Kaseya

Monitoring Configuration

Quick Start Guide

Version R94

English

December 12, 2016

Copyright Agreement

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

Contents

Introduction

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*.

This quick start guide provides an introduction to the first five methods of monitoring and to notification in general. See the **Configuring Log Parsers Step-by-Step** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/EN_logparsers_R94.pdf#zoom=70&navpanes=0)* quick start guide for information about the monitoring of log files.

> Note: You can quickly apply monitor settings to an organization *by policy* using the **Standard Solution Package setup wizard** *(http://help.kaseya.com/webhelp/EN/SSP/9040000/index.asp#11220.htm)*.
>
> Note: See the **Network Monitor quick start guide** *(http://help.kaseya.com/webhelp/EN/KNM/9040000/EN_knmquickstart_R94.pdf#zoom=70&navpanes=0)* for an introduction to monitoring both machines and devices *without agents*.

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

Other add-on modules have alerts not listed here.

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, System Check, **Event Log Alerts** *(page 7)* and Log Monitoring 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 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 counters, services, and processes and SNMP set 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 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 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
- Alarm Network Status
- Alarm Rotator
- Alarm Ticker
- Network Status
- Group Alarm Status
- Monitoring Set Status

- Monitor Status
- Machines Online
- Top N - Monitor Alarm Chart

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
- Monitor > Dashboard List > any Alarm Summary Window 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
- Monitor > Dashboard List > Alarm Network Status
- Monitor > Dashboard List > Alarm Rotator
- Monitor > Dashboard List > Alarm Ticker
- Monitor > Dashboard List > Group Alarm Status
- Monitor > Dashboard List > Monitor Set Status
- Monitor > Dashboard List > Monitor Status
- Monitor > Dashboard List > Top N - Monitor Alarm Count
- Monitor > Dashboard List > KES Status
- Monitor > Dashboard List > KES Threats
- 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
- Monitor > Monitor Log
- Monitor > SNMP Log
- Monitor > Dashboard > Network Status
- Monitor > Dashboard > Group Alarm Status
- Monitor > Dashboard > Monitoring Set Status
- 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 dashlet of the Monitor > **Dashboard List** page. You can create new groups using the **Group Alarm Column Names** tab in Monitor > Monitor Lists. Group alarm column names are assigned to monitor sets using Define Monitor Set.

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.

There are multiple types of alerts available to you.

Alert Types

- The **Alerts - Summary** page shows what alerts are enabled for each machine. You can apply or clear settings or copy enabled alerts settings.
- The **Alerts - Agent Status** page alerts when an agent is offline, first goes online, or someone has disabled remote control on the selected machine.
- The **Alerts Application Changes** page alerts when a new application is installed or removed on selected machines.
- The **Alerts - Get File** 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.
- The **Alerts - Hardware Changes** 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.
- The **Alerts - Low Disk** page alerts when available disk space falls below a specified percentage of free disk space.
- 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**.
- The **Alerts - Agent Procedure Failure** page alerts when an agent procedure fails to execute on a managed machine.
- The **Alerts - Protection Violation** page alerts when a file is changed or access violation detected on a managed machine.
- The **Alerts - New Agent Installed** page alerts when a new agent is installed on a managed machine by selected *machine groups*.
- The **Alerts - Patch Alert** page alerts for patch management events on managed machines.
- The **Alerts - Backup Alert** page alerts for backup events on managed machines.
- The **Alerts - System** page alerts for selected events occurring on the *Kaseya Server*.

To Create An Alert

The same general procedure applies to all alert types.

1. Select an alert function from the **Select Alert Function** drop-down list.
2. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
    - Create **A**larm
    - Create **T**icket
    - Run **S**cript
    - **E**mail Recipients
3. Set additional email parameters.
4. Set additional alert-specific parameters. These differ based on the alert function selected.

5. Check the paging rows to apply the alert to.
6. Click the Apply button.

To Cancel an Alert

1. Select one or more paging rows.
2. Click the Clear button.
   The alert information listed next to the paging row is removed.

Event Log Alerts

The Events Logs Alert page is one of the more advanced types of alerts and requires special configuration. It starts with a good understanding of event logs.

Event Logs

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

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

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

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

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

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

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

- System > Database Views > vNtEventLog

Creating Event Sets from Event Log Entries

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 ℹ 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 for a description of each field shown in the wizard.

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.

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 you assign.
4. Specify the actions to take in response to an alert condition using the Event Log Alerts > Set Alert Actions 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.
6. Select the machines an event set should be applied to.
7. Click the Apply button.

System Checks

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

Monitor Sets

Monitor Sets use Windows-based **performance counters** to provide information as to how well the operating system or an application, service, or driver is performing. Counter data can help determine system bottlenecks and fine-tune system and application performance. For example, a server may continue working without generating any errors or warnings in the event logs. Nevertheless, users may complain the server's response time is slow.

> Note: Counters in VSA monitor sets are based on real time state-based data, not log files. See **Alarms** *(page 2)* for more information.

Performance Objects, Instances and Counters

When setting up counter thresholds in **monitor sets** *(page 9)*, 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.

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.
2. Create and maintain monitor sets using Monitor > Monitor Sets.
3. Assign monitor sets to machine IDs using Monitor > Assign Monitoring.
4. Optionally customize standard monitor sets as *individualized monitor sets*.
5. Optionally customize standard monitor sets using *Auto Learn*.

6. Review monitor set results using:
    ➢ Monitor > Monitor Log
    ➢ Monitor > Live Counter
    ➢ Monitor > Dashboard > Network Status
    ➢ Monitor > Dashboard > Group Alarm Status
    ➢ Monitor > Dashboard > Monitoring Set Status
    ➢ Info Center > Reporting > Reports > Monitor > Monitor Set Report
    ➢ Info Center > Reporting > Reports > Monitor > Monitor Action Log

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.

Defining Monitor Sets

Each monitor set is defined using four tabs.

▪ 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.

▪ 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.*

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

▪ The **Monitor Icons** tab selects the monitor icons that display in the Monitor Log page when various alarm states occur.

Configuring Counter Thresholds

After you add a new monitor set using Monitor > **Monitor Sets**, you can add or edit counter thresholds using the **Counter Thresholds** tab.

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. 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 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 > **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.

Configuring Services Check

Monitor services using a monitor set as follows. 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. 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 > **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 > **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 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.

Configuring Process Status

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. 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.

Setting Counter Thresholds Manually - An Example

In this example, the `ZC-PS1-Print Server Monitor` monitor set is reviewed to illustrate how monitor sets counter thresholds are defined.

1. Click Monitor > **Monitor Sets** to display the first page of all the monitor sets available in your VSA. In this case sample monitor sets have been loaded into the VSA. Sample monitor set names start with a ZC prefix. You load sample sets into the VSA using System > **Configure**.

2. Click the **Edit** button next to the `ZC-PS1-Print Server Monitor` monitor set.

Select the Monitor Set to edit or delete

| << | ZC-EX2- Exchange 2007 Basic ▼ | >> | Add | Import | Page 3 of 6 |

	Name	Description	Group Alarm Column
Edit	ZC-EX2- Exchange 2007 Basic Services - 2	Basic services for Microsoft Exchange 2007.	
Edit	ZC-EX2- Exchange 2007 Service - MSExchangeMonitoring	Service for Microsoft Exchange 2007.	
Edit	ZC-EX2- Exchange 2007 Service - MSExchangePop3	MSExchangePop3 Service for Microsoft Exchange 2007.	
Edit	ZC-EX2- Exchange 2007 Service - MSExchangeRepl	MSExchangeRepl service for Microsoft Exchange 2007.	
Edit	ZC-FX1-Fax Server Basic Services	Monitor for Faxes sent,Total faxes,Failed faxes,Received faxes & Total ...	
Edit	ZC-GMS1-Good Messaging Services	GoodLink Mobile Messaging (Runs GoodLink Mobile Messaging to sync mail to P...	
Edit	ZC-IIS2 -IIS Basic Services	Internet Information Service (IIS) Monitoring	
Edit	ZC-IIS2 -IIS Service - CiSvc	Internet Information Service (IIS) Monitoring	
Edit	ZC-IIS2 -IIS Services - IISADMIN	Internet Information Service (IIS) Monitoring	
Edit	ZC-IIS2-IIS Monitor	IIS Monitor Set	
Edit	ZC-PS1-Print Server Monitor	It's used to check job Errors, Total job Printed,Total pages printed,ou...	
Edit	ZC-Server Reboot	Check the Status of Server Uptime.	
Edit	ZC-SQL2 - MSSQLSERVER Services - MSSQLSERVER	MSSQLSERVER Service	
Edit	ZC-SQL2-MS SQL Server Production	Monitors the Performance of the SQL Server	
Edit	ZC-SV1- 2000 Server Basic Services	checks windows service for every 3 Minutes & restarted if stopped.	
Edit	ZC-SV1- Windows Server 2000 Service - Computer Browser (browser)	Computer Browser (browser)	
Edit	ZC-SV1- Windows Server 2000 Service - Cryptographic Services (Cryptsvc)	Cryptographic Services (Cryptsvc)	
Edit	ZC-SV1- Windows Server 2000 Service - Dhcp	DHCP Client	
Edit	ZC-SV1- Windows Server 2000 Service - dmserver	Logical Disk Manager - dmserver	
Edit	ZC-SV1- Windows Server 2000 Service - Dnscache	DNS Service for clients.	

| << | >> | Add | Import | Page 3 of 6 |

3. The **Define Monitor Sets** page displays. The **Counter Thresholds** tab displays initially, which is the tab we want to review. This spreadsheet view displays the settings defined for each of the counters. If you wanted to edit a counter, you would click on the edit icon in the far left column to display the edit wizard for that counter.

> **Note:** You can edit a sample ZC monitor set, but these sample monitor sets are subject to being overwritten if updating is enabled using System > Configure. If you want to customize a ZC sample set and ensure your changes are preserved, create a copy of the ZC sample set and make changes to that copy.

We want to review the settings of all the counters in this monitor set, so we'll stay with the spreadsheet view.

Define Monitor Sets   Take ownership of MonitorSet ZC-PS1-Print Server Monitor   Close

Monitor Set Name
ZC-PS1-Print Server Monitor   Save As...
Monitor Set Description
It's used to check job Errors, Total job Printed,Total   Export Monitor Set...
pages printed,out of paper errors and print spooler
service.
Group Alarm Column Name: Other ▼

| Counter Thresholds | Services Check | Process Status | Monitor Icons |

| << | >> | Page 1 of 1 |

	Object	Counter	Instance	Counter Name	Description	Collection Operator	Collection Threshold	Sample Interval	Alarm Operator	Alarm Threshold	Duration	Re-Arm Alarm	Warning%	Trend Activated?	Trending Window	Re-Arm Trending
	Print Queue	Job Errors	_Total	Print Queue	(Print Queue) Total Numbe...	Over	-1	5 min	Over	160	30 min	1 sec	10		14 sec	1 sec
	Print Queue	Total Jobs Printed	_Total	Print Queue	(Print Queue) Number of &...	Over	-1	5 min	Over	17500	30 min	1 sec	0		14 sec	1 sec
	Print Queue	Out of Paper Errors	_Total	Print Queue	(Print Queue) Out of Pape...	Over	-1	5 min	Over	0	10 min	1 sec	0		14 sec	1 sec
	Print Queue	Jobs	_Total	Print Queue	Total Number of Print Job...	Over	-1	5 min	Over	100	20 min	1 sec	0		14 sec	1 sec
	Print Queue	Total Pages Printed	_Total	Print Queue	Total number of pages pri...	Over	-1	5 min	Over	50000	30 min	1 sec	0		14 sec	1 sec

| << | >> | Page 1 of 1 |

4. Let's examine the first five columns of the **Counter Thresholds** tab for this monitor set.

In this case the counters are all for the same `Print Queue` object. Monitor sets are not limited to a single performance object, but it makes sense to logically group counters within a single monitor set around a certain Windows function.

The **Instance** column is really a sub-category of the object, not the counter. Counters are defined for a combination of object and instance. For example, the instances of the `Print Queue` object are the names of specific printers the target machine can print to, along with the instance called `_Total`.

The `_Total` instance combines the numerical value of any counter data from all printers and sums it. But it also acts as a kind of "wildcard instance". Without the `_Total` instance you would have to specify an instance using an exact printer name, which makes applying the same monitor set to multiple machines difficult. The true benefit of the `_Total` instance in this case is determining if there *are any printer errors on any printers at all*. Once you know that you can

investigate the specific cause.

Object	Counter	Instance	Counter Name	Description
Print Queue	Job Errors	_Total	Print Queue	(Print Queue) Total Numbe...
Print Queue	Total Jobs Printed	_Total	Print Queue	(Print Queue) Number of &...
Print Queue	Out of Paper Errors	_Total	Print Queue	(Print Queue) Out of Pape...
Print Queue	Jobs	_Total	Print Queue	Total Number of Print Job...
Print Queue	Total Pages Printed	_Total	Print Queue	Total number of pages pri...

5. The next set of columns describes collection and alarm threshold settings. Notice that **Collection Operator** and **Collection Threshold** values are all set to `Over -1`. The `Over -1` collection criteria is frequently used to ensure that any value, including zero, is collected, regardless of whether an alarm threshold is ever encountered. This ensures that you can review all the data generated by a counter.

Each counter provides a new value every five minutes, as specified by the **Sample Interval** column.

High **Alarm Threshold** values are set for the `Total Jobs Printed` and `Total Pages Printed` counters. This is appropriate because a high volume printer will easily approach this many print jobs and pages printed.

The **Alarm Threshold** value for `Jobs` and `Job Errors` are much smaller. The `Jobs` counter returns the number of jobs currently being processed, so it's expected this would be small. The `Job Errors` counter returns the number of job errors that have occurred since the print server was last started. A high volume printer will quickly exceed this alarm threshold if there is problem with the printer.

The `Out of Paper Errors` counter shows a zero threshold, which is the normal value when no out of paper errors have occurred since the print server was last started. If even a single "out of paper" error occurs, *any* value `Over 0` will trigger an alert condition, signaling it's time to add paper to the printer.

Counter	Collection Operator	Collection Threshold	Sample Interval	Alarm Operator	Alarm Threshold	Duration	Re-Arm Alarm
Job Errors	Over	-1	5 min	Over	160	30 min	1 sec
Total Jobs Printed	Over	-1	5 min	Over	17500	30 min	1 sec
Out of Paper Errors	Over	-1	5 min	Over	0	10 min	1 sec
Jobs	Over	-1	5 min	Over	100	20 min	1 sec
Total Pages Printed	Over	-1	5 min	Over	50000	30 min	1 sec

6. The final five columns specify warning alarms and trending alarms. The warning alarm is specified as a percentage. For the `Jobs Errors` counter, a warning alarm is triggered when the value of the counter reaches 10% of its alarm threshold.

A trending alarm, if activated, calculates a trend line based on collected data. If the trend line determines that the alarm threshold will be exceeded within the **Trending Window** time period, a trending alarm is triggered.

Unless a resource is critical, or already the subject of an investigation, warning alarms and trending alarms are generally not used. Typically a trending window should be set to the amount of time you need to prepare for an alert condition, if it occurs.

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

Counter	Warning%	Trend Activated?	Trending Window	Re-Arm Trending
Job Errors	10		14 sec	1 sec
Total Jobs Printed	0		14 sec	1 sec
Out of Paper Errors	0		14 sec	1 sec
Jobs	0		14 sec	1 sec
Total Pages Printed	0		14 sec	1 sec

Assigning Monitor Sets

You assign monitor sets using Monitor > **Assign Monitoring** to specific machine IDs. You have the option of customizing applied monitor sets in two ways:

- Individualized Monitor Sets
- Auto Learn

Individualized Monitor Sets

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

1. Using Monitor > **Assign Monitoring**, select a *standard* monitor set using the `<Select Monitor Set>` drop-down list.
2. Assign this standard monitor set to a machine ID. The monitor set name displays in the **Monitor Set** column.
3. Click the individualized monitor set icon in the **Monitor Set** column to display the same options you see when defining a standard monitor set. *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 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.

SNMP Sets

Certain network devices such as printers, routers, firewalls, servers and UPS devices can't support the installation of an agent. But a VSA agent installed on a managed machine on the same network as the device can read or write to that device using **simple network management protocol (SNMP).**

Basic SNMP Monitoring

The fastest way to begin learning how to use the VSA to monitor SNMP devices is to assign a pre-defined "SNMP set" to a device and see the results. Once you've seen how simple the basic configuration is, you can review more advanced SNMP features.

You can begin monitoring of SNMP-enabled devices in three steps:

1. Discover SNMP devices using Discovery > By Network or **By Agent** *(page 16)*.
2. Assign pre-defined SNMP sets to discovered devices using Monitor > **Assign SNMP** *(page 16)*.
3. Display SNMP alarms using Monitor > **SNMP Log** *(page 18)*

Scanning Networks with SNMP Enabled

By Network or **By Agent** in the **Discovery** module uses an existing VSA agent on a managed machine to periodically scan the local area network for any and all new devices connected to that network since the last time a network scan ran.

The discovery machine issues SNMP requests to the SNMP devices it discovers on that same network. So you must run a network scan with SNMP-enabled to have access to SNMP-enabled devices using the VSA.
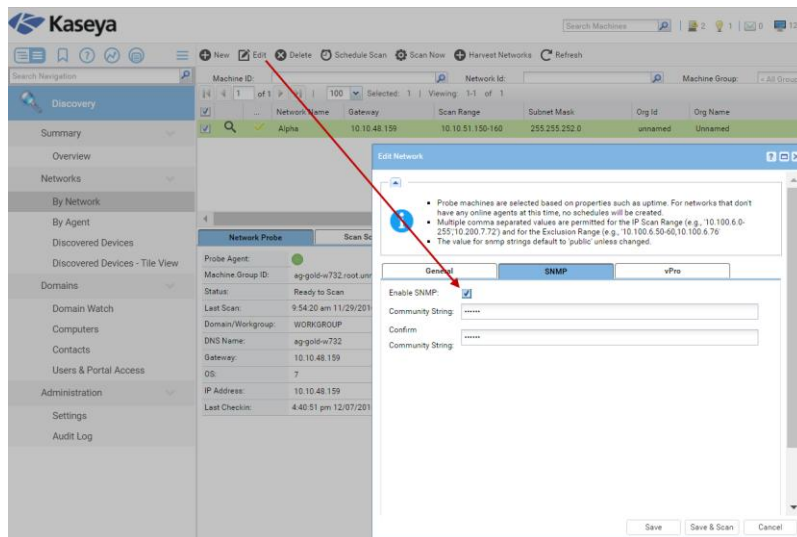
To include SNMP devices in the a network scan:

1. Select a machine ID on the same network as the SNMP devices you want to discover.
2. Check the **Enable SNMP** checkbox.
3. Enter a `community name` in the **Read Community Name** and **Confirm** fields.

   A community name is a credential for gaining access to an SNMP-enabled device. The default "read" community name is typically `public`, in all lower case, but each device may be configured differently. You may have to identify or reset the community name on the device directly if you're not sure what community name to use.
4. Click the **Save & Scan** button at the bottom of the **Edit Network** dialog. This will start the scan immediately.
5. Review discovered SNMP-enabled devices using the Monitor > **Assign SNMP** *(page 16)* page.

Assign SNMP

SNMP devices only display in the Monitor > **Assign SNMP** page *after* network scanning is run on the discovery machine.

To assign the monitoring of an SNMP-enabled device using the **Assign SNMP** page:

1. Select the discovery machine on the left side of the page. This displays all the SNMP-enabled devices on the same LAN.
2. Select an SNMP set in the drop-down list.

> **Note:** If you don't see any SNMP sets in the drop-down list, visit the **SNMP Sets** page, select an SNMP set, then click the **Save As** button to make a copy of it. Make a copy of an SNMP set that is similar to the device you want to monitor, just to experiment with. For example, if you want to monitor a router, make a copy of an SNMP set for routers. If you want to monitor a printer, make a copy of a printer SNMP set, and so on. The first time you use an SNMP set, you don't have to be concerned if some of the objects in the SNMP set don't apply to the device you want to monitor. You can **edit your copy of an SNMP set** *(page 20)* anytime before or after you assign it to a machine.

3. Select one or more discovered SNMP-enabled devices.
4. Click the **Apply** button.
5. Wait about15 minutes for SNMP-enabled devices to return SNMP monitoring data to the VSA. Then display monitoring results in the **SNMP Log** *(page 18)* page.

SNMP Log

The **SNMP Log** page displays the results from SNMP monitored devices, in chart or table formats, after they are assigned to a device using **Assign SNMP** *(page 16)*. It takes about 15 minutes for data to display in the page after the SNMP set is assigned to the device. Some objects in the SNMP set may not return data. Data not being returned can occur if a particular object in the SNMP set does not apply to the device. Or the object may be correct for the device, but happens to be currently inactive. Browse through the various objects in the SNMP set on this page until you find one that is returning data. Familiarize yourself with how the display of data can be changed using the various controls.
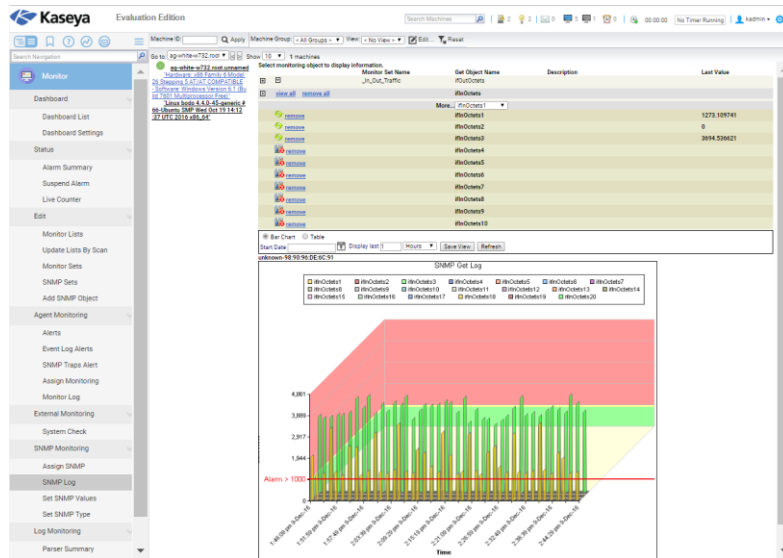
To select the data to display:

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.

SNMP Concepts

Before attempting to edit an SNMP set you should familiarize yourself with the following SNMP concepts.

Three Types of SNMP Messages

Three kinds of SNMP messages are supported by the VSA.

1. **Get "read" messages** - The SNMP-enabled device responds to a "get" SNMP request from SNMP management software, such as a a VSA agent on a machine. *Most SNMP functions in the VSA—including SNMP Sets—involve Get messages.*

2. **Set "write" messages** - SNMP management software, such as the VSA, writes a value to the MIB object on an SNMP-enabled device. This might be done for reference purposes or to change the behavior of the device. One VSA page executes SNMP set messages: **Set SNMP Values**.

3. **Trap "listen" messages** - Messages sent by an SNMP-enabled device to a "listening" agent, without being requested to do so, based on some event the device has encountered. One VSA page configures and responds to SNMP trap messages: **SNMP Traps Alert** (page 26).

MIB Objects

Editing the SNMP sets used by the VSA to monitor SNMP devices requires a basic understanding of MIB objects and MIB files. If you're already familiar with these concepts, skip to **Editing SNMP Sets** *(page 20)*.

Each SNMP-enabled device responds only to a specific set of SNMP requests. Each SNMP request is uniquely identified by an object ID, or **OID**. For example, an OID called `ifInOctets` is represented by the numerical-based OID `.1.3.6.1.2.1.2.2.1.10`. The corresponding character-based OID for `ifInOctets` is `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets`.

Each device manufacturer publishes the OIDs supported by the SNMP-enabled devices they manufacturer in the form of a **MIB file**, so OIDs are usually called **MIB objects**. The MIB files can be imported into a MIB management application, such as the VSA. The VSA comes pre-installed with many popular MIB objects, so importing MIB objects is usually only required for devices with specialized MIB objects.

Within the VSA, MIB objects are combined to create an **SNMP set**. After a network is scanned, SNMP sets are assigned to a SNMP-enabled device on the same network and used to monitor the performance of that device.

MIB Tree

Manufacturers have attempted to standardize the identification of MIB objects they use in devices by organizing them into a MIB Tree. Routers, for example, may use many of the same MIB objects, and only have few a specialized MIB objects that differ to support their particular product.

You can use either the numerical-based OID or the character based OID to locate the position of the MIB object on the tree. Below is an example of a character-based MIB tree.
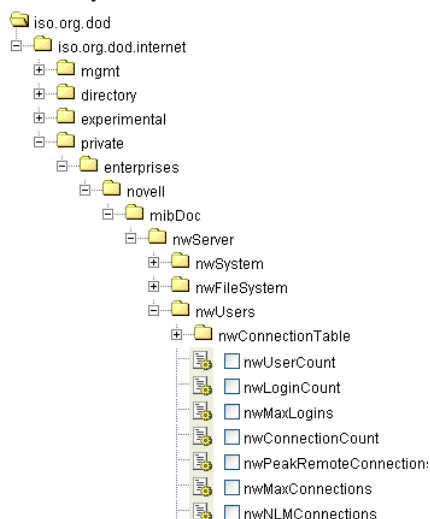
MIB Objects in the Monitor Lists Page

Within the VSA you can see a listing of all MIB objects currently available to include in an SNMP set. Select the Monitor > **Monitor Lists** page, then click the **MIB OIDs** button to see a table similar to the one below. You can add MIB objects to the list by importing MIB files into the VSA to support a particular

SNMP-enabled device. See **Adding SNMP Objects** *(page 25)*.

Editing SNMP Sets

SNMP Sets - Part 1

In the VSA select Monitor > **SNMP Sets**, then select a particular sample SNMP set, to see a table view of columns similar to the one in the image below.

This SNMP set example displays a pair of MIB objects belonging to the parent MIB object called `IFEntry`. `IFEntry` objects monitor the flow of data into and out of a device, such as a cable plugged into the port of a switcher. In TCP/IP terms, this point in the flow of data is referred to as the *interface* of the device, so `IFEntry` means "interface entry". The MIB object `ifInOctets` specifically refers to the number of 8-bit bytes, called "octets" in this case, flowing into a single interface. The MIB object `ifOutOctets` is the number of 8-bit bytes flowing out of a single interface.

Using just these two MIB objects you can monitor the data rate into and out of a network connection and assign an alarm threshold if the data flow exceeds a certain value.

MIBObject	SNMP Version	SNMP Instance	Data Type	Name	Description
ifEntry.ifInOctets	1	1-3	ratePerSecond	ifInOctets	
ifEntry.ifOutOctets	1	1-3	ratePerSecond	ifOutOctets	

MIBObject - The MIB object identifier is based on the last two levels of its character-based OID. For example, in the first row the complete character-based OID for this MIB object is `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets`, so the first column in the table displays `ifEntry.ifInOctets`.

SNMP Version - SNMP is an evolving protocol. Version 1 is supported by all devices and is the default. Version 2c defines more attributes, such as additional datatypes, and encrypts the packets to and from the SNMP agent. *Only select version 2c if you know the device supports version 2c.*

SNMP Instance - There may be multiple instances of a MIB object on a single device. For example, a switcher has many ports. You can specify the range of instances on a device that you want to monitor, such as `1-5,6` or `1,3,7`. If there is only one instance of a MIB object on the device, specify a `0` or leave it blank.

Value Returned as - If the MIB object returns a numeric value, you can choose to return the value as a **Total** or a **Rate Per Second**. Typically for interface monitoring, you'd rather know the rate of data flowing into and out of a port, so `IfInOctets` and `IfOutOctets` are set to rate per second. MIB objects that return a string instead of a number don't display this extra field in SNMP Sets.

Name and Description - These are the "friendly" identifiers for a MIB object. You can change their defaults

in the Monitor > Monitor List page or change them within a SNMP set.

SNMP Sets - Part 2

The next set of columns in the table view specify the *collection threshold* and *alarm threshold* for the values returned by the device to the VSA.

Name	Collection Operator	Collection Threshold	SNMP Timeout	Alarm Operator	Alarm Threshold	Duration	Re-Arm Alarm
ifInOctets	Over	-1	2 sec	Over	1000000	30 sec	1 days
ifOutOctets	Over	-1	2 sec	Over	1000000	30 sec	1 days

Collection

Minimize the collection of log data on the VSA by using a collection threshold that only brings back data when it matters to you. If you want everything, and the **Collection Operator** is `Over`, then set the **Collection Threshold** to `-1`, meaning everything greater than -1.

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

Alarms

Specify when an alert condition occurs. This doesn't mean an alarm will necessarily be triggered. The triggering of an alarm for an alert condition is decided when the SNMP set is assigned to a device.

- **Alarm Operator** - For character string return values, the options are `Changed`, `Equal` or `NotEqual` to the **Alarm Threshold**. For numeric return values, the options are `Equal`, `NotEqual`, `Over`, `Under` or `Percent Of`. Selecting the `Percent Of` option displays a new **Percent Object** field. The **Percent Object** serves 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.
- **Re-Arm Alarm** - Suppress additional alert conditions for this same issue for this time period. This reduces the confusion of many alert conditions for the same issue.

SNMP Sets - Part 3

The last few columns in the table view of an SNMP set address being notified *before* an alert condition occurs. These are less frequently used than the previous columns.

Warning alarms and **trending 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.

Name	Warning%	Trend Activated?	Trending Window	Re-Arm Trending
ifInOctets	10	No - Trending is not need...	14 days	1 days
ifOutOctets	10	No - Trending is not need...	14 days	1 days

Warning Alarms

- **Warning %** - Optionally display a *warning alert condition* when the returned value is within a specified percentage of the **Alarm Threshold**. A warning icon displays instead of a an alarm.

Trending Alarms

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.
- **Re-Arm Trending** - Suppresses additional trending alert conditions for this same issue during this time period.

Advanced SNMP Features

Manually editing an SNMP set implies you know the MIB objects that should or should not belong to a device and the collection and alarm threshold values that should be assigned to it. But what if you're not sure what these are for a particular device? Two advanced discovery features are provided in Monitor > **Assign SNMP** *(page 16)* to help you:

- **Quick Sets** (page 22) - A limited SNMP "walk" is performed on an SNMP device to discover the MIB objects actively being used on the device. You can select just the MIB objects that have values and create a "quick set" to begin monitoring the device immediately. The latest value is shown for each MIB object when you create the quick set.
- **Auto Learn** (page 24) - You can use the initial value displayed when creating a quick set—or the pre-defined values in a standard SNMP set—and hope for the best. Or you can enable Auto Learn for an applied quick set or standard set and let the monitoring agent calculate the appropriate thresholds for you. By default the learning cycle is for one hour. During this time Auto Learn determines the average value returned by a MIB object on a device and set thresholds for collection and alert conditions. You can change the auto learn criteria if you like, or modify the resulting calculations after auto learn has completed its cycle.

This **Advanced SNMP Features** section also discusses:

- **SNMP individualized sets** (page 24) - This is a standard SNMP set that is applied to an individual device and then customized manually.
- **SNMP types** (page 25) - This is a method of assigning standard SNMP sets to devices automatically, based on the **SNMP type** *(page 25)* determined during a network scan.
- **Adding SNMP Objects** (page 25) -   Add MIB objects to the VSA for an SNMP set if they're not already available.
- **SNMP traps** (page 26) - Configures alerts for a managed machine acting as a SNMP trap "listener", when it detects an **SNMP trap** message.

SNMP Quick Sets

The **SNMP Info** link page displays a list of MIB objects provided by the specific SNMP device you selected. These MIB objects are discovered by performing a limited SNMP "walk" on all discovered SNMP devices each time a **network is scanned** *(http://help.kaseya.com/webhelp/EN/KDIS/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** *(page 24)*, 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.

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

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

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

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

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

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

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

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".

Auto Learn 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 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.

Use the following procedure to configure SNMP auto learn settings in the **Auto Learn** popup window:

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

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

Individualized SNMP Sets

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

1. Select a *standard* SNMP set using the `<Select Monitor Set>` drop-down list.
2. Assign this standard SNMP set to a SNMP device. The SNMP set name displays in the **SNMP Info / SNMP Set** column.

3. Click the individualized monitor set icon in the **SNMP Info / SNMP Set** column to display the same options you see when defining a standard SNMP set. *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.

SNMP Types

Most SNMP devices are classified as a certain type of SNMP device using the MIB object `system.sysServices.0`. For example, some routers identify themselves as routers generically by returning the value 77 for the `system.sysServices.0` MIB object. You can use the value returned by the `system.sysServices.0` MIB object to auto assign SNMP sets to devices, as soon as they are discovered by a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/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.
2. Add or edit the value returned by the MIB object `system.sysServices.0` *and associated with each SNMP type* using the **SNMP Services** tab in Monitor > **Monitor Lists**.
3. Associate a SNMP *type* with a SNMP *set* using the **Automatic Deployment to** drop-down list in Monitor > SNMP Sets > Define SNMP Set.
4. Perform a **network scan** *(http://help.kaseya.com/webhelp/EN/KDIS/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:
- Assign a SNMP type to an SNMP device using Monitor > Set SNMP Type. Doing so causes SNMP sets using that same type to start monitoring the SNMP device.

Adding SNMP Objects

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 manually you can do so using Monitor > Add SNMP Object 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. 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.
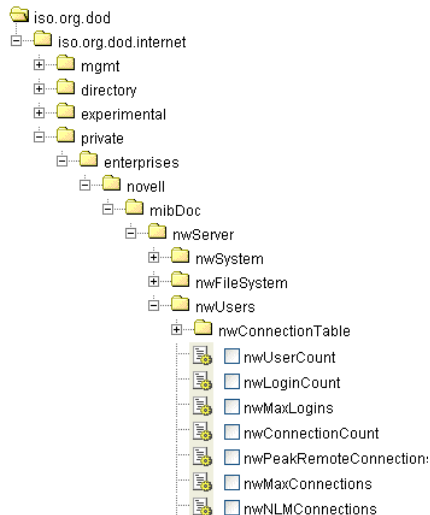
SNMP Traps

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.

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.*

SNMP Sets

You can review alarms for SNMP Trap alerts using the Monitor > **Alarm Summary** page.

Index