

The **Define SNMP Set** page maintains a collection of MIB objects included in a SNMP set.

A SNMP set is a set of MIB objects used to monitor the performance of SNMP enabled network devices. 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 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 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/9040000/index.asp#1944.htm)*.
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** *(page 84)*. This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using   Monitor > **SNMP Log** *(page 93)* or **Dashboard List** *(page 6)*.

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 18)*.
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** *(page 28)*.
- Optionally add an SNMP object using Monitor > **Add SNMP Object** *(page 33)*.
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** *(page 95)*.
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** *(page 94)*.

> **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.

Click the following tabs to define SNMP set details.

- **SNMP Sets** *(page 32)*
- **SNMP Icons** *(page 35)*

SNMP Monitor Set Name

Enter a descriptive name for the SNMP set that helps you identify it in SNMP set lists.

SNMP Monitor Set Description

Describe the SNMP set in more detail. The rationale for the creation of the set is meaningful here; the reason for the creation of the set is sometimes lost over time.

Automatic Deployment to

Selecting a type automatically assigns a newly discovered SNMP device to a **Set SNMP Type** *(page 95)* when performing a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/index.asp#1944.htm)* function.

Group Alarm Column Name

Assign this SNMP set to a **Group Alarm Column Name**. If a SNMP set alarm is triggered, the group alarm it belongs to is triggered as well. Group alarms display in the Group Alarm Status pane of the **Dashboard List** *(page 6)* page.

Save

Saves changes to a record.

Save As

Saves a record using a new name.

Export SNMP Set...

Click the **Export SNMP Set...** link to display the procedure in XML format in the **Export Monitor Sets** popup window. You can copy it to the clipboard or download it to a text file. SNMP sets can be *imported* using the **SNMP Sets** *(page 28)* page.

SNMP Set Details

Monitor > Edit > SNMP Sets > Define SNMP Set
- Select a SNMP set in a folder, then SNMP Sets

The **SNMP Sets** tab enables you to maintain all MIB objects associated with a SNMP set.

Select Page

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

Edit icon

Click the edit icon next to row to edit the row.

Delete Icon

Click the delete icon to delete this record.

Add / Edit

Click **Add** or the edit icon to use a wizard that leads you through the six steps required to add or edit the monitoring of a MIB object.

1. Add the object/version/instance combination required to retrieve information from a SNMP device.
   - **MIB Object** - Select the MIB object. Click **Add Object** *(page 33)* to add a MIB object that currently does not exist on the **Monitor Lists** *(page 18)* page.
   - **SNMP Version** - Select a SNMP version. Version 1 is supported by all devices and is the default. Version 2c defines more attributes and encrypts the packets to and from the SNMP agent. Only select version 2c if you know the device supports version 2c.
   - **SNMP Instance** - The last number of an object ID may be expressed as a table of values instead of as a single value. If the instance is a single value, enter `0`. If the instance is a table of values, enter a range of numbers, such as `1-5,6` or `1,3,7`.

   > Note: If you're not sure what numbers are valid for a particular SNMP instance, select a machine ID that has performed a network scan using Monitoring > **Assign SNMP** *(page 84)*. Click the SNMP Info hyperlink for the device you're interested in. This displays all MIB object IDs and the SNMP instances available for the device.

   - **Value Returned as** - If the MIB object returns a numeric value, you can choose to return this value as a **Total** or a **Rate Per Second**.
2. Optionally change the default MIB object **Name** and **Description**.
3. Select the log data collected. If the returned value is numeric, you can minimize the collection of unwanted log data by setting a collection operator just over or just under the collection threshold.
   - **Collection Operator** - For character string return values, the options are `Changed`, `Equal` or `NotEqual`. For numeric return values, the options are `Equal`, `NotEqual`, `Over` or `Under`.
   - **Collection Threshold** - Set a fixed value that the returned value is compare to, using the selected **Collection Operator**, to determine what log data is collected.
   - **SNMP Timeout** - Specify the number of periods the agent waits for a reply from the SNMP device before giving up. Two seconds is the default.
4. Specify when a SNMP alert condition is triggered.
   - **Alarm Operator** - For character string return values, the options are `Changed`, `Equal` or `NotEqual`. For numeric return values, the options are `Equal`, `NotEqual`, `Over`, `Under` or `Percent Of`.

> ➢ **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alert condition is triggered.
> ➢ **Percent Object** - Selecting the `Percent Of` option for **Alarm Operator** causes this field to display. Enter another object/version/instance in this field whose value can serve as a 100% benchmark for comparison purposes.
> ➢ **Duration** - Specify the time the returned values must continuously exceed the alarm threshold to generate the alert condition. Many alert conditions are only alarming if the level is sustained over a long period of time.
> ➢ **Ignore additional alarms for** - Suppress additional alert conditions for this same issue for this time period. This reduces the confusion of many alert conditions for the same issue.

5. **Warn when within X% of alarm threshold** - Optionally display a warning alert condition in the **Dashboard List** *(page 6)* 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 35)*.

6. Optionally activate a **trending alarm**. Trending alarms use historical data to predict when the next alert condition will occur.

> ➢ **Trending Activated?** - If yes, a linear regression trendline is calculated based on the last 2500 data points logged.
> ➢ **Trending Window** - The time period used to extend the calculated trendline into the future. If the predicted trendline exceeds the alarm threshold within the future time period specified, a trending alert condition is generated. Typically a trending window should be set to the amount of time you need to prepare for an alert condition, if it occurs.
> ➢ **Ignore additional trending alarms for** - Suppresses additional trending alert conditions for this same issue during this time period.
> ➢ By default, trending alarms display as an orange icon ⬤ in the **Dashboard List** *(page 6)* page. You can change this icon using the **SNMP Icons** *(page 35)* tab.
> ➢ Warning status alarms and trending status alarms don't create alarm entries in the alarm log, but they change the image of the alarm icon in various display windows. You can generate a trending alarm report using Reports > Monitor.

Next

Moves to the next wizard page.

Previous

Moves back to the previous wizard page.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Add SNMP Object

`Monitor > Edit > Add SNMP Object`
`Monitor > Edit > SNMP Sets > Define SNMP Set`
• `Select a SNMP set in a folder, then SNMP Sets > Add Object`

When you select objects to include in an SNMP set you're given the opportunity of adding a new SNMP object. This should not be necessary for the most part, because scanning By Network or By Agent retrieves the objects you typically require. But if you do need to add an SNMP object from a MIB file

SNMP Sets

manually you can do so using Monitor > **Add SNMP Object** *(page 33)* 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 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 18)*. This is the list of MIB objects you currently can include in an SNMP set.

If a vendor has supplied you with a MIB file, you can follow these steps:

1. Load the vendor's MIB file by clicking **Load MIB ....** There may be a message stating there are dependent files that need to be loaded first. The vendor may need to provide those also.
2. Click the ⊞ expand icons in the MIB tree—*see the sample graphic below*—and find the desired items to monitor. Select each corresponding check box.
3. Click **Add MIB Objects** to move the selected items from Step 2 into the MIB object list.
4. Configure the settings for monitoring the new SNMP object within an SNMP set as you normally would.
5. The number of MIB objects in the tree can soon become unwieldy. Once the desired MIB objects have been added, the MIB file can be removed.

Load MIB

Click **Load MIB...** to browse for and upload a MIB file. When a MIB object is added, if the system does not already have the following standard MIB II files—required by most MIBs—it loads them automatically: `snmp-tc`, `snmp-smi`, `snmp-conf`, `rfc1213`, `rfc1759`. Once these files are loaded, the MIB tree located at the bottom of the **Add SNMP Object** page can be opened and navigated to find the new objects that the user can select. Most private vendor MIBs are installed under the `Private` folder. *See the sample graphic below*.

> **Note:** The MIB file can be loaded and removed at any time and does *not* affect any MIB objects that are used in SNMP sets.

MIB Tree

The MIB tree represents all MIB file objects that are currently loaded for the user to select from.

34
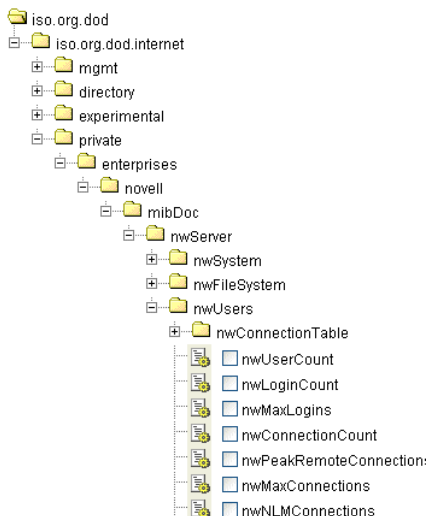
Add MIB Objects

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 30)*.

Remove MIB

After selections have been made the MIB file can be removed. The size of the MIB tree can become so large that it is hard to navigate. Click **Remove MIB** to clean that process up.

SNMP Icons

Monitor > SNMP Sets
- Select a SNMP set in a folder, then SNMP Icons

The **SNMP Icons** tab selects the SNMP icons that display in the **Dashboard List** *(page 6)* 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 a orange traffic light 🟠.
- **Select the Image for Not Deployed Status** - The default icon is a grey traffic light ⚪.

Save

Saves changes to a record.

Upload additional monitoring icons

Select the **Upload additional monitoring icons** link to upload your own icons to the status icon drop-down lists.

Restore

Sets all SNMP icons back to their defaults.

Alerts

Monitor > Agent Monitoring > Alerts

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

> **Note:** Monitor Sets represent a more complex method for monitoring alert conditions. Typical alert conditions should be defined using the **Alerts** page.

Select Alert Function

Select an alert type using the **Select Alert Function** drop-down list.
- **Summary** *(page 36)*
- **Manage Agents** *(page 37)*
- **Application Changes** *(page 40)*
- **Get Files** *(page 43)*

- **Hardware Changes** *(page 45)*
- **Low Disk** *(page 47)*
- **Agent Procedure Failure** *(page 50)*
- **Protection Violation** *(page 52)*
- **New Agent Installed** *(page 54)*
- **Patch Alert** *(page 56)*
- **Backup Alert** *(page 59)*
- **System** *(page 63)*

Alerts - Summary

Monitor > Agent Monitoring > Alerts *(page 35)*
- Select `Summary` from the Select Alert Function drop-down list

The **Alerts - Summary** (page 36) page shows what alerts are enabled for each machine. You can apply or clear settings or copy enabled alerts settings. Specifically you can:

- Apply or clear settings for alarm, ticket and email notification *for all enabled alert types at one time* on selected machines.
- **Copy** all the enabled alert settings from a selected machine ID or machine ID template and apply them to multiple machine IDs.

> **Note:** You can only modify or clear alerts initially enabled using the **Copy** option or else by *using the other alerts pages*.

Although you can not assign   agent procedures using this page, agent procedure assignments are displayed in the paging area.

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.

- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Copy

Only active when **Summary** is selected. **Copy** takes all the alert type settings for a single machine ID, selected by clicking **Copy alert settings from <machine_ID> to all selected machine IDs**, and applies these same settings to all other checked machine IDs.

Select All/Unselect All

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

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

Alert Type

Lists all alert types you can assign to a machine ID using the Monitor > **Alerts** *(page 35)* page. Displays any agent procedure assignments for this machine ID.

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

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

Email Address

A comma separated list of email addresses where notifications are sent. The word `disabled` displays here if no alerts of this alert type are assigned to this machine ID.

Alerts - Agent Status

Monitor > Agent Monitoring > Alerts *(page 35)*
- Select `Agent Status` from the Select Alert Function drop-down list

The **Alerts - Agent Status** (page 37) page alerts when an agent is offline, first goes online, or someone

has disabled remote control on the selected machine.

Agent Online/Offline Alerts

Offline alerts are triggered when the last check-in time of an agent exceeds the specified alert value. For example, the agent process may have been terminated or the agent may not be able to connect to the network, or the machine the agent is running on may be powered down. Once an agent re-establishes connection to the Kaseya Server, an online alert, if configured, can also be triggered. An agent online alert only occurs if an agent offline alert has also been set for the same machine.

> **Note:** When ever the Kaseya Server service stops, the system suspends all agent online/offline alerts. If the Kaseya Server stops for more than 30 seconds, then agent online/offline alerts are suspended for one hour after the Kaseya Server starts up again. Rather than continuously try to connect to the Kaseya Server when the Kaseya Server is down, agents go to sleep for one hour after first trying to connect a couple times. The one hour alert suspension prevents false agent offline alerts when the Kaseya Server starts back up.

Passing Alert Information to Emails and Procedures

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

- **1 - Alert when single agent goes off-line**
- **2 - Alert when users disable remote control**
- **3 - Alert when agent first goes online** - An agent online alert only occurs if an agent offline alert has also been set for the same machine.
- **4 - Alert when multiple agents in the same group go off-line** - If more than one offline alert is triggered at the same time, email notification is consolidated by group.

> Note: Changing this email alarm format changes the format for all Agent Status alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🔴 in a numbered column indicates   a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3	4
<at>	#at#	alert time	🔴	🔴	🔴	🔴
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🔴	🔴	🔴	🔴
<gr>	#gr#	group ID	🔴	🔴	🔴	🔴
<id>	#id#	machine ID	🔴	🔴	🔴	
<mc>	#mc#	number of machines going offline				🔴
<ml>	#ml#	list of multiple machines going offline				🔴
<qt>	#qt#	offline time / online time / time remote disabled	🔴	🔴	🔴	🔴
	#subject#	subject text of the email message, if an email was sent in response to an alert	🔴	🔴	🔴	🔴

	#body#	body text of the email message, if an email was sent in response to an alert	🔴	🔴	🔴	🔴

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Agent has not checked in for <N> <periods>

If checked, an alert is triggered if the agent has not checked in for the specified number of periods.

Alert when agent goes online

If checked, an alert is triggered if the agent goes online

Alert when user disables remote control

If checked, an alert is triggered if the user disables remote control

Select All/Unselect All

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- 🔵 An agent icon adorned with a red clock badge is a temporary agent.

Edit Icon

Click a row's edit icon 📝 to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

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

Email Address

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

Time Offline

Displays the number of periods a machine ID must be off-line before an alert condition occurs.

Rearm Time

The number of periods to ignore additional alert conditions after the first one is reported. This prevents creating multiple alarms for the same problem.

Agent Goes Online

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

RC Disabled

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

Alerts - Application Changes

Monitor > Agent Monitoring > Alerts *(page 35)*
- Select `Application Changes` from the Select Alert Function drop-down list.
- Similar information is provided using Audit > Add/Remove and Reports > Software.

The **Alerts Application Changes** (page 40) page alerts when a new application is installed or removed on selected machines. You can specify the directories to exclude from triggering an alert. This alert is based on the latest audit.

Passing Alert Information to Emails and Procedures

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

- **Alert when application list change**

Note: Changing this email alarm format changes the format for all `Application Changes` alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column 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 parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Procedure after alert

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
- Click Format Email to display the Format Alert Email popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If Remove is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the From Address using System > Outbound Email.

Alert when audit detects New application installed

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

Alert when audit detects Existing application deleted

If checked, an alert condition is encountered when a new application is removed.

Exclude directories

You can specify the directories to exclude from triggering an alert. The exclude path may contain the wildcard asterisk (*) character.   Excluding a folder excludes all subfolders. For example, if you exclude `*\windows\*`, c:\Windows and all subfolders are excluded. You can add to the current list of applications, replace the current application list or remove the existing application list.

Select All/Unselect All

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- An agent icon adorned with a red clock badge is a temporary agent.

Edit Icon

Click a row's edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

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

Email Address

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

Installed Apps

Displays a checkmark ✔ if an alert is sent when an application is installed.

Removed Apps

Displays a checkmark ✔ if an alert is sent when an application is removed.

(Exclude)

Lists directories excluded from sending an alert when an application is installed or removed.

Alerts - Get Files

Monitor > Agent Monitoring > Alerts *(page 35)*

- Select `Get Files` from the Select Alert Function drop-down list

The **Alerts - Get File** (page 43) page alerts when a procedure's **getFile()** or **getFileInDirectoryPath()** command executes, uploads the file, and the file is now different from the copy previously stored on the Kaseya Server. If there was no previous copy on the Kaseya Server, the alert is created. Once defined for a machine ID, the same **Get File** alert is *active for any agent procedure* that uses a **Get File** command and is run on that machine ID.

> Note: The VSA issues the alert only if the **send alert if file changed** option has been selected in the procedure. Turn off alerts for specific files in the agent procedure editor by selecting one of the without alerts options.

Passing Alert Information to Emails and Procedures

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

- Alert when file fetched with **Get File** changes from the last fetch
- Alert when file fetched with **Get File** is unchanged from last fetch

> Note: Changing this email alarm format changes the format for all `Get Files` alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

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

		<db-vMachine.ComputerName>
<fn>	#fn#	filename
<gr>	#gr#	group ID
<id>	#id#	machine ID
<sn>	#sn#	procedure name that fetched the file
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Procedure after alert

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.
- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Select All/Unselect All

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

Check-in status

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

- 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
- An agent icon adorned with a red clock badge is a temporary agent.

Edit Icon

Click a row's edit icon   to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

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

Email Address

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

Alerts - Hardware Changes

Monitor > **Agent Monitoring** > **Alerts** *(page 35)*
- Select `Hardware Changes` from the Select Alert Function drop-down list

The **Alerts - Hardware Changes** (page 45) page alerts when a hardware configuration changes on the selected machines. Detected hardware changes include the addition or removal of RAM, PCI devices, and disk drives. This alert is based on the latest audit.

Passing Alert Information to Emails and Procedures

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

- **1 - Alert when disk drive or PCI card is added or removed**
- **2 - Alert when the amount of installed RAM changes**

> Note: Changing this email alarm format changes the format for all `Hardware Changes` alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🔴 in a numbered column indicates   a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2
<at>	#at#	alert time	●	●
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	●	●
<gr>	#gr#	group ID	●	●
<ha>	#ha#	list of hardware additions	●	
<hr>	#hr#	list of hardware removals	●	
<id>	#id#	machine ID	●	●
<rn>	#rn#	new RAM size		●
<ro>	#ro#	old RAM size		●
	#subject#	subject text of the email message, if an email was sent in response to an alert	●	●
	#body#	body text of the email message, if an email was sent in response to an alert	●	●

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.
- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.

- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Select All/Unselect All

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

Check-in status

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

- 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
- An agent icon adorned with a red clock badge is a temporary agent.

Edit Icon

Click a row's edit icon 🖉 to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

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

Email Address

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

Alerts - Low Disk

Monitor > Agent Monitoring > Alerts *(page 35)*
- Select `Low Disk` from the Select Alert Function drop-down list

The **Alerts - Low Disk** (page 47) page alerts when available disk space falls below a specified percentage of free disk space. A subsequent low disk alert is not created unless the target machine's low disk space is corrected, or unless the alert is cleared, then re-applied. This alert is based on the

latest audit.

Passing Alert Information to Emails and Procedures

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

- **Alert when disk drive free space drops below a set percent**

> Note: Changing this email alarm format changes the format for all Low Disk alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<df>	#df#	free disk space
<dl>	#dl#	drive letter
<dt>	#dt#	total disk space
<gr>	#gr#	group ID
<id>	#id#	machine ID
<pf>	#pf#	percent free space
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the Email Recipients field. It defaults from System > Preferences.
- Click Format Email to display the Format Alert Email popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If Remove is clicked, all email addresses are removed without modifying any alert parameters.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the From Address using System > Outbound Email.

Send alert when selected machines have less than <N> % free space on any fixed disk partition

An alert is triggered if a machine's free disk space is less than the specified percentage.

Select All/Unselect All

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- An agent icon adorned with a red clock badge is a temporary agent.

Edit Icon

Click a row's edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

- A = Create Alarm
- T = Create Ticket
- S = Run Agent Procedure
- E = Email Recipients

Email Address

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

Alerts - Agent Procedure Failure

Monitor > Agent Monitoring > Alerts *(page 35)*
- Select `Agent Procedure Failure` from the Select Alert Function drop-down list

The **Alerts - Agent Procedure Failure** (page 50) page alerts when an agent procedure fails to execute on a managed machine. For example, if you specify a file name, directory path or registry key in an agent procedure, then run the agent procedure on a machine ID for which these values are invalid, you can be notified about the agent procedure failure using this alerts page.

Passing Alert Information to Emails and Procedures

The following type of alert emails can be sent and formatted:
- **Format email message generated by Agent Procedure Failure alerts**

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

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<em>	#em#	procedure error message
<en>	#en#	procedure name that fetched the file
<gr>	#gr#	group ID
<id>	#id#	machine ID
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Select All/Unselect All

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

Check-in status

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

- 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
- An agent icon adorned with a red clock badge is a temporary agent.

Edit Icon

Click a row's edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

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

Email Address

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

Alerts - Protection Violation

Monitor > Agent Monitoring > Alerts *(page 35)*
- Select `Protection Violation` from the `Select Alert Function` drop-down list

The **Alerts - Protection Violation** (page 52) page alerts when a file is changed or access violation detected on a managed machine. Options include **Distributed file changed on agent and was updated**, **File access violation detected**, and **Network access violation detected**.

Prerequisites

- Agent Procedures > Distribute File
- Agent > File Access
- Agent > Network Access

Passing Alert Information to Emails and Procedures

The following type of alert emails can be sent and formatted:
- **Format email message generated by Protection Violations alerts.**

> Note: Changing this email alarm format changes the format for all `Protection Violation` alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<pv>	#pv#	violation description from Agent Log
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Distributed file changed on agent and was updated

If checked, an alert is triggered when a file distributed using Procedure > Distributed File is changed on the managed machine. The agent verifies the distributed file at every full check-in.

File access violation detected

If checked, an alert is triggered when an attempt is made to access a file specified as blocked using Agent > File Access.

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 Agent > Network Access.

Select All/Unselect All

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

Check-in status

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

   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
- ◉ An agent icon adorned with a red clock badge is a temporary agent.

Edit Icon

Click a row's edit icon 🖉 to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:
- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

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

Alerts - New Agent Installed

Monitor > Agent Monitoring > Alerts *(page 35)*
- Select `New Agent Installed` from the Select Alert Function drop-down list

The **Alerts - New Agent Installed** (page 54) page alerts when a new agent is installed on a managed machine by selected *machine groups*.

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:
- **Agent checked in for the first time**

Note: Changing this email alarm format changes the format for all `New Agent Installed` emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

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

		<db-vMachine.ComputerName>
<ct>	#ct#	time the agent checked in for the first time
<gr>	#gr#	group ID
<id>	#id#	machine ID
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Select All/Unselect All

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

Machine Group

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

Email Address

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

Alerts - Patch Alert

Patch Management > Configure > Patch Alert
Monitor > Agent Monitoring > Alerts (page 35)

- Select `Patch Alert` from the Select Alert Function drop-down list.

The Alerts - Patch Alert (page 56) page alerts for patch management events on managed machines.

- A new patch is available for the selected machine ID.
- A patch installation failed on the selected machine ID.
- The agent credential is invalid or missing for the selected machine ID.
- Windows Auto Update changed.

To Create a Patch Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
   - Create **A**larm
   - Create **T**icket
   - Run **S**cript
   - **E**mail Recipients
2. Set additional email parameters.
3. Set additional patch alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the Apply button.

To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the Clear button.
   The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

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

- **1 - New Patch Available**
- **2 - Patch Install Failed**
- **3 - Patch Approval Policies Updated**
- **4 - Agent Credential Invalid**
- **5 - Windows Auto Update Configuration Changed**

> **Note:** Changing the email alarm format changes the format for all   Patch Alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A ⬤ in a numbered column indicates   a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3	4	5
<at>	#at#	alert time	●	●	●	●	●
<au>	#au#	auto update change					●
<bl>	#bl#	new bulletin list			●		
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	●	●	●	●	●
<fi>	#fi#	failed bulletin ID		●			
<gr>	#gr#	group ID	●	●		●	●
<ic>	#ic#	invalid credential type				●	
<id>	#id#	machine ID	●	●		●	●
<pl>	#pl#	new patch list	●				
	#subject#	subject text of the email message, if an email was sent in response to an alert	●	●	●	●	●
	#body#	body text of the email message, if an email was sent in response to an alert	●	●	●	●	●

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.

- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Patch Alert Parameters

The system can trigger an alert for the following alert conditions for a selected machine ID:

- **New patch is available**
- **Patch install fails**
- **Agent credential is invalid or missing**

> **Note:** An agent **credential** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3492.htm)* is not required to install patches **unless** the machine's File Source is configured as `Pulled from file server using UNC path`. If an agent credential is assigned, it will be validated as a local machine credential without regard to the **File Source** configuration. If this validation fails, the alert will be raised. If the machine's **File Source** is configured as `Pulled from file server using UNC path`, a credential is required. If it is missing, the alert will be raised. If it is not missing, it will be validated as a local machine credential and as a network credential. If either of these validations fails, the alert will be raised.

- **Windows Auto Update changed**

Select All/Unselect All

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- An agent icon adorned with a red clock badge is a temporary agent.

Edit icon

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

Machine.Group ID

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

Approval Policy Updated

Displays as the first row of data. This is a system alert and not associated with any machines. An alert is generated when a new patch is added to all patch policies. An NN-- in the **ATSE** column indicates you cannot set an alert or a ticket for this row. You can specify an email recipient. You can also run an agent procedure on a specified machine. See Approval by Policy.

ATSE

The ATSE response code assigned to machine IDs:
- A = Create **A**larm
- T = Create **T**icket
- S = Run Procedure
- E = **E**mail Recipients

Email Address

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

New Patch

If checked, an alarm is triggered when a new patch is available for this machine ID.

Install Failed

If checked, an alarm is triggered when a patch installation has failed for this machine ID.

Invalid Credential

If checked, an alarm is triggered when the credential is invalid for this machine ID.

Win AU Changed

If checked, an alarm is triggered if the group policy for **Windows Automatic Update** on the managed machine is changed from the setting specified by Patch Management > Windows Auto Update. A log entry in the machine's **Configuration Changes** log is made regardless of this alert setting.

Alerts - Backup Alert

Backup > Backup Alert

Monitor > Agent Monitoring > Alerts *(page 35)*
- Select `Backup Alert` from the Select Alert Function drop-down list

The **Alerts - Backup Alert** (page 59) page alerts for backup events on managed machines.

The list of machine IDs you can select depends on the machine ID / group ID filter and the scope you are using. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove page.

To Create a Backup Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
   - Create **A**larm
   - Create **T**icket
   - Run **S**cript
   - **E**mail Recipients

2. Set additional email parameters.
3. Set additional backup alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.

   The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

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

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

> **Note:** Changing the email alarm format changes the format for all `Backup Alert` emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<be>	#be#	backup failed error message
<bt>	#bt#	backup type
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<im>	#im#	backup image location
<mf>	#mf#	megabytes free space remaining
<sk>	#sk#	backup skip count
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Backup Alert Parameters

The system triggers an alarm whenever the system discovers one of four different backup alert conditions for a selected machine ID:

- **Any Backup Completed** - Alerts when any volume or folder backup completes successfully.
- **Full Backup Completed** - Alerts when a full volume or folder backup completes successfully.
- **Backup Fails -** Alerts when a volume or folder backup stops prior to completion for any reason. Typically, backup fails because the machine is turned off mid-backup or because the network connection to the file server referenced by Image Location is lost.
- **Recurring backup skipped if machine offline <N> times** - Alerts when **Skip if machine offline** is set in Schedule Volumes and the backup is rescheduled the specified number of times because the machine is offline. Use this alert to notify you that backups are not even starting because the machine is turned off at the scheduled volume backup time.
- **Image location free space below <N> MB** - Alerts when the hard disk being used to store the backups is less than a specified number of megabytes.

Three additional parameters can be set:

- **Add** - Adds alert parameters to selected machine IDs when **Apply** is selected without clearing existing parameters.
- **Replace** - Replaces alert parameters on selected machine IDs when **Apply** is selected.
- **Remove** - Clear alert parameters from selected machine IDs. Click the edit icon ▤ next to a machine ID group *first* to select the alert parameters you want to clear.

> **Note:** You may specify different alert email addresses for each backup alert type. This lets you send backup complete alerts to the user and only send failures to the user.

Select All/Unselect All

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

Check-in status

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

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

> **Note:** Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > **Control Machine** page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

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

Email Address

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

Any Complete

If checked, an alarm is triggered when any backup is completed for this machine ID.

Full Complete

If checked, an alarm is triggered when a full backup is 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

- Select System from the Select Alert Function drop-down list

The **Alerts - System** (page 63) page alerts for selected events occurring on the *Kaseya Server*. Selecting the **Alerts - System** page does not display a managed machine list. The events listed only apply to the Kaseya Server. This option only displays for master role users.

Passing Alert Information to Emails and Procedures

The following types of monitoring alert emails can be sent and formatted:
- **1 - Admin account disabled manually by a Master admin**
- **2 - Admin account disabled because logon failed count exceeded threshold**
- **3 - KServer has stopped**
- **4 - Database backup failed**
- **5 - Email reader failed (Ticketing module only)**

> Note: Changing this email alarm format changes the format for all System alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A ● in a numbered column indicates   a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3	4	5
<an>	#an#	disabled VSA user name	●	●			
<at>	#at#	alert time	●	●	●	●	●
<bf>	#bf#	database backup error data				●	
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	●	●	●	●	●
<el>	#el#	email reader error message					●
<fc>	#fc#	value that tripped the failed logon attempt counter	●	●			
<fe>	#fe#	time account re-enables	●	●			
<kn>	#kn#	Kaseya Server IP/name	●	●	●		
<ms>	#ms#	disabled VSA user type (master or standard)	●	●			
	#subject#	subject text of the email message, if an email was sent in response to an alert	●	●			
	#body#	body text of the email message, if an email was sent in response to an alert	●	●			

Apply

Click **Apply** to apply alert parameters to the system.

Clear

Click **Clear** to remove all alert parameters from the system.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Admin account disabled

If checked, an alert is triggered when a VSA user account is disabled, whether manually or automatically.

KServer stopped

If checked, an email notification is triggered when the Kaseya Server stops.

System database backup failed

If checked, an email notification is triggered when the Kaseya Server's database backup fails

Email reader in ticketing failed

If checked, an email notification is triggered if the Ticketing > Email Reader fails.

System alerts sent to

Displays the email recipients who are sent system alerts.

Event Log Alerts

Monitor > Agent Monitoring > Event Log Alerts

The **Event Log Alerts** page alerts when an event log entry for a selected machine matches a specified criteria. After selecting the **event log type**, you can filter the alert conditions specified by **event set** and by **event category**. You then set the alert action to take in response to the alert condition specified.

> Note: You can display event logs directly. On a Windows machine click **Start**, then click **Control Panel**, then click **Administrative Tools**, then click **Event Viewer**. Click **Application**, **Security** or **System** to display the events in each log.

Event Sets

Because the number of events in Windows events logs 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 entry has to match all the field filters of a condition to be considered a match.

A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to. For details on how to configure event sets, see Monitor > Event Log Alerts > **Edit Event Sets** *(page 67)*.

Sample Event Sets

A growing list of sample event sets are provided. The names of sample event sets begin with ZC. You can modify sample event sets, but its better practice to copy a sample event set and customize the copy. Sample event sets are subject to being overwritten every time the sample sets are updated during a maintenance cycle.

Global Event Log Black List

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

Flood Detection

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

Monitor Wizard Icon for Event Sets

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

Select a log entry, then click the **Setup Event Log Monitor** to create a new event set criteria based on that log entry. The new event set criteria can be added to any new or existing event set. The new or changed event set is immediately applied to the machine that served as the source of the log entry. Changing an existing event set affects all machines assigned to use that event set. The monitor wizard icon displays in:

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

See Monitor > **Event Log Alerts** *(page 64)* for a description of each field shown in the wizard.

Configuring and Assigning Event Log Alerts

1. Optionally enable event logging for the machines you want to monitor using Agent > Event Log Settings. **Event categories** highlighted in red (EWISFCV) indicate these event categories are not collected by the VSA.

   > Note: If NO or ALL event logs types and categories are collected for a machine, then event log alerts are generated for that machine. If SOME event log types and categories are collected for a machine, then NO event log alerts are generated.

2. Select the **event set**, the **event log type** and other parameters using the Event Log Alerts > Assign Event Set header tab.

3. Optionally click the **Edit** button on the **Assign Event Set** header tab to **create or change the alert conditions for the event sets** *(page 67)* you assign.

4. Specify the actions to take in response to an alert condition using the Event Log Alerts > **Set Alert Actions** *(page 67)* header tab.

5. Optionally click the **Format Email** button on **Set Alert Actions** header tab to **change the format of mail alerts for event sets** *(page 67)*.

6. Select the machines an event set should be applied to.

7. Click the **Apply** button.

Actions

- **Apply** - Applies a selected events set to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.
- **Clear** - Removes selected event set from selected machine IDs.
- **Clear All** - Removes all event set settings from selected machine IDs.

Paging Area

The paging area displays the same columns whichever header tab is selected.

- **Select All/Unselect All** - Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.
- **Check-in status** - These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

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

- **Machine.Group ID** - The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.
- **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:
  - ➢ A = Create **A**larm
  - ➢ T = Create **T**icket
  - ➢ S = Run Agent Procedure
  - ➢ E = **E**mail Recipients
- **EWISFCV** - The event category being monitored.
- **Email Address** - A comma separated list of email addresses where notifications are sent.
- **Event Set** - The event set assigned to this machine ID. Multiple events sets can be assigned to the same machine ID.
- **Interval** - The number of times an event occurs within a specified number of periods. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** option is selected. Displays `Missing` if the **Alert when this event doesn't occur within <N> <periods>** option is selected. Displays `1` if the **Alert when this event occurs once** is selected.

- **Duration** - The number of periods an event must occur to trigger an alert condition. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** or **Alert when this event doesn't occur within <N> <periods>** options are selected.
- **Re-Arm** - Displays the number of periods to wait before triggering any new alert conditions for the same combination of event set and event category. Applies only if a re-arm period greater than zero is specified using **Ignore additional alarms for <N> <periods>**.

Set Alert Actions tab

Monitor > Agent Monitoring > Event Log Alerts > Set Alert Action tab

Use the **Set Alert Action** tab to specify the actions to take in response to an event set alert condition. You can also select machines and assign events sets when this header tab is selected.

- **Create Alarm** - If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.
- **Create Ticket** - If checked and an alert condition is encountered, a ticket is created.
- **Run Script** - If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.
- **Email Recipients** - If checked and an alert condition is encountered, an email is sent to the specified email addresses.
  - ➤ The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
  - ➤ Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
  - ➤ If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
  - ➤ If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
  - ➤ If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
  - ➤ Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Edit Event Sets

Monitor > Agent Monitoring > Event Log Alerts *(page 64)*

- 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 entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to.

> **Note:** Normally, if two conditions are added to an event set, they are typically interpreted as an OR statement. If either one is a match, the alert is triggered. The exception is when the **Alert when this event doesn't occur within <N> <periods>** option is selected. In this case the two conditions should be interpreted as an AND statement. Both must *not* happen within the time period specified to trigger an alert.

> **Note:** You can display event logs directly. On a Windows machine click **Start**, then click **Control Panel**, then click **Administrative Tools**, then click **Event Viewer**. Click **Application**, **Security** or **System** to display the events in that log. Double-click an event to display its **Properties** window. You can copy and paste text from the **Properties** window of any event into **Edit Event Set** fields.

To Create a New Event Set

1. Select the Monitor > **Events Logs Alerts** page.
2. Select an **Event Log Type** from the second drop-down list.
3. Select `<New Event Set>` from the **Define events to match or ignore** drop-down list. The **Edit Event Set** popup window displays. You can create a new event set by:
   - ➢ Entering a new name and clicking the **New** button.
   - ➢ Pasting event set data as text.
   - ➢ Importing event set data from a file.
4. If you enter a new name and click **New**, the **Edit Event Set** window displays the five properties used to filter events.
5. Click **Add** to add a new event to the event set.
6. Click **Ignore** to specify an event that should *not* trigger an alarm.
7. You can optionally **Rename**, **Delete** or **Export Event Set**.

Ignore Conditions

If an event log entry matches one more more **ignore conditions** in an event set, then no alert is triggered *by any event set*, even if multiple conditions in multiple event sets match an event log entry. Because ignored conditions override *all event sets*, it's a good idea to define just one event set for all ignored conditions, so you only have to look in one place if you suspect an ignored condition is affecting the behavior of all your alerts. You must assign the event set containing an ignored condition to a machine ID for it to override all other event sets applied to that same machine ID.

Ignore conditions only override events sharing the same log type. So if you create an "ignore set" for all ignore conditions, it must be applied multiple times to the same machine ID, *one for each log type*. For example, an ignore set applied only as a System log type will not override event conditions applied as Application and Security log type events.

1. Select the Monitor > **Event Log Alerts** page.
2. Check the **Error** checkbox and select `<All Events>` from the event set list. Click the **Apply** button to assign this setting to all selected machine IDs. This tells the system to generate an alert for every error event type. Note the assigned log type.
3. Create and assign an "ignore event set" to these same machine IDs that specifies all the events you wish to ignore. The log type must match the log type in step 2.

Using the Asterisk (*) Wildcard

Include an asterisk (*) wildcard with the text you enter to match multiple records. For example:

```
*yourFilterWord1*yourFilterWord2*
```

This would match and raise an alarm for an event with the following string:

```
"This is a test. yourFilterWord1 as well as yourFilterWord2 are in the description."
```

Exporting and Importing Edit Events

You can export and import event set records as XML files.

- You can *export* an existing event set record to an XML file using the **Edit Event Set** popup window.
- You can *import* an event set XML file by selecting the `<Import Event Set>` or `<New Event Set>` value from the event set drop-down list.

Example:
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<event_sets>
 <set_elements setName="Test Monitor Set" eventSetId="82096018">
   <element_data ignore="0" source="*SourceValue*"
     category="*CategoryValue*" eventId="12345"
     username="*UserValue*" description="*DescriptionValue*"/>
 </set_elements>
</event_sets>
```

Format Email Alerts for Event Sets

Monitor > Agent Monitoring > Event Log Alerts > Set Alert Action > Format Email

This **Format Email Alerts** window specifies the format of emails sent in response to *event set* alert conditions. The following types of alert emails can be formatted using this window:

- **1 - Single event log alert** - Same template applied to all event log types.
- **2 - Multiple event log alerts** - Same template applied to all event log types.
- **3 - Missing event log alert** - Same template applied to all event log types.

> Note: Changing this email alarm format changes the format for all **Event Logs Alerts** alert emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🔴 in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3
<at>	#at#	alert time	🔴	🔴	🔴
<cg>	#cg#	Event category	🔴		
<cn>	#cn#	computer name	🔴		
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🔴	🔴	🔴
<ed>	#ed#	event description	🔴	🔴	
<ei>	#ei#	event id	🔴		
<es>	#es#	event source	🔴		

<et>	#et#	event time	●		
<eu>	#eu#	event user	●		
<ev>	#ev#	event set name	●	●	●
<gr>	#gr#	group ID	●	●	●
<id>	#id#	machine ID	●	●	●
<lt>	#lt#	log type (Application, Security, System)	●	●	●
<tp>	#tp#	event type - (Error, Warning, Informational, Success Audit, or Failure Audit)	●		
	#subject#	subject text of the email message, if an email was sent in response to an alert	●	●	●
	#body#	body text of the email message, if an email was sent in response to an alert	●	●	●

SNMP Traps Alert

Monitor > Agent Monitoring > SNMP Traps Alert

The **SNMP Traps Alert** page configures alerts for a managed machine, acting as a SNMP trap "listener", when it detects an **SNMP trap** message.

When **SNMP Traps Alert** is assigned to a managed machine, a service is started on the managed machine called `Kaseya SNMP Trap Handler`. This service listens for SNMP trap messages sent by SNMP-enabled devices on the same LAN. Each time an SNMP trap message is received by the service, an SNMP trap `Warning` entry is added to the managed machine's `Application` event log. The **source** of these `Application` event log entries is always `KaseyaSNMPTrapHandler`.

> **Note:** Create an event set that includes `KaseyaSNMPTrapHandler` as the **source**. Use asterisks * for the other criteria if you don't want to filter the events any more than that.
>
>
>
> **Note:** SNMP uses the default UDP port 162 for SNMP trap messages. Ensure this port is open if a firewall is enabled.

Event Sets

Because the number of events in Windows events logs 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 entry has to match all the field filters of a condition to be considered a match. A field with an asterisk character (*) means any string, including a zero string, is considered a match. A match of any *one* of the conditions in an event set is sufficient to trigger an alert for any machine that event set is applied to. For details on how to configure event sets, see Monitor > Event Log Alerts > **Edit Event Sets** *(page 67)*.

Creating an SNMP Traps Alert

1. Select the Monitor > **SNMP Traps Alert** page.
2. Select the **Event Set** filter used to filter the events that trigger alerts. Do not select an event set to include *all* SNMP Trap events.
3. Check the box next to the `Warning` **event category**. *No other event categories are used by SNMP Trap Alert.*

> **Note: Event categories** highlighted in red (EWISFCV) indicate these event categories are not collected by the VSA. **Event log alerts are still generated even if event logs are not collected by the VSA.**

4. Specify the *frequency* of the alert condition required to trigger an alert:
   - ➢ **Alert when this event occurs once**.
   - ➢ **Alert when this event occurs <N> times within <N> <periods>**.
   - ➢ **Alert when this event doesn't occur within <N> <periods>**.
   - ➢ **Ignore additional alarms for <N> <periods>**.
5. Click the **Add** or **Replace** radio options, then click **Apply** to assign selected event type alerts to selected machine IDs.
6. Click **Remove** to remove all event based alerts from selected machine IDs.
7. Ignore the **SNMP Community** field. *This option is not yet implemented.*

Passing Alert Information to Emails and Procedures

> **Note:** SNMP Traps Alert shares the same Format Email window with Monitor > **Event Log Alerts** *(page 64)*.

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.
- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.

- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Select All/Unselect All

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

Check-in status

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

- 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
- An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

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

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:

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

EWISFCV

The event category being monitored.

Email Address

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

Event Set

Displays `All Events` if no *SNMP trap event set* was selected, meaning all SNMP trap events are

included.

Interval

The number of times an event occurs within a specified number of periods. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** option is selected. Displays `Missing` if the **Alert when this event doesn't occur within <N> <periods>** option is selected. Displays `1` if the **Alert when this event occurs once** is selected.

Duration

The number of periods and event must occur to trigger an alert. Applies only if the **Alert when this event occurs <N> times within <N> <periods>** or **Alert when this event doesn't occur within <N> <periods>** options are selected.

Re-Arm

Displays the number of periods to wait before triggering any new alerts for the same combination of event set and event category. Applies only if a re-arm period greater than zero is specified using **Ignore additional alarms for <N> <periods>**.

Assign Monitoring

Monitor > Agent Monitoring > Assign Monitoring

The **Assign Monitoring** page creates monitor set alerts for managed machines. An alert is a response to an alert condition. An alert condition exists when a machine's performance succeeds or fails to meet a pre-defined criteria.

Monitor Sets

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

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

1. Optionally update monitor set counter objects, instances and counters manually and review them using **Monitor Lists** *(page 18)*.
2. Create and maintain monitor sets using Monitor > **Monitor Sets** *(page 21)*.
3. Assign monitor sets to machine IDs using Monitor > **Assign Monitoring** *(page 73)*.
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.
6. Review monitor set results using:
   - ➢ Monitor > **Monitor Log** *(page 79)*
   - ➢ Monitor > **Live Counter** *(page 17)*
   - ➢ Monitor > Dashboard > **Network Status** *(page 10)*
   - ➢ Monitor > Dashboard > **Group Alarm Status** *(page 10)*
   - ➢ Monitor > Dashboard > **Monitoring Set Status** *(page 11)*
   - ➢ Info Center > Reporting > Reports > Monitor > Monitor Set Report
   - ➢ Info Center > Reporting > Reports > Monitor > Monitor Action Log

> **Note:** Changes made to a monitor set affect all machine IDs the monitor set is already assigned to, within a couple minutes of the change.

Individualized Monitor Sets

You can *individualize* monitor set settings for a single machine.

1. Using Monitor > **Assign Monitoring**, select a *standard* monitor set using the `<Select Monitor Set>` drop-down list.
2. Assign this standard monitor set to a machine ID. The monitor set name displays in the **Monitor Set** column.
3. Click the individualized monitor set icon ![icon] in the **Monitor Set** column to display the same options you see when defining a **standard monitor set** *(page 21)*. *An individualized monitor set adds an (IND) prefix to the name of the monitor set.*
4. Optionally change the name or description of the individualized monitor set, then click the **Save** button. Providing a unique name and description helps identify an individualized monitor set in reports and log files.
5. Make changes to the monitoring settings of the individualized monitor set and click the **Commit** button. Changes apply only to the single machine the individualized monitor set is assigned to.

> **Note:** Changes to a standard monitor set have no 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 78)* popup window. Use a wizard to define parameters used to calculate alarm threshold values.
3. Assign this standard monitor set, modified by your Auto Learn parameters, to selected machine IDs.

> **Note:** You cannot apply Auto Learn settings to a monitor set that is already assigned to a machine ID. If necessary, clear the existing assignment of the monitor set to the machine ID, then perform steps 1 through 3 above.

Once auto learn is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon ![icon] for a specific machine ID and manually adjust the calculated alarm thresholds values. You can also re-run Auto Learn again, using a new session of actual performance data to re-calculate alarm threshold values.

To Create a Monitor Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
   - Create **A**larm

> ➤ Create **T**icket
> ➤ Run **S**cript
> ➤ **E**mail Recipients

2. Set additional email parameters.
3. Select the monitor set to add or replace.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

To Cancel a Monitor Set Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.
   The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

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

- Monitoring threshold alarm
- Monitoring trending threshold alarm
- Monitoring exit alarm state notification

> **Note:** Changing this email alarm format changes the format for *all* monitor set and SNMP set emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<ad>	#ad#	alarm duration
<ao>	#ao#	alarm operator
<at>	#at#	alert time
<av>	#av#	alarm threshold
<cg>	#cg#	event category
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<dv>	#dv#	SNMP device name
<gr>	#gr#	group ID
<id>	#id#	machine ID
<ln>	#ln#	monitoring log object name
<lo>	#lo#	monitoring log object type: counter, process, object
<lv>	#lv#	monitoring log value
<mn>	#mn#	monitor set name
	#subject#	subject text of the email message, if an email was sent in response to an alert

	#body#	body text of the email message, if an email was sent in response to an alert

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

(Apply Filter)

Enter text in the filter edit box, then click the funnel icon 🔻 to apply filtering to the drop-down list displayed in **Select Monitor Set**. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the set name.

Select Monitor Set

Select monitor sets from the **Select Monitor Set** list, then click the **Apply** button to assign the monitor set to selected machine IDs. You may assign more than one monitor set to a machine ID. Add or edit monitor sets using Monitor > **Monitor Sets** *(page 21)*.

> **Note:** Sample monitor sets do not display in the **Assign Monitoring** *(page 73)* > **Select Monitor Set** drop-down list. Create a copy of a sample monitor set by selecting the sample set in **Monitor Sets** *(page 21)* and clicking the **Save As** button. Your copy of the sample monitor set will display in the drop-down list. In a SaaS-based VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

Add Monitor Set

When a monitor set is assigned to machine IDs, the monitor set is added to the list of monitor sets currently assigned to those machine IDs.

Replace Monitor Set

When a monitor set is assigned to machine IDs, the monitor set replaces all monitor sets already assigned to those machine IDs.

Apply

Applies the selected monitor set to checked machine IDs.

Clear

Clears the assignment of a selected monitor set from selected machine IDs.

Clear All

Clears all monitor sets assigned to selected machine IDs.

Select All/Unselect All

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

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
- An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

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

Monitor Sets

Displays the list of all monitor sets assigned to machine IDs.

- Edit - Always displays next to a monitor set. Click this icon to set header parameters to those matching the selected machine ID.

- Override auto learn values - Displays if Auto Learn is applied to this standard monitor set. Click this icon to display or change the actual values calculated by **Auto Learn** *(page 78)* 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 21)* 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:

- A = Create Alarm
- T = Create Ticket

- S = Run Agent Procedure
- E = Email Recipients

Email Address

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

Auto Learn - Monitor Sets

Monitor > Agent Monitoring > Assign Monitoring > Auto Learn

The **Auto Learn Alarm Thresholds** window maintains auto learn alarm thresholds for monitor sets.

You can enable **Auto Learn** alarm thresholds for any standard monitor set you assign to selected machine IDs. This automatically fine-tunes alarm thresholds based on actual performance data on a per machine basis.

Each assigned machine collects performance data for a specified time period. During that time period no alarms are triggered. At the end of the auto learn session, the alarm threshold for each assigned machine is adjusted automatically based on the actual performance of the machine. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized monitor sets.

Select Page

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

Edit

A list of objects/instance/counters displays for the selected monitor set you want to setup to "auto learn". Click the edit icon to use a wizard that leads you through the three steps required to edit auto learn alarm thresholds.

1. Enable Auto Learn for this object/counter/instance combination, if appropriate, by selecting `Yes - Include`. If `No - Do not include` is selected, no other selections in this wizard are applicable.
   - ➢ **Time Span** - Enter the period of time performance data is collected and used to calculate alarm thresholds automatically. Alarms will not be reported during this time period.
2. Displays the **Object**, **Counter** and, if necessary, the counter **Instance** of the alarm threshold being modified. These options cannot be changed.
3. Enter calculated value parameters.
   - ➢ **Computation** - Select a calculated value parameter. Options include `MIN`, `MAX` or `AVG`. For example, selecting `MAX` means calculate the maximum value collected by an object/counter/instance during the **Time Span** specified above.
   - ➢ **% Increase** - Add this percentage to the **Computation** value calculated above, with the **Computation** value representing 100%. The resulting value represents the alarm threshold.
   - ➢ **Minimum** - Set a minimum value for the alarm threshold. The value is automatically calculated as *two standard deviations below* the calculated **Computation** value, but can be manually overridden.
   - ➢ **Maximum** - Set a maximum value for the alarm threshold. The value is automatically calculated as *two standard deviations above* the calculated **Computation** value, but can be manually overridden.

> **Note:** Once auto learn is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon 🏷 for a specific machine ID and manually adjust the calculated alarm thresholds values. You can also re-run Auto Learn again, using a new session of actual performance data to re-calculate alarm threshold values.

Next

Moves to the next wizard page.

Previous

Moves back to the previous wizard page.

Save

Saves changes to a record.

Cancel

Ignores changes and returns to the list of records.

Monitor Log

Monitor > Agent Monitoring > Monitor Log

- *Clicking the monitoring log icon* 📊 *next to a single alarm for a specific machine ID in the* Monitoring Set Status *(page 11) 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 of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes. If no machine IDs display use Monitor > **Assign Monitoring** *(page 73)* to apply monitor sets to machine IDs.

Select monitoring object to display information

The page displays a list of monitoring objects assigned to the selected machine ID.

View

Select a counter object by clicking the **View** link. The selected row is **bolded.** A selected row displays either as a chart or table.

> **Note:** If a monitoring object cannot be represented by a chart, only the table view is available.

Expand Icon

Click the expand icon ⊞ to display details about a monitoring object.

Refresh Data

Click the refresh icon 🔄 to refresh data when no values display. Applies to non-responsive monitoring.

If your monitor doesn't show any log values, verify the following:

1. Check the sample interval of the counter object. Once a monitor set is deployed counters return values to the monitor log using their specified sample interval. Wait for the sample interval plus the agent check-in interval for the first value to come back.

2. If there are no values returned, check **Counter Thresholds** *(page 24)* for the Monitor Counter commands. If no values on the monitored machine or device meet the collection threshold they will not be inserted into the monitor log.

If a monitor isn't responding, the log displays the message `Monitor Not Responding`. There can be several reasons for no response from the monitor:

- **Counters -** If your monitoring set includes a counter that does not exist on a managed machine, the log displays `Not Responding`. You can troubleshoot the monitoring of counters for a specific machine in two ways:
  - ➢ Use the Monitor > **Update Lists By Scan** *(page 20)* page to scan for all monitor counters and services *for that specific machine ID*.
  - ➢ Connect to the machine managed by this agent, select the **Run** command in the **Start** menu, enter `perfmon.exe`, click **OK**, create a new **Counter Log**, and check for the existence of the counter objects/counters/instances that aren't responding.
  - ➢ A counter value of -998 in the monitor logs indicates the monitor set is returning no data. Check that the the `Performance Logs & Alerts` service in Windows is running. This is a pre-requisite for monitoring of performance counters.
- **Services -** If your monitoring set includes a service that does not exist on a managed machine, the log displays `Service Does Not Exist`.
- **Processes -** If your monitoring set includes a process that does not exist on a managed machine, the log displays `Process Stopped`.
- **Permissions** - Make sure that the permissions for the agent's working directory are set to full access for `SYSTEM` and `NETWORK SERVICE`. This can happen if the agent working directory is placed in the `c:\program files\` or `c:\windows` directories. This is not recommended as these directories have special permissions set by the OS.

Type

The type of monitor object: counter, process or service.

Monitor Set Name

The name of the monitor set.

Object Name

The name of the monitor object.

Last Value

The last value reported.

Bar Chart / Table

Select the **Bar Chart** or **Table** radio option to display data in either format. Only monitor objects of type **Counters** can be displayed in bar chart format.

- A bar chart displays the last 2000 data points at the sample interval rate. The background of the chart displays in red for alarm threshold, yellow for warning threshold and green for no alarm.
- Table log data displays the most current values first and displays alarm and warning icons on log data that falls within these thresholds. See **Define Monitor Set** *(page 30)* for more information.

Start Date / Display Last

Display log data for the last number of intervals selected since the specified date. If no date is specified, the current date is used. For example, if you select **Display Last** 500 minutes, each bar in the chart represents 1 minute.

Save View

You can save the **Display Last** value for a specific monitor object.

Log rows per Page

These fields only display in Table format. Select the number of rows to display per page.

Display Value Over / Under Value

These fields only display in Table format. Filter the table rows displayed by filtering log data that is over or under the value specified.

Refresh

Click the refresh button after making filter changes.

Select Page

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

System Check

Monitor > External Monitoring > System Check

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

To Create a System Check Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
    ➢ Create **A**larm
    ➢ Create **T**icket
    ➢ Run **S**cript
    ➢ **E**mail Recipients
2. Set additional email parameters.
3. Set additional system-check parameters. You may check multiple systems using the same machine ID.
4. Check the machine IDs to apply the alert to.
5. Click the Apply button.

To Cancel a System Check Alert

1. Select the machine ID checkbox.
2. Click the Clear button.
    The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

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

▪ System check alert

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<p1>	#p1#	address checked
<p2>	#p2#	additional parameter
<sc>	#sc#	system check type
<scn>	#scn#	system check custom name
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click **Clear** to remove all parameter settings from selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.

- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

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. 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

🔵 An agent icon adorned with a red clock badge is a temporary agent.

Delete

Click the delete icon ✖ to delete a system check.

Edit Icon

Click a row's edit icon 📝 to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

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

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

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

Email Address

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

Type

The type of system check:

- Web Server
- DNS Server
- Port Connection
- Ping
- Custom

Interval

The interval for the system check to recur.

Duration

The number of periods the system check alarm is suppressed, after the initial problem is *detected.* This prevents triggering an alarm for a temporary problem.

ReArm

The number of periods to ignore additional alert conditions after the first one is reported. This prevents creating multiple alarms for the same problem.

Assign SNMP

Monitor > SNMP Monitoring > Assign SNMP

The **Assign SNMP** page creates SNMP alerts for SNMP devices discovered using the By Network or **By Agent** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/index.asp#1944.htm)* pages. An alert is a response to an alert condition.

A SNMP set is a set of MIB objects used to monitor the performance of SNMP enabled network devices. 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 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 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/9040000/index.asp#1944.htm)*.
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** *(page 84)*. This can include quick, standard, individualized or auto learn SNMP sets.
3. Display SNMP alarms using   Monitor > **SNMP Log** *(page 93)* or **Dashboard List** *(page 6)*.

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 18)*.
- Optionally maintain SNMP sets using Monitor > **SNMP Sets** *(page 28)*.
- Optionally add an SNMP object using Monitor > **Add SNMP Object** *(page 33)*.
- Optionally assign a SNMP type to an SNMP device manually using Monitor > **Set SNMP Type** *(page 95)*.
- Optionally write values to SNMP devices using Monitor > **Set SNMP Values** *(page 94)*.

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 ![icon] in the **SNMP Info / SNMP Set** column to display the same options you see when defining a **standard SNMP set** *(page 28)*. *An individualized SNMP set adds an (IND) prefix to the name of the SNMP set.*
4. Make changes to your new individualized SNMP set. These changes apply only to the single SNMP device it is assigned to.

> Note: Changes to a standard SNMP set have no affect on individualized SNMP sets copied from it.

Auto Learn Alarm Thresholds for SNMP Sets

You can enable **Auto Learn** alarm thresholds for any standard SNMP set or quick set you assign to selected SNMP devices. This automatically fine-tunes alarm thresholds based on actual performance data on a per SNMP device basis.

Each assigned SNMP device generates performance data for a specified time period. During that time period no alarms are triggered. At the end of the **Auto Learn** session, the alarm threshold for each assigned SNMP device is adjusted automatically based on the actual performance of the SNMP device. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another

session of **Auto Learn** again. **Auto Learn** cannot be used with individualized SNMP sets.

To apply **Auto Learn** settings to selected SNMP devices:

1. Select a *standard* SNMP set using the `<Select SNMP Set>` drop-down list. Or click the edit icon of an SNMP set already assigned to a device to populate the `<Select SNMP Set>` drop-down list with its identifier.

2. Click **Auto Learn** to display the **Auto Learn** *(page 78)* popup window. Use a wizard to define parameters used to calculate alarm threshold values.

3. Assign this standard SNMP set, modified by your **Auto Learn** parameters, to selected SNMP devices, if not already assigned.

Once **Auto Learn** is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon 🌡 for a specific SNMP device and manually adjust the calculated alarm threshold values. You can also re-run **Auto Learn** again, using a new session of actual performance data to re-calculate alarm threshold values.

Quick Sets

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **network is scanned** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/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/9040000/index.asp#1944.htm)*.

2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** *(page 84)*.

3. Click the hyperlink underneath the name of the device, called the **SNMP info** *(page 90)* link, in the **Assign SNMP** page to display a dialog.

   ➢ Click **Discovered MIB Objects** and select one or more of the MIB objects that were discovered on the SNMP device you just selected.

   ➢ Click **Quick Set Items** and, if necessary, edit the alarm thresholds for selected MIB objects.

   ➢ Enter a name after the **(QS)** prefix in the header of the dialog.

   ➢ Click the **Apply** button to apply the quickset to the device.

4. Display SNMP monitoring data returned by the quick set using Monitor > **SNMP Log** *(page 93)*, the same as you would for any other standard SNMP set.

5. Optionally maintain your new quick set using Monitor > SNMP Sets.

To Create a SNMP Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:

   ➢ Create **A**larm

   ➢ Create **T**icket

   ➢ Run **S**cript

   ➢ **E**mail Recipients

2. Set additional email parameters.

3. Select the SNMP set to add or replace.

4. Check the SNMP device to apply the alert to.

5. Click the **Apply** button.

To Cancel a SNMP Alert

1. Select the SNMP device checkbox.
2. Click the **Clear** button.
   The alert information listed next to the SNMP device is removed.

Passing Alert Information to Emails and Procedures

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

- Monitoring threshold alarm
- Monitoring trending threshold alarm
- Monitoring exit alarm state notification

> **Note:** Changing this email alarm format changes the format for *all* monitor set and SNMP set emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert.

Within an Email	Within a Procedure	Description
<ad>	#ad#	alarm duration
<ao>	#ao#	alarm operator
<at>	#at#	alert time
<av>	#av#	alarm threshold
<cg>	#cg#	event category
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<dv>	#dv#	SNMP device name
<gr>	#gr#	group ID
<id>	#id#	machine ID
<ln>	#ln#	monitoring log object name
<lo>	#lo#	monitoring log object type: counter, process, object
<lv>	#lv#	monitoring log value
<mn>	#mn#	monitor set name
	#subject#	subject text of the email message, if an email was sent in response to an alert
	#body#	body text of the email message, if an email was sent in response to an alert

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

If checked and an alert condition is encountered, an email is sent to the specified email addresses.
- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

(Apply Filter)

Enter text in the filter edit box, then click the funnel icon to apply filtering to the drop-down list displayed in **Select SNMP Set**. Filtering is case-insensitive. Match occurs if filter text is found anywhere in the set name.

Select SNMP Set

Select SNMP sets from the **Select SNMP Set** list, then click the **Apply** button to assign the SNMP set to selected machine IDs. You may assign more than one SNMP set to a machine ID. Add or edit SNMP sets using Monitor > **SNMP Sets** *(page 28)*.

> **Note:** Sample SNMP sets do not display in the **Assign SNMP** *(page 84)* > **Select SNMP Set** drop-down list. Create a copy of a sample SNMP set by selecting the sample set in **SNMP Sets** *(page 28)* and clicking the **Save As** button. Your copy of the sample SNMP set will display in the drop-down list. In a SaaS-based VSA, **Save** and **Save As** buttons are available. You can make changes to the sample set and use it immediately, because it does not get refreshed.

Add Monitor Set

Adds the selected SNMP set to selected SNMP devices.

Replace Monitor Set(s)

Adds the selected SNMP set to selected SNMP devices and removes all other SNMP sets currently assigned to selected SNMP device.

Edit SNMP List

Manually add a new SNMP device or edit the information of existing SNMP devices. Enter the IP and MAC address, name and description for the SNMP device. You can also enter the `sysDescr`, `sysLocation` and `sysContact` values typically returned by polling.

Apply

Applies the selected SNMP set to selected SNMP devices.

Clear

Clears the assignment of a selected SNMP set from selected SNMP devices.

Clear All

Clears all SNMP sets assigned to selected SNMP devices.

Select All/Unselect All

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

Name / Type

The name returned by the ARP protocol when a network scan 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 network scan is performed. Click the **SNMP Info** *(page 90)* 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 78)* 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 28)* 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:
- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

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

SNMP Quick Sets

Monitor > SNMP Monitoring > Assign SNMP > SNMP Info link

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **network is scanned**

(http://help.kaseya.com/webhelp/EN/KDIS/9040000/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/9040000/index.asp#1944.htm).
2. Assign SNMP sets to discovered devices using Monitor > **Assign SNMP** *(page 84)*.
3. Click the hyperlink underneath the name of the device, called the **SNMP info** *(page 90)* link, in the **Assign SNMP** page to display a dialog.
   ➢ Click **Discovered MIB Objects** and select one or more of the MIB objects that were discovered on the SNMP device you just selected.
   ➢ Click **Quick Set Items** and, if necessary, edit the alarm thresholds for selected MIB objects.
   ➢ Enter a name after the **(QS)** prefix in the header of the dialog.
   ➢ Click the **Apply** button to apply the quickset to the device.
4. Display SNMP monitoring data returned by the quick set using Monitor > **SNMP Log** *(page 93)*, the same as you would for any other standard SNMP set.
5. Optionally maintain your new quick set using Monitor > SNMP Sets.

Use the following tabs on the **SNMP Info link** page to configure an SNMP quick set.

Discovered MIB Objects tab

The **Discovered MIB Objects** tab lists all objects sets discovered by the last SNMP "walk" that apply to the selected SNMP device. You can use this tab to add objects and instances to an SNMP quick set for this device.

- **Add Instance** - Click to add this instance of this object to an SNMP "quick set" displays in the **SNMP Set** tab of this same window.
- **Add All Instances** - Click to add all instances of this object to an SNMP "quick set" displays in the **SNMP Set** tab of this same window.
- **SNMP Object** - The name of the SNMP object. If no name is provided for the object, the OID numerical designation displays.
- **Instance** - The instance of the object. Many objects have multiple instances, each of which have a different value. For example, the different instances could be ports on a router, or paper trays on a printer. The field is blank if the last number of an OID is zero, which indicates there can only be one member of this object. If an instance is not blank, or any number other than 0, than more than one "instance" of this same object exists for the device. You can specify monitoring of multiple instances of an object by entering a range of numbers, such as `1-5,6` or `1,3,7`. You can also enter `All`.
- **Current SNMP Value** - The value returned by the object/instance combination by the latest SNMP "walk".

Quick Set Items tab

The **Quick Set Items** tab configures the objects and instances selected to be included in your SNMP quick set. Click the edit icon 🖫 to define SNMP monitoring attributes for the selected objects. You can

also use the **Add** button to add a new object and set these same attributes.

- **SNMP Object** - The SNMP object name or OID number.
- **SNMP Instance** - The last number of an object ID may be expressed as a table of values instead of as a single value. If the instance is a single value, enter `0`. If the instance is a table of values, enter a range of numbers, such as `1-5,6` or `1,3,7`. You can also enter `All`.
- **Alarm Operator** - For character string return values, the options are `Changed`, `Equal` or `NotEqual`. For numeric return values, the options are `Equal`, `NotEqual`, `Over`, or `Under.`
- **Alarm Threshold** - Set a fixed value that the returned value is compared to, using the selected **Alarm Operator**, to determine when an alarm is triggered.
- **Value Returned as** - If the MIB object returns a numeric value, you can choose to return this value as a **Total** or a **Rate Per Second**.
- **Current SNMP Value** - The value returned by the object/instance combination by the latest SNMP "walk".
- SNMP Sets tab

SNMP Icons tab

- Customize the alarm icons for this *specific SNMP quick set*. See **SNMP Icons** *(page 35)* for a general explanation of how to use this page.

Select Page

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

Commit

Save changes made to this page.

Cancel

Ignore any changes made to this page and return to the SNMP Sets list.

Clear

Clears all SNMP objects from all tabs. The default list of objects repopulates the **Discover Objects Set** tab a few minutes later.

Auto Learn - SNMP Sets

Monitor > SNMP Monitoring > Assign SNMP > Auto Learn

The **Auto Learn Alarm Thresholds** window maintains auto learn alarm thresholds for SNMP sets.

You can enable **Auto Learn** alarm thresholds for any standard SNMP set or quick set you assign to selected SNMP devices. This automatically fine-tunes alarm thresholds based on actual performance data on a per SNMP device basis.

Each assigned SNMP device generates performance data for a specified time period. During that time period no alarms are triggered. At the end of the **Auto Learn** session, the alarm threshold for each assigned SNMP device is adjusted automatically based on the actual performance of the SNMP device. You can manually adjust the alarm threshold values calculated by **Auto Learn** or run another session of **Auto Learn** again. **Auto Learn** cannot be used with individualized SNMP sets.

To apply **Auto Learn** settings to selected SNMP devices:

1. Select a *standard* SNMP set using the `<Select SNMP Set>` drop-down list. Or click the edit icon of an SNMP set already assigned to a device to populate the `<Select SNMP Set>` drop-down list with its identifier.

2. Click **Auto Learn** to display the **Auto Learn** *(page 78)* popup window. Use a wizard to define parameters used to calculate alarm threshold values.

3. Assign this standard SNMP set, modified by your **Auto Learn** parameters, to selected SNMP devices, if not already assigned.

Once **Auto Learn** is applied to a machine ID and runs for the specified time period, you can click the override auto learn icon 👒 for a specific SNMP device and manually adjust the calculated alarm threshold values. You can also re-run **Auto Learn** again, using a new session of actual performance data to re-calculate alarm threshold values.

Select Page

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

Edit

Click the edit icon 📝 to use a wizard that leads you through the three steps required to edit auto learn alarm thresholds.

1. Enable Auto Learn for this SNMP object, if appropriate, by selecting `Yes - Include`. If `No - Do not include` is selected, no other selections in this wizard are applicable.
   - ➢ **Time Span** - Enter the period of time performance data is collected and used to calculate alarm thresholds automatically. Alarms will not be reported during this time period.

2. Displays the **SNMP Object** of the alarm threshold being modified. This option cannot be changed.
   - ➢ **Interface**

3. Enter calculated value parameters.
   - ➢ **Computation** - Select a calculated value parameter. Options include `MIN`, `MAX` or `AVG`. For example, selecting MAX means calculate the maximum value collected by an SNMP object during the **Time Span** specified above.
   - ➢ **% Increase** - Add this percentage to the **Computation** value calculated above, with the **Computation** value representing 100%. The resulting value represents the alarm threshold.
   - ➢ **Minimum** - Set a minimum value for the alarm threshold. The value is automatically calculated as *two standard deviations below* the calculated **Computation** value, but can be manually overridden.
   - ➢ **Maximum** - Set a maximum value for the alarm threshold. The value is automatically calculated as *two standard deviations above* the calculated **Computation** value, but can be manually overridden.

Next

Move the user to the next wizard page.

Previous

Move the user back to the previous wizard page.

Cancel

Ignore any changes made to wizard pages and return to the **Counter Objects** list.

Save

Save changes made to the wizard pages.

SNMP Log

Monitor > SNMP Monitoring > SNMP Log

The **SNMP Log** page displays SNMP log data of MIB objects in a **SNMP Set** *(page 28)* 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 are displayed. Clicking the machine ID link displays all SNMP devices associated with the machine ID. Click the SNMP device link to display all MIB objects associated with the SNMP device.

View

Click the **View** link to display log data for a MIB object in a chart or table.

Remove

Click **Remove** to remove log data from a chart or table.

View All

If the SNMP monitor object has multiple instances, clicking the **View All** link displays all data for every instance.

Remove All

If the SNMP monitor object has multiple instances, clicking the **Remove All** link removes all data displayed for each instance.

Monitor Set Name

The name of the SNMP set the MIB object belongs to.

Get Object Name

The name of the MIB object used to monitor the SNMP device.

Description

The description of MIB object in the SNMP set.

Bar Chart / Table

Select the **Bar Chart** or **Table** radio button to display data in either format.

- A bar chart displays the last 2000 data points at the sample interval rate. The background of the chart displays in red for alarm threshold, yellow for warning threshold and green for no alarm.
- Table log data displays the most current values first and displays alarm and warning icons on log data that falls within these thresholds. See **Define SNMP Set** *(page 30)* for more information.

Display Last

Bar charts display log data for the last number of intervals selected. For example, if you select Display Last 500 minutes, each bar in the chart represents 1 minute.

Save View

You can save custom views for each MIB object. The next time this MIB object is selected the saved information is loaded.

Log rows per Page

These fields only display in Table format. Select the number of rows to display per page.

Display Value Over / Under Value

These fields only display in Table format. Filter the table rows displayed by filtering log data that is over or under the value specified.

Refresh

Click the refresh button to display the most current log data.

If your monitor doesn't show any log values, verify the following.

1. If there are no values returned, check the collection threshold for MIB objects in SNMP sets. If no values on the monitored device meet the collection threshold they are not included in the SNMP log.

2. The log value sample interval is determined by the total number of `SNMPGet` commands retrieving information from SNMP devices to the agent of the machine ID. The more `SNMPGet` commands the larger the sample interval. Check all SNMP devices associated with a machine ID. If some `SNMPGet` commands are returning values but others are not, the `SNMPGet` commands for the failed requests are not compatible.

If a monitor isn't responding, the log displays the message `Monitor Not Responding`. The `SNMPGet` command is incompatible with the device.

Set SNMP Values

Monitor > SNMP Monitoring > Set SNMP Values

The **Set SNMP Values** page enables you to write values to SNMP network devices. The SNMP objects must be `Read Write` capable and requires entering the Write Community password assigned to the SNMP device.

An SNMP community is a grouping of devices and management stations running SNMP. SNMP information is broadcast to all members of the same communiity on a network. SNMP default communities are:

- Write = private
- Read = public

> **Note:** This page only displays machines that have been previously identified using a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/index.asp#10627.htm)*.

Check-in status

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

🔵⏰   An agent icon adorned with a red clock badge is a temporary agent.

Machine ID.Group ID

Lists Machine ID.Group IDs currently matching the Machine ID / Group ID filter and assigned a SNMP Community name. Click a machine ID to display SNMP devices associated with that machine ID.

SNMP Device

Select the specific SNMP device of interest. This displays a history of SNMPSet values written to an SNMP device by the agent of the machine ID.

Create a SNMPSet command

Click **Create a SNMPSet command** to write a new value to this SNMP device. The following fields display:

- **Description** - Enter an easy to remember description of this event. This displays in the history of SNMPSet values for this SNMP device.
- **MIBObject** - Select the MIB object. Click **Add Object** *(page 33)* to add a MIB object that currently does not exist on the **Monitor Lists** *(page 18)* page.
- **SNMP Version** - Select a SNMP version. Version 1 is supported by all devices and is the default. Version 2c defines more attributes and encrypts the packets to and from the SNMP agent. Only select version 2c if you know the device supports version 2c.
- **writeCommunity** - The write Community password for the SNMP device. The default write community password is `private`.
- **timeOutValue** - Enter the number of seconds to wait for the SNMP device to respond before the write command times out.
- **setValue** - Enter the value to set the selected MIB object on the SNMP device.
- **attempts** - Enter the number of times to try and write to the MIB object, if it fails to accept the write command.

Execute SNMPSet

Prepares a procedure that executes a SNMPSet command for the selected SNMP device.

Cancel

Ignores any data entered and re-displays the **Create a SNMP command** link and history.

Set SNMP Type

Monitor > SNMP Monitoring > Set SNMP Type

The **Set SNMP Type** page assigns types to SNMP devices *manually*. SNMP devices assigned to one of these types are monitored by SNMP sets of the same type. You can also give individual SNMP devices custom names and descriptions as well as remove the device from your database.

Most SNMP devices are classified as a certain type of SNMP device using the MIB object `system.sysServices.0`. For example, some routers identify themselves as routers generically by returning the value 77 for the `system.sysServices.0` MIB object. You can use the value returned by the `system.sysServices.0` MIB object to auto assign SNMP sets to devices, as soon as they are discovered by a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/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 to devices *by type automatically* as follows:

1. Add or edit SNMP *types* using the **SNMP Device** tab in Monitor > **Monitor Lists** *(page 18)*.
2. Add or edit the value returned by the MIB object `system.sysServices.0` *and associated with each SNMP type* using the **SNMP Services** tab in Monitor > **Monitor Lists**.
3. Associate a SNMP *type* with a SNMP *set* using the **Automatic Deployment to** drop-down list in Monitor > SNMP Sets > **Define SNMP Set** *(page 30)*.
4. Perform a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/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 to devices *manually* as follows:

1. Assign a SNMP type to an SNMP device using Monitor > **Set SNMP Type** *(page 95)*. 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 network is scanned, 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 **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/index.asp#10627.htm)*.

Type

The SNMP type assigned to the SNMP device.

Custom Name

The custom name and custom description assigned to the SNMP device. If a device is given a custom name, the custom name displays instead of the SNMP name and IP address in alarms and in the SNMP log. To change the custom name and description click the edit icon 🖹 next to the custom name.

Device IP

The IP address of the SNMP device.

MAC Address

The MAC address of the SNMP device.

SNMP Name

The name of the SNMP device.

Parser Summary

Monitor > Log Monitoring > Parser Summary

The **Parser Summary** page displays and optionally define alerts for all parser sets assigned to all machine IDs within the user's scope. **Parser Summary** can also copy parser sets assignments to multiple machine IDs.

> **Note:** Copying a parser set to a machine ID on this page *activates* the log parser on the machine IDs it is copied to. Parsing occurs whenever the log file being parsed is updated.
>
> **Note:** You can download a **Configuring Log Parsers Step-by-Step**
> *(http://help.kaseya.com/webhelp/EN/VSA/9040000/EN_logparsers_R94.pdf#zoom=70&navpanes=0)* PDF from the first topic of online user assistance.

Log Monitoring Setup

1. **Log Parser** - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.
2. **Assign Parser Sets** - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. *Activate* parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.
3. **Parser Summary** - Quickly copy *active* parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

Notification

The agent collects log entries and creates an entry in the 'log monitoring' log based on the criteria defined by the parser set, *whether or not any of the notification methods are checked.* You don't have to be notified each time a new log monitoring entry is created. You can simply **review the 'Log Monitoring' log** *(page 110)* periodically at your convenience.

To Copy Parser Set Assignments

1. Select a source machine to copy parser set assignments from.
2. Select machine IDs to copy parser set assignments to.
3. Click **Copy**.

To Create a Parser Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
   - Create **A**larm
   - Create **T**icket
   - Run **S**cript
   - **E**mail Recipients
2. Set additional email parameters.
3. Check the machine IDs to apply the alert to.
4. Click the **Apply** button.

To Cancel a Parser Set Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.

   The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

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

- Log Monitoring parser alerts.
- Multiple log monitoring parser alerts.
- Missing log monitoring parser alert.

> Note: Changing this email alarm format changes the format for both **Assign Parser Sets** and **Parser Summary** emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A 🔴 in a numbered column indicates a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3
<ad>	#ad#	duration		🔴	
<at>	#at#	alert time	🔴	🔴	🔴
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	🔴	🔴	🔴
<ec>	#ec#	event count		🔴	
<ed>	#ed#	event description	🔴	🔴	
<gr>	#gr#	group ID	🔴	🔴	🔴
<id>	#id#	machine ID	🔴	🔴	🔴
<lpm>	#lpm#	Log file set criteria	🔴	🔴	🔴
<lpn>	#lpn#	Log parser set name	🔴	🔴	🔴
<lsn>	#lsn#	Log file set name	🔴	🔴	🔴
	#subject#	subject text of the email message, if an email was sent in response to an alert	🔴	🔴	🔴
	#body#	body text of the email message, if an email was sent in response to an alert	🔴	🔴	🔴

Create Alarm

> If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Copy

Click **Copy** to copy the parser sets of the machine ID selected using the **this machine ID** link to other machine IDs selected in the paging area.

Apply

Applies alert checkbox settings to selected machine IDs.

Clear All

Clears all alert checkbox settings from selected machine IDs.

Select All/Unselect All

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View 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
- An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

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

Delete

Click the delete icon ✕ next to a parser set to delete its assignment to a machine ID.

Log Set Names

Lists the names of parser sets assigned to this machine ID.

ATSE

The ATSE response code assigned to machine IDs:

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

Email Address

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

Interval

The interval to wait for the alert event to occur or not occur.

Duration

Applies only if **Alert when this event occurs <N> times within <N> <periods>** is selected. Refers to **<N> <periods>**.

Re-Arm

Applies only if **Ignore additional alarms for <N> <periods> is selected**.

Log Parser

Monitor > Log Monitoring > Log Parser

The **Log Parser** page defines log parsers and assigns them to selected machine IDs.

> **Note:** You can download a **Configuring Log Parsers Step-by-Step**
> *(http://help.kaseya.com/webhelp/EN/VSA/9040000/EN_logparsers_R94.pdf#zoom=70&navpanes=0)* PDF from the first topic of online user assistance.
>
> **Note:** The log parsers are only *active* if they are subsequently assigned a log parser set using **Assign Parser Sets** *(page 105)*.

Log Monitoring

The VSA is capable of monitoring data collected from many standard log files. **Log Monitoring** extends that capability by extracting data from the output of any text-based log file. Examples include application log files and syslog 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 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** *(page 105)* or **Parser Summary** *(page 97)*.

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 procedure event itself. Only a new configuration, or reconfiguration, using **Log Parser**, **Assign Parser Sets** or **Parser Summary** generates a procedure you can see in the Procedure History or Pending Procedure tabs of the **Machine Summary** page.

Apply

Click **Apply** to assign a selected log parser to selected machine IDs.

Clear

Click **Clear** to remove a selected log parser from selected machine IDs.

Clear All

Click **Clear All** to remove all log parsers from selected machine IDs.

New...

Select `<Select Log Parser>` in the **Log File Parser** drop-down list and click **New...** *(page 101)* to create a new log parser.

Edit...

Select an existing log parser in the **Log File Parser** drop-down list and click **Edit...** *(page 101)* to edit the log parser.

Add Log Parser / Replace Log Parsers

Select **Add Log Parser** to add a log parser to existing machine IDs. Select **Replace Log Parsers** to add a log parser and remove all other log parsers from selected machine IDs.

Log File Parser Definition

Monitor > Log Monitoring > Log Parser > Log File Parser Definition

The **Log File Parser Definition** page defines templates and parameters used to parse log files. Definitions are subsequently assigned to machine IDs using the **Log Parser** *(page 100)* page. Log parsers are

initially private, but can be shared with other users.

The Log File Parsing Cycle

The parsing of a log file is triggered whenever the log file is changed. In most cases this involves appending new text to the end of the file. To avoid scanning the entire log file from the beginning each time the file is updated, the agent parses log files as follows:

- After each update the agent stores a "bookmark" of the last 512 bytes of a log file.
- When the log file is updated again, the agent compares the bookmark from the old update with the *same byte position* in the new update.
- Since log files may be archived before the log parser is run, parsing can include 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 procedure event itself. Only a new configuration, or reconfiguration, using **Log Parser**, **Assign Parser Sets** or **Parser Summary** generates a procedure you can see in the Procedure History or Pending Procedure tabs of the **Machine Summary** page.

Save

Select **Save** to save changes to a log file parser definition.

Save As...

Select **Save As...** to save a log file parser definition under a different name.

Delete

Select **Delete** to delete a log file parser definition.

Share...

You can share log file parser definitions you own with other VSA users, user roles, or make the procedure public to all users.

Parser Name

Enter the name of the parser.

Log File Path

Enter the full UNC pathname or mapped drive pathname on the target machine of the log file you want to parse. You can use asterisk (*) or question mark (?) wildcards to specify a set of log files. If a log file set is specified, the log parser starts with the latest log file first. Example: `\\morpheus\logs\message.log` or `c:\logs\message.log`. When specifying a UNC path to a share accessed by an agent machine—for example `\\machinename\share`—ensure the share's permissions allow read/write access using the **agent credential** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3492.htm)* specified for that agent machine in Agent > Manage Agents.

Log Archive Path

Enter the full UNC pathname or mapped drive pathname on the target machine of the archive files you want to parse. You can use asterisk (*) or question mark (?) wildcards to specify a set of archive files. If an archive set is specified, the log parser starts with the latest log file first. Example: If `message.log` is archived daily to a file in `messageYYYYMMDD.log` format, then you can specify `c:\logs\message*.log`. When specifying a UNC path to a share accessed by an agent machine—for example `\\machinename\share`—ensure the share's permissions allow read/write access using the **agent credential** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#3492.htm)* specified for that agent machine in Agent > Manage Agents.

Description

Enter a description for the log parser.

Template

The template is used to compare with the log entry in the log file to extract out the required data into parameters. Parameters are enclosed with $ character in template.

Enter a pattern of text and log file parameters. This pattern is used to search from the beginning of each line in a log file. If a pattern finds a match in the log file, the log file parameters in the pattern are populated with the values extracted from the log file.

You can use a percent (%) wildcard to specify an alphanumeric string of any length. A log file parameter is bracketed with the dollar ($) symbol. Enter $$ to match a pattern of text containing a $ symbol. Enter %% to match a pattern of text containing a % symbol.

> **Note:** Template text patterns are *case sensitive*.

Example

- Log text: `126 Oct 19 2007 12:30:30 127.0.0.1 Device0[123]: return error code -1!`
- Template: `$EventCode$ $Time$ $HostComputer$ $Dev$[$PID$]:%error code $ErrorCode$!`
- Parsed result:
  ```
  EventCode=126
  Time= 2007/10/19 12:30:30 Friday
  HostComputer=127.0.0.1
  Dev=Device0
  PID=123
  ErrorCode=-1
  ```

Guidelines

- To enter a tab character in the template edit box:
    1. Copy and paste a tab character from log data.
    2. Use {tab} if it is enter manually.
- To create a template it is easier to copy the original text into the template, then replace the characters that can be ignored with %. Then replace the characters that are saved to a parameter with a parameter name.
- Make sure all parameters in the template are defined in **Log File Parameters**.
- A date time parameter must have both date and time information from the source data, otherwise just use a string parameter.

Skipping Characters

To skip characters, use `$[n]$`, where `n` is the number of characters to skip. Use `$var[n]$` to retrieve a fixed number of characters to be a variable value.

Example

- Log text: `0123456789ABCDEFGHIJ`
- Template: `$[10]$ABC$str[3]$`
- Result for parameter `str` is `DEF`.

Multilayer Template

If checked, multiple lines of text and log file parameters are used to   parse the log file.

> **Note:** The character string {tab} can be used as a tab character and {nl}   can be used as a new line break. {nl} cannot be used in single line template. % can be used as wildcard character.

Output Template

Enter a pattern of text and log file parameters to store in **Log Monitoring**.

Example:

- Output template: `Received device error from $Dev$ on $HostComputer$. Code = $ErrorCode$.`
- Result output: `Received device error from Device0 on 127.0.0.1. Code = -1.`

Apply

Click **Apply** to add or update a parameter entered in the **Name** field.

Clear All

Click **Clear All** to remove all parameters from the parameter list.

Log File Parameters

Name

Once the template is created, you need to define the list of parameters used by the template. All the parameters in the template have to be defined, otherwise the parser returns an error. Available parameters are *integer, unsigned integer, long, unsigned long, float, double, datetime, string.* The length of parameter name is limited to 32 characters.

Enter the name of a parameter used to store a value. Parameters are subsequently used in the **Template** and **Output Template** text boxes.

> **Note:** Do *not* bracket the name of the parameter with $ symbols in the **Name** field. This is only required when the parameter is entered in the **Template** and **Output Template** text boxes.

Type

Enter the data type appropriate for the parameter. If data parsed from a log file cannot be stored using that data type, the parameter remains empty.

Date Format

If the **Type** selected is `Date Time`, enter a **Date Format**.

- `yy, yyyy, YY, YYYY` - two or four digit year
- `M` - single or two digit month
- `MM` - two digit month
- `MMM` - abbreviation of month name, ex. "Jan"
- `MMMM` - full month name, ex. "January"
- `D, d` - single or two digit day

- `DD, dd` - two digit day
- `DDD, ddd` - abbreviation name of day of week, Ex. "Mon"
- `DDDD, dddd` - full name of day of week, ex. "Monday"
- `H, h` - single or two digit hour
- `HH, hh` - two digit hour
- `m` - single or two digit minute
- `mm` - two digit minute
- `s` - single or two digit second
- `ss` - two digit second
- `f` - one or more digit of fraction of second
- `ff` - ffffffff - two to nine digit
- `t` - one character time mark, ex. "a"
- `tt` - two-character time mark, ex. "am"

> **Note:** *Date and time filtering in views and reports are based on the log entry time.* If you include a `$Time$` parameter using the `Date Time` data type in your template, **Log Monitoring** uses the time stored in the `$Time$` parameter as the log entry time. If a `$Time$` parameter is *not* included in your template, then the time the entry was added to **Log Monitoring** serves as the log entry time. Each date time parameter must contain at least the month, day, hour, and second data.

Example:
- Date time string: `Oct 19 2007 12:30:30`
- DateTime template: `MMM DD YYYY hh:mm:ss`

UTC Date

Log Monitoring stores all date/time values as **universal time, coordinated** (UTC). This enables UTC date and times to be automatically converted to the user's local time when **Log Monitoring** data is displayed or when reports are generated.

If blank, the date and time values stored in the log file parameter are converted from the local time of the machine ID assigned the log parser to UTC. If checked, the date and time values stored in the log file parameter are UTC and no conversion is necessary.

Assign Parser Sets

`Monitor > Log Monitoring > Assign Parser Sets`

The **Assign Parser Sets** page creates and edits parser sets and assigns parsers sets to machine IDs. Optionally triggers an alert based on a parser set assignment. A machine ID only displays in the paging area if:

- That machine ID has been previously assigned a **log file parser definition** *(page 101)* using Monitor > **Log Parser** *(page 100)*.
- That same log file parser definition is selected in the **Select Log File Parser** drop-down list.

> **Note:** Assigning a parser set to a machine ID on this page *activates* the log parser. Parsing occurs whenever the log file being parsed is updated.

> **Note:** You can download a **Configuring Log Parsers Step-by-Step** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/EN_logparsers_R94.pdf#zoom=70&navpanes=0)* PDF from the first topic of online user assistance.

Notification

The agent collects log entries and creates an entry in the 'log monitoring' log based on the criteria defined by the parser set, *whether or not any of the notification methods are checked.* You don't have to be notified each time a new log monitoring entry is created. You can simply **review the 'Log Monitoring' log** *(page 110)* periodically at your convenience.

Parser Definitions and Parser Sets

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

A **parser definition** is used to:

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

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

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

Log Monitoring Setup

1. **Log Parser** - Identify a log file to parse using a log file parser definition. A log file parser definition contains the log file parameters used to store values extracted from the log file. Then assign the log parser to one or more machines.
2. **Assign Parser Sets** - Define a parser set to generate Log Monitoring records, based on the specific values stored in the parameters. *Activate* parsing by assigning a parser set to one or more machine IDs previously assigned that log parser. Optionally define alerts.
3. **Parser Summary** - Quickly copy *active* parser set assignments from a single source machine to other machine IDs. Optionally define alerts.

To Create a Parser Set Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
   - Create **A**larm
   - Create **T**icket
   - Run **S**cript
   - **E**mail Recipients
2. Set additional email parameters.
3. Select the parser set to add or replace.
4. Check the machine IDs to apply the alert to.
5. Click the **Apply** button.

To Cancel a Parser Set Alert

1. Select the machine ID checkbox.
2. Click the **Clear** button.
   The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

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

- **1 - Log Monitoring parser alerts.**
- **2 - Multiple log monitoring parser alerts.**
- **3 - Missing log monitoring parser alert.**

> **Note:** Changing this email alarm format changes the format for both **Assign Parser Sets** and **Parser Summary** emails.

The following variables can be included in your formatted email alerts and are passed to agent procedures assigned to the alert. A ● in a numbered column indicates   a variable can be used with the alert type corresponding to that number.

Within an Email	Within a Procedure	Description	1	2	3
<ad>	#ad#	duration		●	
<at>	#at#	alert time	●	●	●
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>	●	●	●
<ec>	#ec#	event count		●	
<ed>	#ed#	event description	●	●	
<gr>	#gr#	group ID	●	●	●
<id>	#id#	machine ID	●	●	●
<lpm>	#lpm#	Log file set criteria	●	●	●
<lpn>	#lpn#	Log parser set name	●	●	●
<lsn>	#lsn#	Log file set name	●	●	●
	#subject#	subject text of the email message, if an email was sent in response to an alert	●	●	●
	#body#	body text of the email message, if an email was sent in response to an alert	●	●	●

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > **Dashboard List** *(page 6)*, Monitor > **Alarm Summary** *(page 14)* and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

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

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.

Email Recipients

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

- The email address of the currently logged on user displays in the **Email Recipients** field. It defaults from System > Preferences.
- Click **Format Email** to display the **Format Alert Email** popup window. This window enables you to format the display of emails generated by the system when an alert condition is encountered. This option only displays for master role users.
- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

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 100)* page.

Define log sets to match

After a log parser is selected, click **Edit** *(page 109)* to define a new parser set or select an existing parser set from the **Define log sets to match** *(page 109)* drop-down list.

Alert when...

Specify the *frequency* of the parser set condition required to trigger an alert:

- **Alert when this event occurs once**
- **Alert when this event occurs <N> times within <N> <periods>**
- **Alert when this event doesn't occur within <N> <periods>**
- **Ignore additional alarms for <N> <periods>**

Add / Replace

Click the **Add** or **Replace** radio options, then click **Apply** to assign a selected parser set to selected machine IDs.

Remove

Click **Remove** to remove all parser sets from selected machine IDs.

Apply

Applies the selected parser set to checked machine IDs.

Clear

Clears the assignment of a selected parser set from selected machine IDs.

Clear All

Clears all parser sets assigned to selected machine IDs.

Select All/Unselect All

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a

check-in icon displays the agent Quick View 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
- An agent icon adorned with a red clock badge is a temporary agent.

Machine.Group ID

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

Delete

Click the delete icon ✗ next to a parser set to delete its assignment to a machine ID.

Log Set Names

Lists the names of parser sets assigned to this machine ID.

ATSE

The ATSE response code assigned to machine IDs:

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

Email Address

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

Interval

The interval to wait for the alert event to occur or not occur.

Duration

Applies only if **Alert when this event occurs <N> times within <N> <periods>** is selected. Refers to **<N> <periods>**.

Re-Arm

Applies only if **Ignore additional alarms for <N> <periods> is selected**.

Log File Set Definition

Monitor > Log Monitoring > Assign Parser Sets

- *Select a log parser from the* Select log file parser *drop-down list.*
- *Then select* <New Parser Set> *or an existing parser set from the* Define log set to match *drop-down list. The* Log File Set Definition *popup window displays.*

The **Log File Set Definition** page defines parser sets. A parser set is a list of conditions that must be matched to create a **Log Monitoring** record. Each condition combines a parameter, operator and value.

Parser Definitions and Parser Sets

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

A **parser definition** is used to:

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

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

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

To Create a New Parser Set

1. Enter a name for the parser set.
2. Optionally rename the parser set by entering a new name and click **Rename** to confirm the change.
3. Select a log file parameter from the **Parser Column** drop-down list. Log file parameters are defined using the **Log File Parser Definition** *(page 101)* this parser set is intended to filter.
4. Select an **Operator** from the drop-down list. Different data types provide different lists of possible operators.
5. Enter the value the log file parameter should have in the **Log File Filter** field to generate a **Log Monitoring** record.

> **Note:** Template text patterns are *case sensitive*.

6. Click **Add** to add this parameter/operator/value combination to the list of conditions defined for this parser set.
7. Click **Edit** to edit and then **Save** an existing parameter/operator/value combination.
8. Click the delete icon ✗ to delete an existing parameter/operator/value combination.

Viewing Log Monitoring Entries

Log Monitoring entries are displayed in **Log Monitoring**, which can be accessed using:

- Agents > Agent Logs > Log Monitoring > (parser definition)
- Live Connect (Classic) > Agent Data > Agent Logs > Log Monitoring > (parser definition). Live Connect is displayed by clicking the check-in status icon of a selected machine ID.
- Audit > Machine Summary > Agent Logs tab > Log Monitoring > (parser definition). The Machine Summary page can also be displayed by *alt-clicking* the check-in status icon of a selected machine ID.
- The Info Center > Reporting > Reports > Monitor - Logs > Log Monitoring report.

Index