



Network Monitor

User Guide

Version R9

English

October 22, 2015

Agreement

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

Contents

Network Monitor Overview	7
Installation.....	9
Pre-Installation Checklist.....	9
Network Monitor Module Requirements.....	9
Server Sizing	9
Installing a New Instance of Network Monitor R9	10
Migration of KNM standalone to KNM integrated.....	11
Configuration Summary.....	14
Management Interface.....	15
Getting Started.....	16
The Monitoring View.....	16
Monitor tree	17
Inheritance.....	17
Crumblines	18
List Views	18
Node and User Search	19
List View Controls.....	19
List View Filtering	19
Data Views	21
Properties and Commands	22
Edit Menus.....	22
Moving Nodes	23
VSA Integration.....	24
Navigation Panel Overview	24
Integration with Discovery	25
Gateway Nodes and Network Discovery	27
Installing/Uninstalling Gateways.....	27
Organizations and Machine Groups	28
Renaming Gateways and Assets	29
Ticket action	29
User Integration	30
Network Monitor Licensing in the VSA.....	30
Gateways	30
Gateway Commands and Views.....	32
Assets tab	33
Monitors tab.....	33
Map tab.....	34
Toplist tab	34
Schedules tab.....	36
Knowledge tab.....	38

Audit tab.....	38
Editing Gateways	38
Basic properties edit tab - gateways.....	39
Advanced edit tab - gateways.....	39
Authentication edit tab	40
NOC edit tab	41
Groups	42
Group Commands and Views	43
Adding / Editing Groups.....	44
Basic properties edit tab - groups.....	44
Advanced edit tab - groups.....	45
Tags edit tab	45
Assets	47
Asset Commands and Views	47
Monitor tab.....	48
State change log tab	48
Editing Assets	49
Basic properties edit tab - assets.....	49
Advanced edit tab - assets.....	50
Dependency Testing.....	51
Asset Templates	52
Monitors.....	53
Monitor Commands and Views	55
Summary tab	56
Actions tab.....	56
Simulate alarm tab	59
Adding Monitors	59
Adding Preconfigured Monitors.....	60
Editing Monitors.....	61
Basic edit tab - monitors	63
Advanced edit tab - monitors	63
Alarm filtering edit tab - monitors	64
Statistics edit tab - monitors.....	64
Alarm Messages.....	65
Format Variables.....	66
Acknowledging Alarms	68
Reports	69
Viewing Report Templates	69
Viewing Quick Reports.....	70
Viewing Customized Reports	72
Emailing and publishing reports.....	72
Scheduling reports	73
Navigation Panel Reference	75
Navigation Panel Overview.....	75
Customized reports	77

Report templates	78
Report properties.....	78
Report styles	79
Report info.....	79
Report data types.....	80
Graphs	81
Data tables.....	82
Downtime report	83
Comments	84
Images.....	84
Toplists	84
Knowledge Base Articles.....	86
Knowledge Base Categories	87
Dashboard	88
Asset maintenance	89
Edit asset maintenance.....	89
Monitor maintenance.....	90
Edit monitor maintenance.....	90
User notification schedules.....	91
Edit user work schedule	91
Schedule blocks.....	92
Windows service list	92
MIB Browser.....	93
MIB Objects	93
Compiling Custom MIB Files	94
Record manager log.....	96
Syslog message.....	97
System administrator console	97
System log.....	99
Trap messages.....	99
My settings	99
Basic properties tab	100
Interface options tab.....	100
User notification groups	100
Create a new user group.....	100
Customized data types.....	101
Asset templates	101
Editing asset templates.....	102
Log settings	102
NOC settings	103
Other system settings	104
SMS settings	104
Default messages	107
Monitor Reference	109
Active Directory monitor.....	110

Bandwidth utilization monitor	111
CIM monitor	112
Citrix server monitor	113
CPU utilization monitor	114
Database server monitor	114
Datastore utilization	115
DHCP query monitor	115
Directory property monitor	116
Disk utilization monitor	117
DNS lookup monitor	117
Environment monitor	118
Event log monitor	118
Exchange server monitor	119
File change monitor	120
FTP server monitor	120
IMAP4 server monitor	121
JVM performance monitor	121
LDAP query monitor	122
Log file monitor	123
Lua script monitor	124
Mail server QOS monitor	124
Memory utilization monitor	125
MySQL monitor	125
NNTP server monitor	127
Oracle monitor	127
Ping monitor	128
POP3 server monitor	129
Process status monitor	129
Radius monitor	129
Salesforce query monitor	130
SMTP server monitor	131
SNMP monitor	131
SNMP trap monitor	132
SQL Server monitor	133
SSH2 script monitor	135
SSH2 server monitor	135
Swap file utilization monitor	135
Syslog monitor	136
TCP port scan monitor	136
Telnet server monitor	137
Terminal service monitor	137
TFTP server monitor	137
Transfer speed monitor	138
VMware performance monitor	138
Web server monitor	139

Windows performance monitor	140
Windows service status monitor	141
WMI Query monitor.....	141
Action Reference	143
Clear event log action	143
Execute command via SSH2 action.....	143
Execute Windows command action	144
HTTP Get/Post action.....	144
List reset action	146
Lua scripts action.....	146
Send mail action	146
Send message via PageGate action	147
Send SMS action.....	147
Send Wake-on-LAN packet action	148
SNMP Set action	148
Ticket action.....	149
Windows service control action.....	149
Scheduled Event Reference	150
Clear eventlog event.....	150
Execute command via SSH2/Telnet event	150
Execute Windows command event.....	151
Export statistics event	151
Generate report event	153
HTTP GET/POST request event.....	154
Lua scripts event	155
Send email event	155
Send message via PageGate event	155
Send SMS event.....	156
Send Wake-On-LAN packet event.....	156
SNMP Set event	156
Trigger monitor event.....	157
Windows service control event.....	157
Advanced Topics.....	159
Init.cfg parameters.....	159
Backup of Network Monitor	160
Data extraction reference.....	160
dir.....	161
monitor_graph.....	161
monitor_status_list.....	161
monitor_statusstring	162
monitor_uptimestring.....	162
device_xml.....	163
devicelist_xml	165
user_status.....	165
test_status	166

version	166
UNIX system support files	167
Enabling the ODBC Driver	169
Windows Troubleshooting and Performance Monitoring	173
Troubleshooting Windows monitoring and authentication	173
Network Monitor Service account and rights assignment	173
Monitors using Windows authentication.....	174
Event log monitor	174
Service monitor.....	174
External resources.....	174
Troubleshooting.....	175
Access denied	175
Network path can not be found	175
Performance related issues with monitored asset.....	176
The RPC server is unavailable.....	176
Windows performance registry	176
How to verify that KNM have access to remote registry service.....	177
Memory leaks in remote registry service on monitored machine	177
Caching of counters	178
Windows Management Instrumentation (WMI).....	178
Verifying that WMI is enabled for the account.....	179
Adjusting the firewall settings.....	181
Additional for non-administrator users.....	181
Verifying that WMI works	181
Full index of Microsoft WMI troubleshooting articles.....	183
Utilities Reference	185
Utilities Overview	185
Compiling Custom MIB Files	185
Lua.....	186
Gizmo	188
Dashboard Map Editor	189
Starting the Map Editor	190
Importing Map Images.....	190
Configuring Maps	191
Editing Map Nodes.....	192
Adding Map Nodes	192
Using the Organizer Tools	193
Publishing Maps	194
Bandwidth usage visualization	194
Creating a bandwidth connection	195
Index	197

Contents

Network Monitor Overview	7
Installation.....	9
Pre-Installation Checklist.....	9
Network Monitor Module Requirements.....	9
Server Sizing	9
Installing a New Instance of Network Monitor R9	10
Migration of KNM standalone to KNM integrated.....	11
Configuration Summary.....	14
Management Interface.....	15
Getting Started.....	16
The Monitoring View.....	16
Monitor tree	17
Inheritance.....	17
Crumblines	18
Lists Views	18
Node and User Search	19
List View Controls.....	19
List View Filtering	19
Data Views	21
Properties and Commands	22
Edit Menus.....	22
Moving Nodes	23
VSA Integration.....	24
Navigation Panel Overview.....	24
Integration with Discovery	25
Gateway Nodes and Network Discovery	27
Installing/Uninstalling Gateways.....	27
Organizations and Machine Groups	28
Renaming Gateways and Assets	29
Ticket action	29
User Integration	30
Network Monitor Licensing in the VSA.....	30
Gateways	30
Gateway Commands and Views.....	32
Assets tab	33
Monitors tab.....	33
Map tab.....	34
Toplist tab	34
Schedules tab.....	36

Knowledge tab.....	38
Audit tab.....	38
Editing Gateways	38
Basic properties edit tab - gateways.....	39
Advanced edit tab - gateways.....	39
Authentication edit tab	40
NOC edit tab	41
Groups	42
Group Commands and Views	43
Adding / Editing Groups.....	44
Basic properties edit tab - groups.....	44
Advanced edit tab - groups.....	45
Tags edit tab	45
Assets	47
Asset Commands and Views	47
Monitor tab.....	48
State change log tab	48
Editing Assets	49
Basic properties edit tab - assets.....	49
Advanced edit tab - assets.....	50
Dependency Testing.....	51
Asset Templates	52
Monitors.....	53
Monitor Commands and Views	55
Summary tab	56
Actions tab.....	56
Simulate alarm tab	59
Adding Monitors	59
Adding Preconfigured Monitors.....	60
Editing Monitors.....	61
Basic edit tab - monitors	63
Advanced edit tab - monitors	63
Alarm filtering edit tab - monitors	64
Statistics edit tab - monitors.....	64
Alarm Messages.....	65
Format Variables.....	66
Acknowledging Alarms	68
Reports	69
Viewing Report Templates	69
Viewing Quick Reports.....	70
Viewing Customized Reports	72
Emailing and publishing reports.....	72
Scheduling reports	73
Navigation Panel Reference	75
Navigation Panel Overview.....	75

Customized reports	77
Report templates	78
Report properties.....	78
Report styles	79
Report info.....	79
Report data types.....	80
Graphs	81
Data tables.....	82
Downtime report	83
Comments	84
Images.....	84
Toplists	84
Knowledge Base Articles.....	86
Knowledge Base Categories	87
Dashboard	88
Asset maintenance	89
Edit asset maintenance.....	89
Monitor maintenance.....	90
Edit monitor maintenance.....	90
User notification schedules.....	91
Edit user work schedule	91
Schedule blocks.....	92
Windows service list	92
MIB Browser.....	93
MIB Objects	93
Compiling Custom MIB Files	94
Record manager log.....	96
Syslog message.....	97
System administrator console	97
System log.....	99
Trap messages.....	99
My settings	99
Basic properties tab	100
Interface options tab.....	100
User notification groups	100
Create a new user group.....	100
Customized data types.....	101
Asset templates	101
Editing asset templates.....	102
Log settings	102
NOC settings	103
Other system settings	104
SMS settings	104
Default messages	107
Monitor Reference	109

Active Directory monitor	110
Bandwidth utilization monitor	111
CIM monitor	112
Citrix server monitor	113
CPU utilization monitor	114
Database server monitor	114
Datastore utilization	115
DHCP query monitor	115
Directory property monitor	116
Disk utilization monitor	117
DNS lookup monitor	117
Environment monitor	118
Event log monitor	118
Exchange server monitor	119
File change monitor	120
FTP server monitor	120
IMAP4 server monitor	121
JVM performance monitor	121
LDAP query monitor	122
Log file monitor	123
Lua script monitor	124
Mail server QOS monitor	124
Memory utilization monitor	125
MySQL monitor	125
NNTP server monitor	127
Oracle monitor	127
Ping monitor	128
POP3 server monitor	129
Process status monitor	129
Radius monitor	129
Salesforce query monitor	130
SMTP server monitor	131
SNMP monitor	131
SNMP trap monitor	132
SQL Server monitor	133
SSH2 script monitor	135
SSH2 server monitor	135
Swap file utilization monitor	135
Syslog monitor	136
TCP port scan monitor	136
Telnet server monitor	137
Terminal service monitor	137
TFTP server monitor	137
Transfer speed monitor	138
VMware performance monitor	138

Web server monitor	139
Windows performance monitor	140
Windows service status monitor	141
WMI Query monitor	141
Action Reference	143
Clear event log action	143
Execute command via SSH2 action	143
Execute Windows command action	144
HTTP Get/Post action	144
List reset action	146
Lua scripts action	146
Send mail action	146
Send message via PageGate action	147
Send SMS action	147
Send Wake-on-LAN packet action	148
SNMP Set action	148
Ticket action	149
Windows service control action	149
Scheduled Event Reference	150
Clear eventlog event	150
Execute command via SSH2/Telnet event	150
Execute Windows command event	151
Export statistics event	151
Generate report event	153
HTTP GET/POST request event	154
Lua scripts event	155
Send email event	155
Send message via PageGate event	155
Send SMS event	156
Send Wake-On-LAN packet event	156
SNMP Set event	156
Trigger monitor event	157
Windows service control event	157
Advanced Topics	159
Init.cfg parameters	159
Backup of Network Monitor	160
Data extraction reference	160
dir	161
monitor_graph	161
monitor_status_list	161
monitor_statusstring	162
monitor_uptimestring	162
device_xml	163
devicelist_xml	165
user_status	165

test_status	166
version	166
UNIX system support files	167
Enabling the ODBC Driver	169
Windows Troubleshooting and Performance Monitoring	173
Troubleshooting Windows monitoring and authentication	173
Network Monitor Service account and rights assignment	173
Monitors using Windows authentication.....	174
Event log monitor	174
Service monitor.....	174
External resources.....	174
Troubleshooting.....	175
Access denied	175
Network path can not be found	175
Performance related issues with monitored asset.....	176
The RPC server is unavailable.....	176
Windows performance registry	176
How to verify that KNM have access to remote registry service	177
Memory leaks in remote registry service on monitored machine	177
Caching of counters	178
Windows Management Instrumentation (WMI).....	178
Verifying that WMI is enabled for the account.....	179
Adjusting the firewall settings.....	181
Additional for non-administrator users	181
Verifying that WMI works	181
Full index of Microsoft WMI troubleshooting articles	183
Utilities Reference	185
Utilities Overview	185
Compiling Custom MIB Files	185
Lua.....	186
Gizmo.....	188
Dashboard Map Editor	189
Starting the Map Editor	190
Importing Map Images.....	190
Configuring Maps	191
Editing Map Nodes.....	192
Adding Map Nodes	192
Using the Organizer Tools	193
Publishing Maps	194
Bandwidth usage visualization	194
Creating a bandwidth connection	195
Index	197

Network Monitor Overview

Network Monitor is a web-based monitoring solution for monitoring the performance and availability of a wide array of network assets. **Network Monitor** monitoring is *agentless*, meaning it does not install any software or files on monitored machines. **Network Monitor** comes with more than 40 built-in methods of monitoring. These methods can be extended using Lua scripts. Advanced **Network Monitor** features include multi-level alarm escalations, and the ability to configure alarm dependencies so that service providers only receive the most relevant alarms. All common operating systems are supported, including:

- AIX (4.2 and above)
- CentOS
- Debian
- Fedora
- FreeBSD
- HP-UX
- Generic Linux
- OpenBSD
- OpenSUSE 10.2
- Red Hat Enterprise Server
- Solaris
- Ubuntu
- Windows






Terms and Concepts

- **Asset** - An asset represents a computer or any other type of network device that can be *addressed by an IP number or host name*. An asset contains settings that are common to all monitors associated with that asset.
- **Monitor** - A monitor tests a specific function in an asset. Most monitors are capable of collecting various statistical data for reporting purposes. When a monitor test fails consecutively a specified number of times, the monitor enters an *Alarm* state and executes a set of actions.
- **Group** - A group is a "container node" for other nodes in the **Network Monitor** monitor tree. Typically groups represent a logical business unit.
- **Actions** - One or more actions can be executed when a monitor fails a consecutive number of tests. A set of recovery actions can be executed when a monitor recovers from an *Alarm* state.
- **Asset template** - An asset template is used to assign a set of monitors to assets. Once assets are linked to an asset template, changes to the asset template are propagated to all the associated assets.
- **User group** - A **Network Monitor** user group is a set of VSA users who can be notified or scheduled to be available for notification. Each asset in **Network Monitor** is assigned to one user group. When a monitor enters an *Alarm* state, notifications are typically sent to the asset's user group.
- **Credential** - A credential is a username and password that authorizes access to a resource. **Network Monitor** stores credentials separately from the rest of the VSA. These credentials are used by monitors, actions and events to gain access to the appropriate resource when carrying out an operation.


Status Icons

A monitor is always in one specific state. This state is visualized in the **Network Monitor** interface with different colors. An asset or network always displays the *most important state reported by any single monitor* that belongs to it. Icons are listed below, ranked by their importance.






Network Monitor Overview

-  - The monitor is deactivated.
-  - This icon is used for assets and networks only. All monitors in the asset or network are deactivated, but the asset or network itself is active.
-  - The monitor has entered an alarm state.
-  - The monitor has failed one or more tests, but has not yet entered alarm state.
-  - The monitor is ok.

Additional guidelines:

- Any state other than deactivated is an activated state.
- An activated monitor tests its asset.
- Deactivating  any or all monitors of an asset does not deactivate the asset.
- Deactivating any or all assets of a network does not deactivate their parent network.
- Deactivating an asset deactivates *all* of its member monitors.
- Deactivating a network deactivates *all* of its member assets.

Other Commonly Used Icons

-  - This icon displays the properties of an item and allows you to edit them.
-  - This icon indicates that the asset or monitor is inherited from a template. Monitors inherited from a template can not be edited directly.
-  - This icon indicates that the asset or monitor is in maintenance state and is not currently monitored.
-  - This icon displays a list of items.
-  - This icon displays a view of an item.

Note: See **System Requirements** (<http://help.kaseya.com/WebHelp/EN/VSA/9000000/reqs/index.asp#home.htm>).

Chapter 1

Installation

In This Chapter

Pre-Installation Checklist	9
Network Monitor Module Requirements	9
Server Sizing	9
Installing a New Instance of Network Monitor R9	10
Migration of KNM standalone to KNM integrated	11
Configuration Summary	14

Pre-Installation Checklist

Completing the following pre-installation checklist before installing **Network Monitor** is recommended.

1. Estimate the memory required by **Network Monitor** to monitor the number of assets on your network, using the recommendations in **Server Sizing** (page 9). Ensure the system hosting the **Network Monitor** server has enough free memory to run **Network Monitor**.
2. Check that the system hosting the **Network Monitor** server meets **all software and hardware requirements** (page 9).
3. If a GSM phone is used, install it and verify that it responds correctly to standard AT commands in a terminal program.

When completed you are ready to install **Network Monitor**.

Network Monitor Module Requirements

Systems Hosting the Network Monitor R9 Server

- Windows Server 2008, 2008 R2, 2012, 2012 R2 with the latest service pack
- Network Monitor should use TCP/IP port 1433 to connect to your SQL Server instance
- Microsoft .Net Framework 4.5 or later

Dashboard Map Editor utility

- Microsoft .Net Framework 4.0 or later

Server Sizing

Recommended minimum requirements for **Network Monitor** depend on the number of assets you intend to monitor, assuming 10 monitors per asset.

Note: A **Network Monitor asset** is a unique IP address. A **monitor** is a single test or metric of that asset. For example, a Windows machine, represented by a single IP address, might have many monitors, with each monitor returning data about a different performance metric for that machine.

Installation

Minimum requirements up to 100 assets

- 1 GHz CPU
- 2 GB memory
- 5 GB free disk space ⁽¹⁾

Minimum requirements up to 250 assets

- 2 GHz CPU
- 2 GB memory
- 10 GB free disk space ⁽¹⁾

Minimum requirements up to 500 assets

- Dual core >2 GHz CPU
- 4 GB memory
- 15 GB free disk space ^{(1) (2)}

Minimum requirements up to 1000 assets

- Intel 2 GHz Quad core CPU
- 4 GB memory
- 25 GB free disk space ^{(1) (2)}

Minimum requirements up to 1500 assets

- Intel 2 GHz Quad core CPU
- 4 GB memory
- 40 GB free disk space ^{(1) (2)}

Notes

¹ Disk consumption is noted per year for a normal installation with the described number of assets and monitors

² Kaseya recommends that **Network Monitor** be installed on a 1+0 Raid array with at least 4 GB of RAM for best possible report generation performance

Installing a New Instance of Network Monitor R9

Network Monitor R9 only runs as an integrated addon module with the VSA.

To add the Network Monitor R9 addon module to an existing VSA R9 on premise environment:

1. **Submit a support request** (<https://helpdesk.kaseya.com/home>) to have your VSA license updated to permit installing Network Monitor R9 as an addon module.
2. Run **Kaseya Server Setup** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/install/index.asp#home.htm>) on the system hosting your Kaseya Server. Click Start > All Programs > Kaseya > **Kinstall**.
3. In step **6. Enter Your Kaseya License Code** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/install/index.asp#10338.htm>) of the **Kaseya Server Setup** installation wizard, accept or re-enter your new license code and click **Next**.
4. Complete the installation or upgrade of your VSA.
5. Logon to your instance of the VSA and navigate to the **Network Monitor** module.

Migration of KNM standalone to KNM integrated

Understanding the migration process

The migration of data from **Network Monitor** standalone to **Network Monitor** integrated with the VSA is a *mapping process* between two datasets.

The goal of the mapping process is to find and map each asset in the standalone configuration with a corresponding asset in the VSA configuration. Doing so preserves the monitoring configurations defined for each asset and their thresholds, reports, actions, schedules and historical data.

To successfully perform this mapping process there needs to be one network for each gateway in the original standalone configuration and one device for each asset, where the device and asset MAC address are the same.

Note: See "What do I do when I find an unmapped asset?" in the FAQ section below.

Preparing the KNM configuration

- Make sure you are on the latest version of KNM v5 (Build 9977).
- Make sure your license covers the number of devices you currently have in standalone.
- Remove all unnecessary gateways and devices.
- Uninstall all gateways on their remote network Windows machines.
 - Use Windows Add/Remove Programs on each Windows machine hosting a gateway to uninstall the gateway. If not present, use `nmservice.exe -u` in a command box to uninstall the gateway. Then delete the `KNM` installation directory to remove any leftover files.
 - For the local gateway, navigate to the local gateway directory and type `nmservice1g.exe -u`.
 - After the migration you will use agents to install and uninstall gateways.
- Archive all log files in the `<Kaseya_Installation_Directory>\knm\logs` directory, then delete these log files.
- Remove all operators (KNM users) from the standalone that do not have access to the VSA.

Discontinued feature and changed features

- Auto login is discontinued.
- **Network Monitor** no longer uses the SSL certificate specified by the `WEBSERVER_CERT` parameter in the `init.cfg` file. **Network Monitor** still supports using an SSL certificate but is configured as part of the VSA installation. For details, see [Using SSL Certificates](http://help.kaseya.com/webhelp/EN/VSA/9000000/install/index.asp#18015.htm) (<http://help.kaseya.com/webhelp/EN/VSA/9000000/install/index.asp#18015.htm>).
- All configuration data will be migrated to the SQL Server using by the VSA.

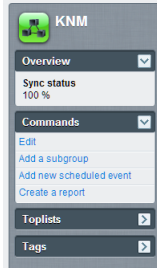
Before installing VSA R9

1. Make the necessary changes and clean up the configuration.
2. Copy the entire KNM folder structure to a safe place.
3. Using the Control Panel, run the uninstaller for Kaseya Network Monitor.
4. Copy the KNM folder created in step 2 to `%KASEYA_HOME%\knm`, where `KASEYA_HOME` is the intended folder where `KInstall` will install VSA.
5. Display the Windows Services console. Click Action > Refresh to verify that all the KNM services really are gone, before running `KInstall`.

Installation

After installing VSA R9

- The `nmservice.exe` process should be running. The `ksubscribers` database should have a new namespace called `KNM`.
- Check the SQL server conversion in the resulting log file `<Kaseya_Installation_Directory>\knm\fbmigrator_log.txt`.
- When starting the integrated Network Monitor module for the first time inside the VSA, the module runs in *sync mode*. In **sync mode** existing VSA assets are mapped to migrated KNM device data. The interface will only show the mapped assets and their related entities, such as orgs, networks and machine groups. **Sync status** progress can be viewed in the property pane on the right side of the browser.



KNM is automatically restarted when 100% sync is reach, if 100% sync cannot be achieved, the user can manually terminate sync mode by running the `vsa-set-sync-complete` console command described below and restart the service.

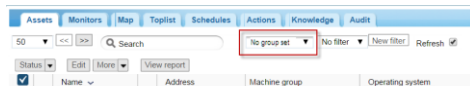
FAQ

What happens to my users?

- They are synced with users in the VSA if they have the same name. Please make any necessary adjustments in the VSA or KNM before performing the conversion.

I can't get 100% sync, can I find out which assets still not synced?

- Yes, in sync mode there is an extra option in the org/group selector that shows assets yet synced called "No group set"



What do I do when I find an unmapped asset?

- Devices that can't be mapped will appear in the `Unmapped group` in the KNM tree. While networks are being scanned assets will be checked against devices in this group, if they match up they will be removed from the unmapped group and placed in the relevant network. You will likely end up with a lot of devices that cannot be mapped. There are a number of different ways to deal with devices in the unmapped group.
 - They can get automatically mapped when scanning a network. If the asset belongs to a network not yet discovered, install an agent probe and scan the network using the **Discovery** module..
 - You can use the manual sync function. You should select one device and then use the manual sync command. This is done from the unmapped group only. The user is then prompted for an asset already received from the VSA that the device will be merged with. This way old data such as statistical data is preserved.
 - You can use the **Add asset** function. You should select a number of devices from the unmapped group and choose this command. This command works in bulk. You will then have to select a machine group that the assets will be created in. Once you click OK the assets will be created and they should be visible in the **Discovery** module.

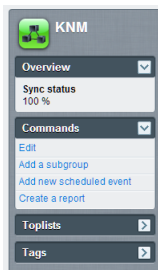
- They can be permanently removed from the configuration by selecting devices and choosing the **Delete** command.

Do I need to attain 100% sync?

- No, you choose what to migrate and what to leave out, if you are happy with what you see in the configuration, you can terminate the sync at any point using the system admin command line.

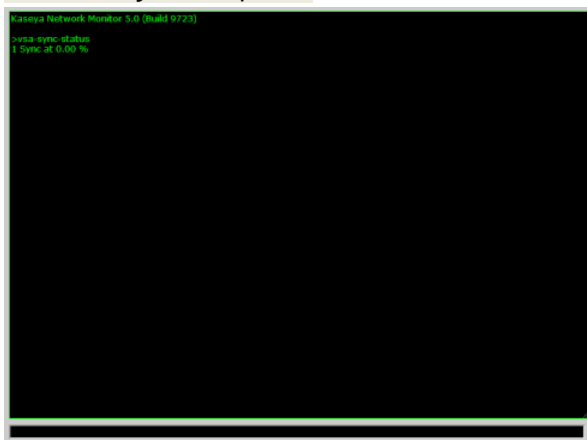
Is the sync percentage shown anywhere in the interface?

- Yes, in the property pane of the KNM node.



What console commands are available for this operation?

- `vsa-sync-status` - Shows the status in percent per tenant.
- `vsa-set-sync-complete` - Restarts KNM after a successful sync.



Configuration Summary

If you're new to **Network Monitor** R9, the following configuration sequence is recommended to help you evaluate the product. Each step includes a link to a more detailed explanation of how to perform that step.

1. Review the **Pre-installation Checklist** (page 9), **Server Sizing** (page 9) and **Network Monitor module requirements** (page 9) topics.
2. Perform the steps described in **Installing a New Instance of Network Monitor R9** (page 10).
3. **Logon to the VSA** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#264.htm>).
4. Review the **Getting Started** (page 16) section of this documentation to familiarize yourself with the module's user interface.
5. Run **Network Discovery** (page 25).
6. **Install a gateway** (page 27) on a discovered network.
7. **Add preconfigured monitors** (page 60) to selected assets.
8. Change the settings for the monitor threshold so as to force the monitor test to fail. This will enable you to watch the **Alarm Status Progression** (page 53).
9. Define **actions** (page 56) that are executed when a monitor fails a test a consecutive number of times.
10. Test the monitor by creating a **Simulate Alarm** (page 59) report to confirm the alarm is configured as you expect.

Chapter 2

Management Interface

In This Chapter

Getting Started	16
VSA Integration	24
Gateways	30
Groups	42
Assets	47
Monitors	53
Reports	69

Getting Started

In This Section

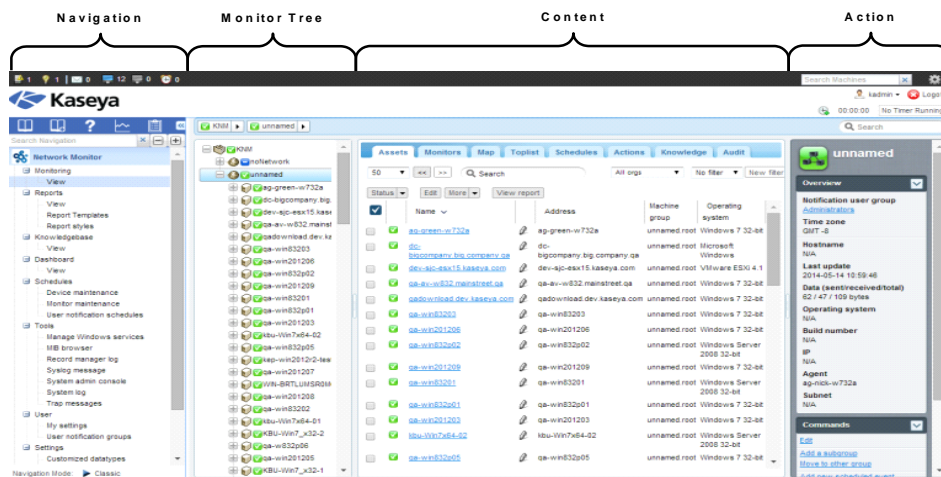
The Monitoring View	16
Monitor tree	17
Inheritance	17
Crumblin	18
Lists Views	18
Node and User Search	19
List View Controls	19
List View Filtering	19
Data Views	21
Properties and Commands	22
Edit Menus	22
Moving Nodes	23

The Monitoring View

Network Monitor > Monitoring > View

The Network Monitor > Monitoring > **View** is the view you work with most often in **Network Monitor**. When selected, the entire screen is divided into four panels.

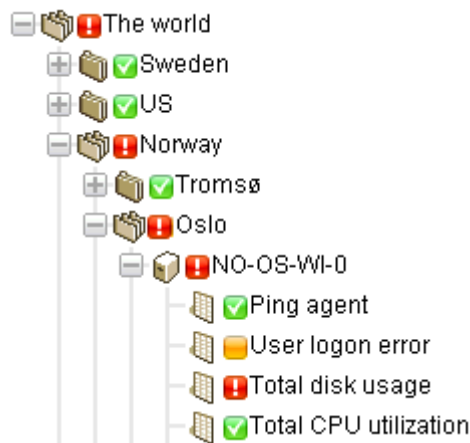
- **Navigation** - Displays the three other panels when you select the VSA > Network Monitor > Monitoring > **View** item in the navigation panel. Other items in the navigation panel provide access to **module-level settings and other views** (page 24).
- **Monitor Tree** - Selects the group, gateway, asset or monitor you want to work with.
- **Content** - Displays user content and settings—such as assets, monitors, or maps—either in a list view, a data view or as tabbed properties sheets.
- **Action** - Displays the main properties and commands you can perform for a selected node.



Monitor tree

The monitor tree organizes all groups, gateways, assets and monitors managed by **Network Monitor**. Using the tree you can quickly browse to any asset and monitor.

- **Gateways** - A gateway monitors assets sharing the same subnet. For a standard install of **Network Monitor** there is only one **Local gateway** and it refers to the same network the **Network Monitor** server is installed on.
- **Groups** - Used to group other nodes on the monitor tree. Groups do not correspond to a physical asset on a network. Think of them as representing logical business units, such as companies or departments, or a set of assets within a network.
 - A node cannot be the child of more than one parent. This includes a subgroup node.
 - Groups can have sub-groups.
 - Groups can be added above or below a gateway.
- **Assets** - Anything with an IP address. This includes computers, routers, switchers, mobile devices, printers, firewalls, etc.
- **Monitors** - A monitor runs a specific test on an asset and reports the result back to the server. An asset can have multiple monitors.



Inheritance

Certain node properties can be **inherited** by nodes at a lower level. This design enhancement affects nearly every other aspect of configuration. With inheritance you can propagate configuration changes to hundreds, even thousands, of assets and monitors effortlessly, simply by making changes to a higher level node in the monitor tree.



Management Interface

For any one node you can elect to use either an inherited setting or override it. For example, the image below shows a setting that is inherited from a higher level node. You'll spot this same convention used throughout the **Network Monitor** user interface for many different types of properties. *Note that overriding an inherited setting affects all lower level nodes inheriting the changes you make.* Inheritance is enabled by default for every property that supports it.

Alert and recovery settings

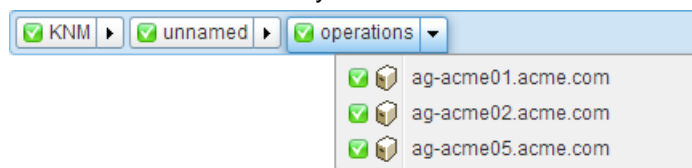
Inherit notification group: ☒ From: [KNM](#)

Inherit alarm messages: ☒ From: [KNM](#)

Inherit alarm actions: ☒ From: [KNM](#)

Crumbline

A crumbline at the top of the monitor tree shows you the currently selected node in the tree. You can click anywhere in the crumbline to jump to that node in the monitor tree. Or you can select one of the child nodes of the currently selected node.



Lists Views

The tabbed middle panel shows the contents of any node selected in the monitor tree. If the selected node is a group, gateway or asset, you'll see a list like the one below.

50 << >> Search All orgs No filter New filter

Name	Address	Machine group	Operating system
ag-acme01.acme.com	ag-acme01.acme.com	unnamed.root	Microsoft Windows
ag-acme02.acme.com	ag-acme02.acme.com	unnamed.root	Microsoft Windows
ag-acme05.acme.com	ag-acme05.acme.com	unnamed.root	Microsoft Windows XP
ag-cher-w732a	ag-cher-w732a	unnamed.root	Windows 7 32-bit
ag-cher-w732b	ag-cher-w732b	unnamed.root	Windows 7 32-bit
ag-ed-w732a	ag-ed-w732a	unnamed.root	Windows 7 32-bit
ag-ed-w732b	ag-ed-w732b	unnamed.root	Windows 7 32-bit
ag-ed-w732c	ag-ed-w732c	unnamed.root	Windows 7 32-bit
ag-erik-w732a	ag-erik-w732a	unnamed.root	Windows 7 32-bit
ag-erik-w732b	ag-erik-w732b	unnamed.root	Windows 7 32-bit
ag-erik-w764c	ag-erik-w764c	unnamed.root	Windows 7 32-bit
ag-jacob-w732a	ag-jacob-w732a	unnamed.root	Windows 7 32-bit
ag-jacob-w732b	ag-jacob-w732b	unnamed.root	Windows 7 32-bit
ag-jacob-w764c	ag-jacob-w764c	unnamed.root	Windows 7 32-bit
AG-KS-XP32A-177	AG-KS-XP32A-177	unnamed.root	Microsoft Windows XP
ag-merce-w73213	ag-merce-w73213	unnamed.root	Windows 7 32-bit
ag-merce-w73216	ag-merce-w73216	unnamed.root	Windows 7 32-bit
ag-merce-w73219	ag-merce-w73219	unnamed.root	Windows 7 32-bit
ag-merce-w732a	ag-merce-w732a	unnamed.root	Windows 7 32-bit
ag-merce-w732b	ag-merce-w732b	unnamed.root	Windows 7 32-bit
ag-merce-w764c	ag-merce-w764c	unnamed.root	Windows 7 32-bit
AG-NICK-2003R2	AG-NICK-2003R2	unnamed.root	Microsoft Windows XP
ag-nick-w732a	ag-nick-w732a	unnamed.root	Windows 7 32-bit
ag-nick-w732b	ag-nick-w732b	unnamed.root	Windows 7 32-bit

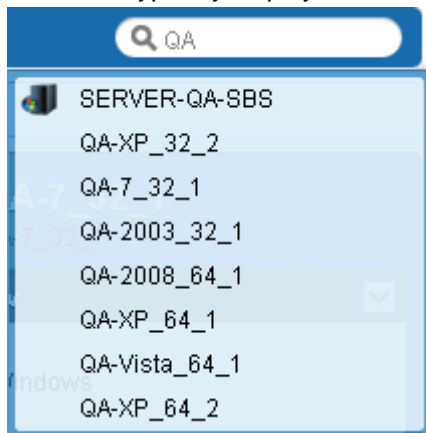
You can see all the assets and monitors that are members of that group or gateway. For example:

- The **Assets** tab displays all the *assets* that are members of the selected node in the hierarchy.
- The **Monitors** tab displays all the *monitors* that are member of the selected node in the hierarchy.

Node and User Search

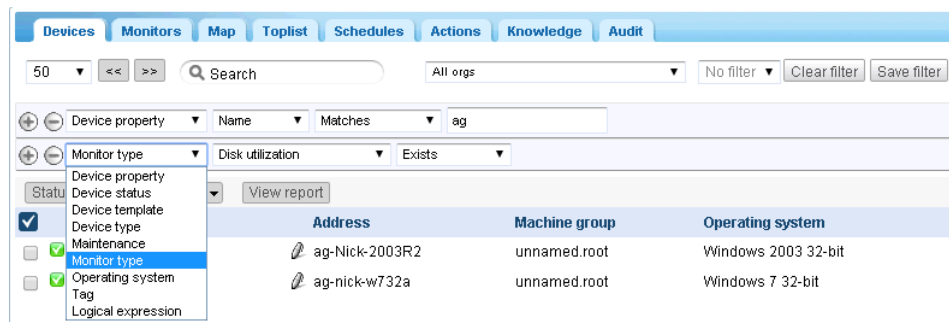
A **Search** edit box displays in the upper right hand corner. Enter a string to search the monitor tree for all *group*, *gateway* and *asset* nodes that match the string entered. **Do not press the Enter key.** Just wait for the list of nodes to be displayed below the edit box, then select one to display that node.

- Searches include any text entered in the **Description** field of a node.
- Searches include the names and descriptions of users and user groups.
- List views typically display a similar **Search** edit box you can use to filter items in the list view.



List View Controls

Each list view provides a set of buttons at the top of the list that can be applied to multiple nodes in the list. You can also page forward, page back, and **filter a list view** (page 19). Click a column header to sort the list by that column.



List View Filtering

Filtering List Views by Search

You can filter list views using the **Search** field. The data you can search for depends on the list view you have selected.

When a Group is Selected	Assets tab	name, description, address and machine group name
	Monitors tab	name, asset name, machine group name

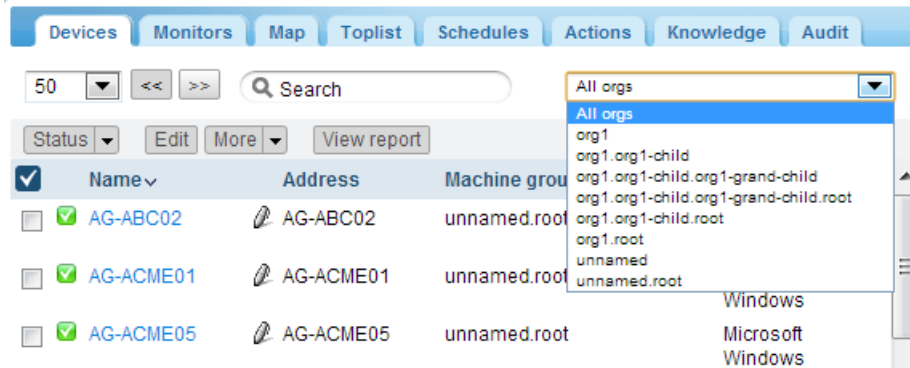
Management Interface

	Schedules tab	event/schedule description
	Knowledge tab	article ID, article title
	Audit tab	message text
When an Asset is Selected	Monitors tab	monitor name, type (e.g. 'CPU utilization')
	Knowledge tab	article ID, article title
	Audit tab	message text
	State change tab	message text
When a Knowledge Base Category is Selected	Articles	article ID, article Title
	Audit	message text

Filtering List Views by Machine Group and Organization

On any node with an **Assets** tab or **Monitors** tab in the **Network Monitor** module, you can filter by organization and machine group.

- An additional drop-down list displays with a default value of **All orgs**.
- Select any item in the **All orgs** drop-down list to filter the list of assets or monitors by that value.



- You can only see organizations and machine groups that have member assets found in the current network.
- Clicking a different gateway in the monitor tree typically shows a different set of organizations and machine groups.
- The list of organizations and machine groups that are visible to you are limited by your selected VSA **scope** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#4578.htm>).
- Filtering does not affect the display of assets in the **monitor tree** (page 27).

Filtering List Views by Multiple Conditions

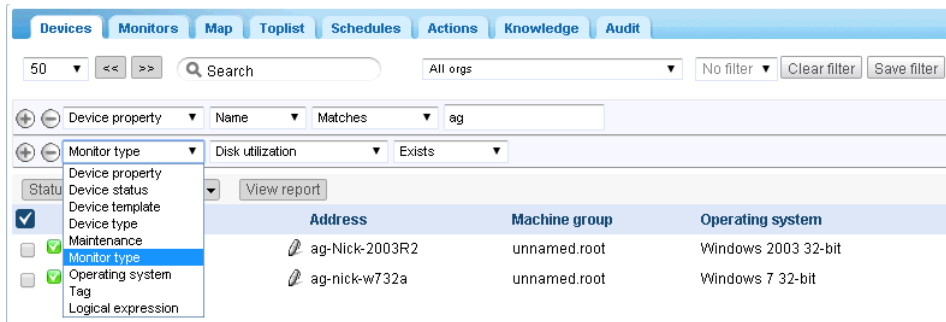
Asset tab and **Monitor** tab list views can be filtered by *multiple conditions*. Types of filters include:

- Asset property
- Asset status
- Asset template - The asset or monitor is or is not associated with an asset template.
- System type
- Tag
- Logical expression

The following actions are available with conditional filters:

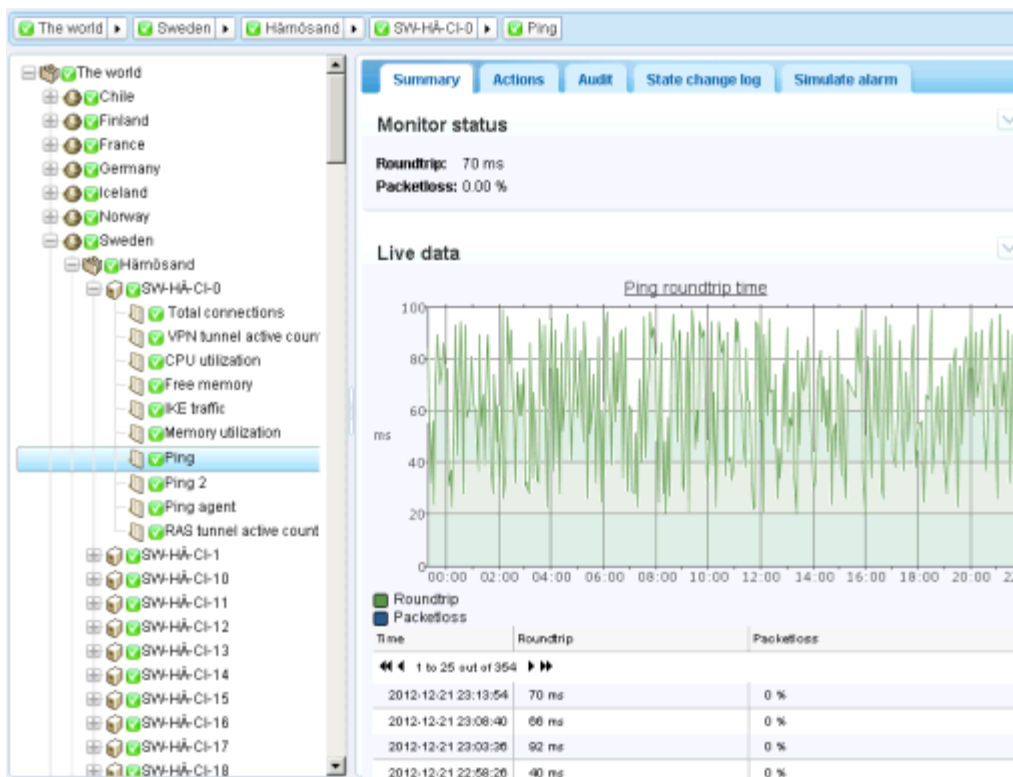
- **New filter** - Adds a new conditional filter.
- **Clear filter** - Clears a conditional filter from the list view.
- **Edit filter** - Displays a saved conditional filter so you can edit it.

- **Save filter** - Saves changes to a conditional filter.
- **Cancel edit** - Cancels edit changes to a conditional filter.
- **Delete filter** - Deletes a conditional filter.



Data Views

If the node selected in the monitor tree is a monitor, then the **Summary** tab shows the data returned by that monitor.



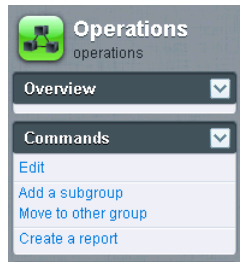
Properties and Commands

When a group, gateway, asset or monitor is selected, certain properties and commands display in the right hand pane.

Group Commands

When a **group** is selected, commonly used commands include:

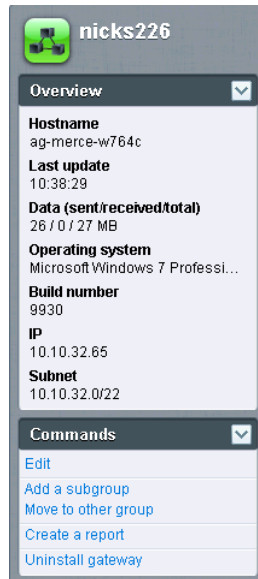
- Edit
- Add a group



Gateway Commands

When a **gateway** is selected, commonly used commands include:

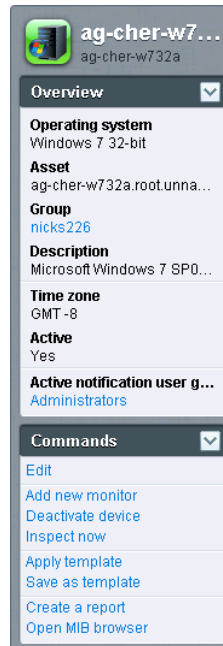
- Edit
- Add a group



Asset Commands

When an **asset** is selected, commonly used commands include:

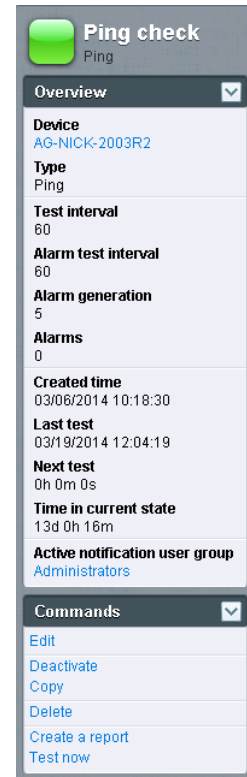
- Edit
- Add new monitor



Monitor Commands

When a **monitor** is selected, commonly used commands include:

- Edit
- Test Now



Edit Menus

When you click the **Edit** command for a selected node you typically see a tabbed set of properties sheets. Hovering the cursor over most fields displays a tooltip balloon on the right side, providing an explanation of the field.

Click the **Save** or **Cancel** button to close the edit menu and return to the **List View** (page 18) or **Data View** (page 21) of the selected node.

Edit device Basic properties Advanced Authentication NOC Tags

Basic properties

Name: ag-nick-w732a
 Address: ag-nick-w732a
 Operating system: Windows Windows 7 32-bit
 Device type: Other unidentified
 Description: Windows 7
 Free text:

Alert and recovery settings

Inherit notification group: ☒ From: nicks226 (Administrators)
 Inherit alarm messages: ☒ From: nicks226
 Inherit actions: ☒ From: nicks226

Save Cancel

Moving Nodes

Let's take a look at how the monitor tree can be reorganized by moving one branch of the monitor tree to the next. You can only move assets between groups *within the same gateway node*.

The screenshot shows the Management Interface with the monitor tree on the left and the list view on the right. The tree shows a hierarchy starting with 'KNM', followed by 'mercedesNN5', and then 'nicks226'. Under 'nicks226', there are several assets including 'Operations', 'ag-acme01.acme.com', 'ag-acme02.acme.com', 'ag-acme05.acme.com', 'ag-cher-w732a', 'ag-cher-w732b', 'ag-ed-w732a', and 'ag-ed-w732b'. A red arrow points from the 'nicks226' group in the tree to the 'Move' button in the list view. The list view shows a table of assets with columns for Name, Address, Machine group, and Operating system.

Name	Address	Machine group	Operating system
ag-acme01.acme.com	ag-acme01.acme.com	unnamed.root	Microsoft Windows
ag-acme02.acme.com	ag-acme02.acme.com	unnamed.root	Microsoft Windows
ag-acme05.acme.com	ag-acme05.acme.com	unnamed.root	Microsoft Windows XP
ag-cher-w732a	ag-cher-w732a	unnamed.root	Windows 7 32-bit

1. Select a gateway or group node.
2. Select the assets you want to move from the list view.
3. Click the **Move** button. The **Move assets** page displays.

Dashboard Monitoring Knowledge base

KNM Default group Kirkland Discovery group

Move devices

Selected devices

Device	Current group
QA-XP_64_1	Discovery group
QA-Vista_64_1	Discovery group
QA-XP_64_2	Discovery group

Select destination group

Search: Kirkland **Select**

Selected group:

Save Cancel

Management Interface

4. Enter text that matches the target node in the **Search** edit box. A drop-down list of possible nodes displays.
5. Click the target node in the drop-down list.
6. Click the **Select** button. The target node now displays in the **Selected group** field.
7. Click **Save**. The nodes are now moved to their new location in the monitor tree.

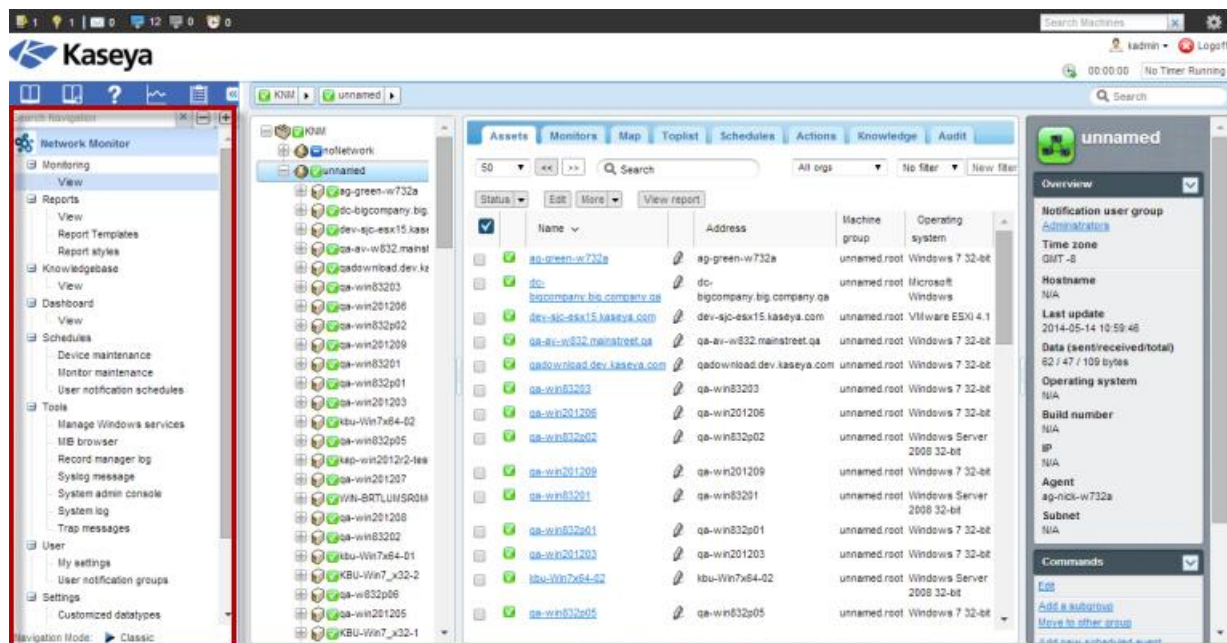
Note: You can also click the **Select** button to browse for a target node.

VSA Integration

Navigation Panel Overview

The **Network Monitor** navigation panel provides different views of content and enables you to configure module-level settings.

Note: The navigation panel takes the place of the "K menu" in earlier, standalone releases of **Network Monitor**.



These functions are detailed in the **Navigation Panel Reference** (page 75) included with this documentation. The following is a summary description of each option in the navigation panel.

Functions	Description
Monitoring > View (page 16)	Selects the monitoring view (page 16).
Reports > View (page 77)	Configures customized reports that are bound to selected sets of nodes.
Report Templates (page 78)	Configures report templates that can be applied to any set of nodes.
Report styles (page 79)	Configures the overall look of reports, report templates and customized reports.
Knowledgebase > View (page 86)	Selects the Knowledge base view.
Dashboard > View (page 88)	Selects the Dashboard view.

Asset maintenance (page 89)	Configures asset maintenance schedules.
Monitor maintenance (page 90)	Configures monitor maintenance schedules.
User notification schedules (page 91)	Configures Network Monitor user work schedules.
Management Windows services (page 92)	Selects the Management Windows services view.
MIB browser (page 93)	Selects the MIB browser view.
Record manager log (page 96)	Selects the Record manager log.
Syslog message (page 97)	Selects the Syslog messages view.
System admin console (page 97)	Selects the System admin console view.
System log (page 99)	Displays log entries created by the Kaseya Network Monitor service.
Trap messages (page 99)	Selects the SNMP Trap messages view.
My settings (page 99)	Selects the Edit my settings view.
User notification groups (page 100)	Maintains user groups. Asset notifications are sent to all members of the notification user group assigned to that asset.
Customized datatypes (page 101)	Creates customized data types for use with monitors capable of storing generic data.
Asset templates (page 101)	Configures sets of monitors that can be applied to an asset in one step.
Log settings (page 102)	Sets log policies for Network Monitor.
NOC configuration (page 103)	Creates customized NOC (Network Operations Center) views.
Other system settings (page 104)	Specifies additional settings for alerts and other events.
SMS (page 104)	Sets SMS message settings.

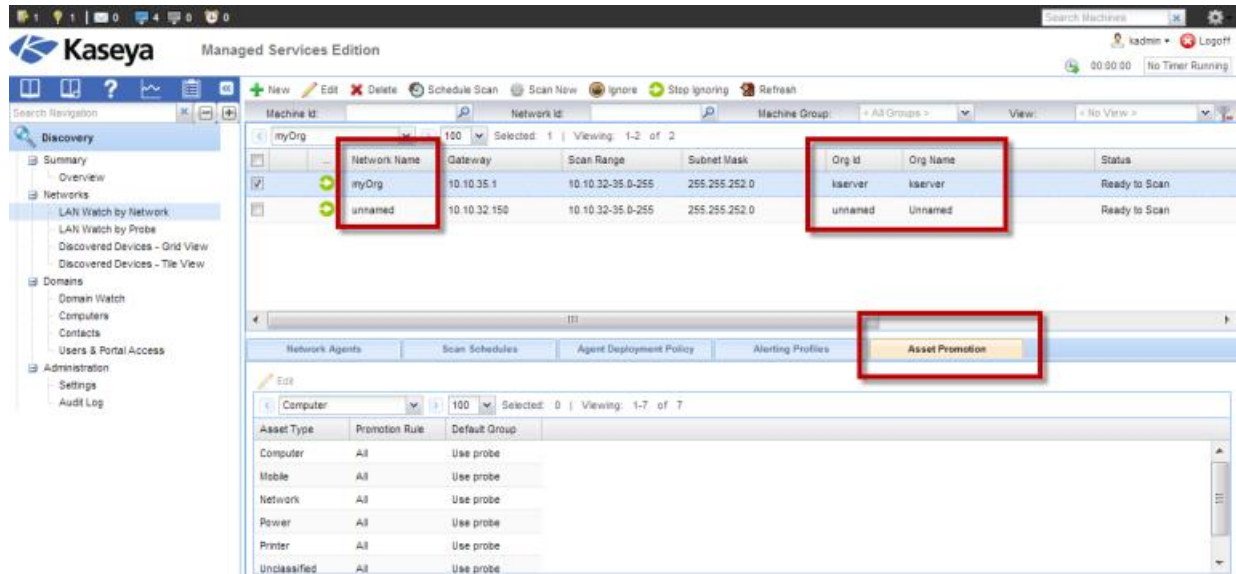
Integration with Discovery

Network Monitor uses the **Discovery** module to perform network discovery. With **Discovery** you only have to install a single agent on a single network machine to discover all the other devices on that network. Once detected, the network displays on the **LAN Watch by Network** (<http://help.kaseya.com/webhelp/EN/KDIS/9000000/index.asp#10627.htm>) page, as shown below.

- See the **Agent Deployment** (http://help.kaseya.com/webhelp/EN/VSA/9000000/EN_agentdeployment_R9.pdf#zoom=70&navpanes=0) quick start guide if you're new to working with agents.

Management Interface

- **Network Monitor** does not support adding or deleting managed devices (assets) manually within the **Network Monitor** module. A device must be discovered by **Discovery** and designated an asset for you to work with it in **Network Monitor**.



Network Discovery

1. Navigate to the Discovery Summary > **LAN Watch by Network** (<http://help.kaseya.com/webhelp/EN/KDIS/9000000/index.asp#10627.htm>) page.
2. Select the network row in the upper panel and click **Edit**.
3. Enter a **Network Name** that is easy to remember.
4. Specify the IP scan range or accept the default value.
5. Select the organization associated with this network.

Note: This assignment allows networks to be included or excluded in **scopes** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#4578.htm>). The scope you are using with your VSA user logon determines whether you can see the network in **Discovery** and the corresponding gateway node in **Network Monitor**. This assignment has no effect on the organization and machine group assigned to discovered assets.

6. Save but do not start the scan yet.

Asset Promotion

Any discovered devices you decide to manage in the VSA are called "assets" and must be associated with an organization and machine group to work with them after discovery. Agent assets are associated with an organization and machine group when an agent is installed. Marking a non-agent device as an "asset" is called *asset promotion*. **Network Monitor** only monitors assets.

Discovery automates the promotion of a device to an asset using the **Asset Promotion** tab. By default, all discovered devices are assigned the same organization and machine group as the agent probe used to scan devices on the network. You can choose to assign discovered devices to different organizations and machine groups if you like, based on asset type.

Scanning

Click **Scan Now** to begin detecting devices on the selected network immediately. You can also schedule device discovery on a recurring basis using the **Schedule Scan** button.

As soon as the scan starts you can navigate to the **Network Monitor** module and begin to see assets displayed in the **monitor tree** (page 27).

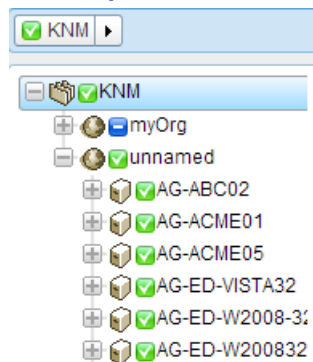
Gateway Nodes and Network Discovery

Gateway Nodes

Each network detected by **Discovery** displays as a gateway node underneath the top KNM node in the monitor tree. There is a one to one correspondence between networks detected in **Discovery** and gateway nodes shown in **Network Monitor**. You cannot delete a gateway node in the **Network Monitor** module of the VSA.

If you change the name of the network in **Discovery**, the name of the gateway node changes in the **Network Monitor** module.

Expand each gateway node to display the assets discovered on the network and marked as assets. The list of assets includes computers and devices installed with an agent and agentless computers and devices **promoted to an asset** (page 25).



Adding Groups Manually

You can add groups to gateway nodes. Recurring network discovery scans do not move re-discovered assets out of the groups they are assigned to.

Moving Assets


You can only move assets between groups *within the same gateway node*.

Installing/Uninstalling Gateways

Gateways collect monitoring data from assets connected to the same network as the gateway. The gateway then forwards that monitoring data to the **Network Monitor** server.

Gateways are installed on agent machines that are members of a **network discovered using the Discovery module** (page 25). All other assets on the network can remain agentless and **Network Monitor** will still be able to monitor them. The agent machine hosts the additional gateway software required to both collect monitoring data and relay it to the **Network Monitor** server.

Installing Gateways

If you have not installed a gateway for a gateway node yet, a blue  icon displays, meaning no connection can be made to the assets in the network. To install a gateway:

1. Select the *gateway node* in the monitor tree.

Management Interface

2. Click the **Install gateway** command.



3. **Select Agent** on the **Settings** tab. Select any Windows-based agent machine on the selected network and install a gateway on it.
4. Click the **Authentication** tab and enter a Window credentials that will allow you to install the gateway.
5. Click **Save** to initiate the installation of the gateway.

In less than a minute, all the blue icons should turn green, meaning all assets can be connected to and are capable of returning data to the **Network Monitor** module server. You can now begin to **add monitors** (page 59) or **add preconfigured monitors** (page 60) to assets.

Uninstalling Gateways

For the same network, you can uninstall a gateway on one agent machine and reinstall the gateway on a different agent machine. Uninstalling a gateway does not uninstall assets and monitors that are members of that gateway node. Reinstalling the gateway on a different agent machine on the same network allows assets and monitors to once again connect and return data.

Organizations and Machine Groups

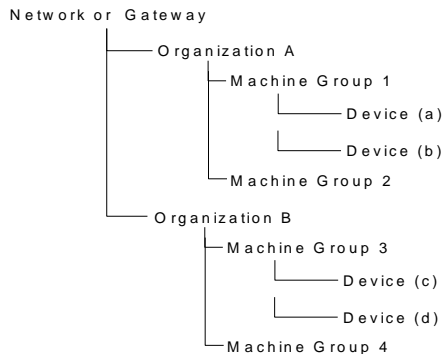
Organizations and machine groups are logical "containers" in the VSA used to organize all "assets" managed by the VSA. An asset is any machine or asset you choose to manage. Within the VSA you can assign any asset to any combination of organization and machine group.

Standard VSA hierarchies—networks, organizations, machine groups and managed assets—are mapped to the **Network Monitor** module as follows:

Discovery		Network Monitor
Networks	→	Gateways
		Create groups above a gateway node.
Organizations / Machine Groups	→	Filter asset lists and monitor lists by organization and machine group.
		Create groups below a gateway node.
Managed Assets (Machine or Asset)	→	Assets
		Monitors - added within Network Monitor

The Network Hierarchy

Each network can contain multiple organizations. For example, two teams from two different companies, could share the same network for an extended project. In this case the VSA would show a single network that includes assets from two different organizations and machine groups.



Note: Machine groups and organizations can be used to filter list views (page 19) in **Network Monitor**.

Renaming Gateways and Assets

You cannot rename gateways or discovered assets **promoted to an asset** (page 25) within the **Network Monitor** module. When you edit these nodes you'll notice their names are display only. The addresses of assets displayed in **Network Monitor** are display only as well. Navigate to the following locations to change the names of the gateway nodes and asset nodes displayed in **Network Monitor**.

Networks

- Rename the corresponding network for a gateway using the Discovery > **LAN Watch by Network** (<http://help.kaseya.com/webhelp/EN/KDIS/9000000/index.asp#10627.htm>) > **Edit** dialog.
- You can use the same **Edit** dialog above to change the organization assigned to the network.

Discovered Assets

Rename discovered *agent-less* assets using:

- Discovery > **Discovered Devices - Grid View** (<http://help.kaseya.com/webhelp/EN/KDIS/9000000/index.asp#10619.htm>) > **Rename Asset**
- Discovery > **Discovered Devices - Tile View** (<http://help.kaseya.com/webhelp/EN/KDIS/9000000/index.asp#10620.htm>) > **Rename Asset**

Change the organization and machine group assigned to agent-less assets promoted to an asset using:

- Audit > **View Assets** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#10649.htm>) > **Change Group**

Discovered *agent-less* devices can be removed from the **Network Monitor** monitor tree. Use the following to "demote" devices that are agent-less. This means you no longer wish to manage them throughout the VSA.

- Audit > **View Assets** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#10649.htm>) > **Demote Asset to Asset**

Ticket action

The **Ticket** action creates a ticket when triggered by an alarm count on an asset **Network Monitor** is monitoring. By default the **Ticket** action is inherited by all assets from the **KNM** group node. The alarm count is set to 1.

Note: A ticket is created in either the **Ticketing** module or **Service Desk**, depending on whether **Service Desk** has been **activated** (<http://help.kaseya.com/webhelp/EN/KSD/9000000/index.asp#5478.htm>) within the VSA.

Parameters

- **Alarm number** - The **alarm count** (*page 56*) this action triggers on.
- **User** - Select a default VSA user for the **Ticket** action. This is the VSA user assigned to the created ticket if no other VSA user is assigned.

User Integration

User logons for **Network Monitor** are created using System > **Users** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#4576.htm>).

- Access to nodes within **Network Monitor** are managed using System > **Scopes** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#4578.htm>). Access to any node depends on the organization and machine groups associated with that node and the selected scope you are using.
- Access to **Network Monitor** functions—such as items in the navigation panel—are managed using System > **User Roles** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#4577.htm>).
- Each VSA user is defined with a specified email address. Each user can update their own email address using System > **Preferences** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#503.htm>).

Note: See the **User Administration** (http://help.kaseya.com/webhelp/EN/VSA/9000000/EN_useradmin_R9.pdf#zoom=70&navpanes=0) quick start guide for more information.

User Notification Groups

The **User group list** (*page 100*) maintains user groups used by **Network Monitor**. A **Network Monitor** user group comprises VSA users.

Network Monitor asset notifications are sent to all members of the user group assigned to that asset using the **Notification user group** setting on the **Basic properties tab** (*page 49*) of the asset.

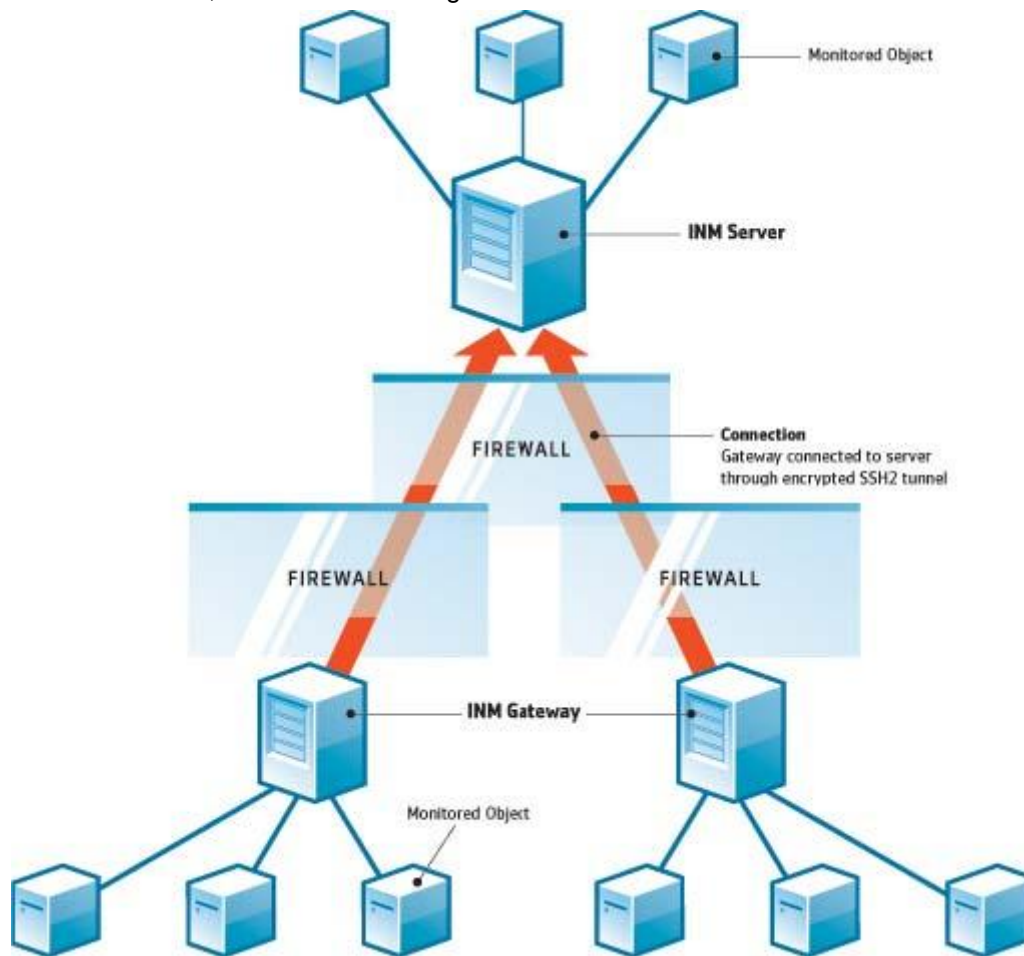
Network Monitor Licensing in the VSA

Used and available licenses for **Network Monitor** are displayed on the VSA > System > **License Manager** (<http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#2924.htm>) page. An agent license is consumed for each non-agent asset—machine or device—monitored using **Network Monitor**. A machine or mobile device that already has an agent installed on it does not consume an additional agent license when monitored by **Network Monitor**. One agent license is consumed for an asset regardless of the number of monitors on that asset.

Gateways

Network Monitor supports the monitoring of servers, routers and other types of assets on *multiple networks*. A **gateway** is installed on the server's local network and each remote network managed by **Network Monitor**. Assets are monitored by the gateway sharing their same network. Each gateway,

local and remote, sends its monitoring results back to the **Network Monitor** server.



Network Monitor Server

The **Network Monitor** server contains a database and management interface providing a consolidated view of all data returned by all gateways. Remote gateway assets are managed exactly the same as any local gateway. This makes **Network Monitor** very simple to configure and manage. This process is completely transparent to the user.

Network Monitor Gateway

A gateway acts on requests from the server. Except for a small cache file, gateways do not store any configuration or statistical data locally. All data is sent immediately to the server. The gateway must be installed on an agent machine.

Server and Gateway Communication

The data between a gateway and the server is always sent from the gateway to the server. The idea behind this solution is that more gateways than servers are deployed, so the administrator only has to open one port on the server firewall to allow communication.

If, for any reason, the gateway cannot connect to the server, the gateway starts buffering test results and statistics while waiting for the server. This buffering time can be configured per gateway.

Security and data integrity is achieved by using the state of the art communication protocol SSH2. The SSH2 protocol encrypts data with public key algorithms and protects connections from man-in-the-middle attacks. This is the same way VPN software establish secure tunnels over the internet.

Time Synchronization

Network Monitor automatically adjusts for time zone differences. The administrators must ensure the clock on gateways are synchronized with the clock in the **Network Monitor** server. We recommend that server and gateways be synchronized with a time synchronizing service such as NTP (Network Time Protocol). Failure to synchronize time between server and gateway **may lead to unpredictable results** in alarm generation and statistical storage.

Gateway nodes

Gateway nodes display as specialized nodes on the monitor tree. Gateway views, commands and properties are similar to **groups** (page 44). Gateway nodes have additional, specialized **properties and commands** (page 32) for managing a gateway installed on a network.

In This Section

Gateway Commands and Views	32
Editing Gateways	38

Gateway Commands and Views

Commands

These commands display when a gateway node is selected, regardless of the view tab selected at the top.

- **Edit** - Edits the **properties** (page 44) of a gateway.
- **Add a subgroup** - Creates a **new subgroup** (page 44) as a child node.
- **Move to other group** - Moves the selected gateway to another group.
- **Delete a group** - Deletes the currently selected gateway node. You cannot delete a group that has child nodes.
- **Add asset** - Adds an asset manually. Specify an asset name, IP address and asset type. Optionally specify a machine group.
- **Add new scheduled event** - Adds a **scheduled event** (page 36).
- **Create a report** - Creates a **report** (page 69).
- **Deploy gateway - Installs a gateway** (page 27) on an agent machine.
- **Uninstall gateway** - Uninstalls the gateway previously installed by the agent. Uninstalling a gateway does not uninstall assets and monitors that are members of that gateway node. Reinstalling the gateway on a different agent machine will allow assets and monitors to once again connect and return data.

Views

Gateways and groups share the same set of views.

- **Assets tab** (page 33) - This tab displays with gateways and groups.
- **Monitors tab** (page 33) - This tab displays with groups, gateways, and assets.
- **Map tab** (page 34) - This tab displays with gateways and groups.
- **Toplist tab** (page 34) - This tab displays with gateways, groups, and assets.
- **Schedules tab** (page 36) - This tab displays with gateways and groups.
- **Actions tab** (page 56) - This tab displays with groups, gateways, assets and monitors.
- **Knowledge tab** (page 38) - This tab displays with gateways, groups, and assets.
- **Audit tab** (page 38) - This tab displays with groups, gateways, assets and monitors.

Assets tab

This tab displays with gateways and groups.

The **Assets** tab displays all assets on multiple levels that are members of this node.

Actions

These are the actions available at the top of the list view when one or more assets are selected.

- **Status**
 - **Activate** - Activates selected assets—and all monitors assigned to those assets.
 - **Deactivate** - Deactivates selected assets—and all monitors assigned to those assets.
- **Edit** - Edits a selected asset. *If multiple assets are selected, edits only those properties shared by those assets.*
- **More**
 - **Move** - Moves selected assets—and all monitors assigned to those assets—to a group.
 - **Inspect Now** - Inspects *multiple* assets to determine the appropriate **pre-configured monitors** (page 60) for these assets. You may want to run **Inspect Now** if the credentials or configuration of the asset have changed. After running **Inspect Now**, click **Add New Monitor** for each asset to see the list of pre-configured monitors.
- **View report** - Generates a **report** (page 69) for selected assets.

Table Columns

- **Name** - The name of the asset.
- **Address** - The network name or IP address.
- **Machine group** - The machine group assigned to the discovered asset in **Discovery**.
- **Operating System** - The system type of the asset.

Monitors tab

This tab displays with gateways, groups, and assets.

The **Monitors** tab displays all monitors on multiple levels that are members of this node.

Actions

These are the actions available at the top of the list view when one or more monitors are selected.

- **Status**
 - **Acknowledge alarm - Acknowledges alarms** (page 68) on selected monitors.
 - **Activate** - Activates selected monitors.
 - **Deactivate** - Deactivates selected monitors.
- **Deletes** - Deletes selected monitors.
- **Edit** - Edits a selected monitor. *If multiple monitors are selected, edits only those properties shared by those monitors.*
- **Test Now** - Tests selected monitors immediately.
- **View report** - Generates a **report** (page 69) for selected assets.

Table Columns

- **Name** - The name of the monitor. Click the name of a monitor to jump to that node.
- **Asset** - The name of the asset. Click the name of the asset to jump to that node.
- **Type** - The **type of monitor** (page 109).
- **Status** - The value returned by the latest test.

Map tab

This tab displays with groups and gateways.

The **Maps** tab displays a large map when a map-enabled node is selected.

- The large map scales automatically to encompass the locations of all map-enabled *child nodes* of the currently selected node.
- Clicking a map location icon jumps to that node in the monitor tree. If an icon represents multiple child nodes *at the same location*, a list of child nodes displays. Clicking a child node jumps to that node in the monitor tree.

Smaller Map

A smaller map, in the lower right hand corner of the page, shows the location of the *currently selected node*.

Inheritance

Gateways, groups, and assets can be associated with a location on a map and a local time zone. Lower level nodes can inherit their geographical locations from their parent nodes. For example, setting the location of gateway or group for a single building can effectively set the location and local time zone for all the assets in the same building.

Configuration

Map settings are typically configured on the **Advanced** tab of a node. **Network Monitor** is integrated with the Google Maps API. This means you can use either the *name of a location* or *GPS coordinates* using decimal notation, such as `-33.469048, -70.642007`, to identify the location of any node.

Map and location settings

Inherit map settings: ☐ From: Aliso Viejo (33.575, -117.725556)

Map setting: Use google maps

Google map display: ☒ Gateway ☒ Groups ☒ Devices

Geographic location: San Clemente California

Inherit timezone: ☒ From: Aliso Viejo (GMT-12)

Map and location settings

- **Inherit map settings** - If checked, **map settings** (page 34) are inherited from the parent node and the other three map options remain hidden. Uncheck to specify your own map settings.
 - **Map setting** - Use google maps. This is the only option available at this time.
 - **Google map display** - Checking these options determines whether gateways, groups and assets are shown on the map.
 - **Geographic location** - Enter the *name of a location* or *GPS coordinates* using decimal notation, such as `-33.469048, -70.642007`.
- **Time zone** - Monitors display their real time charts in the asset's local time.
 - **Inherit time zone** - If checked, inherits time zone settings from the parent node. Uncheck to specify you own time zone settings.

Toplist tab

This tab displays with gateways, groups, and assets.

The **Toplist** tab displays the values returned by multiple assets *for the same type of monitor*. These

values are continuously updated in real time. This enables you to compare the values and identify poor performing monitors. Because multiple assets are required for a toplist, only gateways and groups display a **Toplist** tab. Toplists can also be included in **reports** (page 84).

Monitor	Device	Value
CPU utilization	NO-OS-CI-24	79.0 %
CPU utilization	UR-CI-CI-55	79.0 %
CPU utilization	IC-AK-CI-43	78.9 %
CPU utilization	US-SE-CI-85	78.9 %
CPU utilization	IC-RE-CI-63	78.9 %
CPU utilization	FI-HA-CI-32	78.9 %
CPU utilization	NO-BE-CI-50	78.8 %
CPU utilization	FI-LO-CI-59	78.8 %
CPU utilization	FI-UL-CI-80	78.8 %
CPU utilization	US-MI-CI-4	78.8 %
CPU utilization	SW-IQ-CI-86	78.7 %
CPU utilization	IC-RE-CI-37	78.7 %
CPU utilization	IC-KE-CI-86	78.7 %
CPU utilization	IC-RE-CI-22	78.7 %
CPU utilization	US-DA-CI-5	78.6 %
CPU utilization	SW-HA-CI-7	78.6 %
CPU utilization	NO-TR-CI-3	78.6 %
CPU utilization	US-DA-CI-47	78.6 %
CPU utilization	UR-PA-CI-56	78.6 %
CPU utilization	FI-UL-CI-50	78.5 %
CPU utilization	IC-HA-CI-78	78.5 %
CPU utilization	IC-HA-CI-36	78.5 %
CPU utilization	FI-TA-CI-35	78.4 %
CPU utilization	NO-TR-CI-99	78.3 %
CPU utilization	FI-VA-CI-61	78.3 %

Actions

- **Refresh** - If checked, refreshes the page.
- Choose one of the following:
 - **Snapshot** - A *snapshot* toplist displays the latest value for each monitor in the list.
 - **Stored list** - *Stored list* toplots display the *min*, *max* and *average* of monitor values, for a selected daily, weekly and monthly time periods.
- **Load** - Displays only if **Stored list** is selected. Displays the selected toplist.
- **Load for Compare** - Compares two toplots.

1. Select a *first* toplist and click **Load**.
2. Select a *second* toplist of the same **Type**, then click **Load to Compare**.

The *first* toplist displays on the on left. The second toplist displays on the right. You can now see how the monitored properties for a particular monitor changed between the two toplots.

The following **Sort** options can only be used when comparing two toplots.

- **Top movers** - Entries that have moved the most up or down.
- **Top climbers** - Entries that moved up the most.
- **Top fallers** - Entries that have moved down the most.
- **Type** - The toplist data type and unit of measure.
 - CPU utilization
 - Disk utilization
 - Free disk space
 - Bandwidth utilization

Management Interface

- Ping roundtrip time
- Ping packetloss
- Free memory
- Swap utilization
- Webpage fetch time
- **Data**
 - Sampled min value
 - Sampled max value
 - Period average
- **Sort**
 - Lowest entries first
 - Highest entries first
- **Entries** - Number of entries to display.

Table Columns

- **Asset** - The name of the asset. Click the name of the asset to jump to that node.
- **Monitor** - The name of the monitor. Click the name of the monitor to jump to that monitor.
- **Value** - The value returned by the latest test.

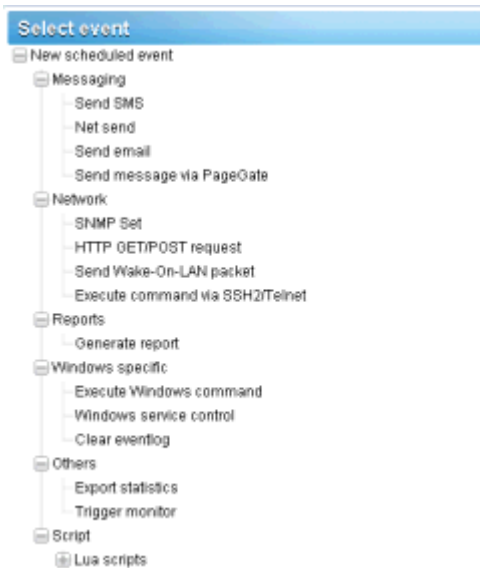
Schedules tab

This tab displays with gateways and groups.

The **Schedules** tab schedules actions for a specific date and time—instead of waiting for a monitor to trigger the action. Events can be scheduled to run once or repeatedly.

Note: Events are not inherited. Any group or gateway can schedule any event for any host. For security reasons, you should use schedule events from the gateway node or group of the asset you're targeting. This ensures scheduled events for these assets can be viewed only by users who are authorized to see them.

Click the **Schedules** tab for any gateway or group. The tab shows any previously scheduled events. Click the **Add schedule event** command. **A list of event actions displays** (page 150). Click one to edit the event.



The configuration details depend on the type of event action you select. When specifying a host, enter the DNS hostname or IP address. Scheduling an event from a parent group or gateway for the asset you're targeting is more likely to provide you with the appropriate credential, if one is required.

The 'Edit scheduled event' dialog box shows the 'Event configuration' section with the following fields: Run-once event (Run once selected, Repeating event unselected), Date (2012-10-30), and Time (15:00). The 'Windows service control' section includes: Hostname (SW-ST-WI-0), Service name (wuauerv), Type (Restart service), and Inherit credentials (checked, From: Stockholm). At the bottom are 'Save' and 'Cancel' buttons.

Scheduling

All events provide the same scheduling options.

Run Once Events

- **Date** - Enter the date.
- **Time** - Enter the time.

Repeating Events

- **Active between** - Specifies the date range the event repeats. Specify the range using a YYYY-MM-DD format. If these fields are left empty the event is always repeats.

- **Day of week** - By checking a day, the event repeats only on selected days of the week.
- **Hour(s) in day** - The hour and minute each day you want the event to repeat. Format is HH:MM, HH:MM, . . .
- **Last in month** - If checked, the event repeats the last day of every month.
- **Days in month** - If checked, the event repeats on specific days of the month. Specify days separated with a comma.

Knowledge tab

This tab displays with gateways, groups, and assets.

The **Knowledge** tab displays the list of knowledge base articles assigned to that node.

Actions

- **Attach article** - Assigns selected articles to selected groups and assets.
- **Detach article** - Unassigns selected articles from selected groups and assets.

Related Topics

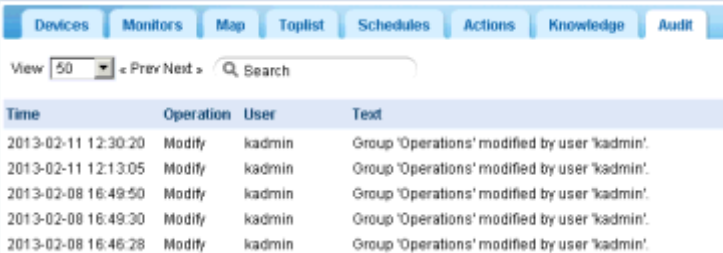
- **Knowledge Base Articles** (page 86)
- **Knowledge Base Categories** (page 87)

Audit tab

This tab displays with gateways, groups, assets and monitors.

An **Audit** tab displays on every node of the monitor tree. Log entries describe every configuration action performed by a **Network Monitor** user on the currently node.

Note: Searches are case sensitive.



The screenshot shows the 'Audit' tab selected in a navigation bar. Below the navigation bar is a search area with a 'View' dropdown set to '50', a '< Prev Next >' button, and a search input field. The main content is a table with the following data:

Time	Operation	User	Text
2013-02-11 12:30:20	Modify	kadmin	Group 'Operations' modified by user 'kadmin'.
2013-02-11 12:13:05	Modify	kadmin	Group 'Operations' modified by user 'kadmin'.
2013-02-08 16:49:50	Modify	kadmin	Group 'Operations' modified by user 'kadmin'.
2013-02-08 16:49:30	Modify	kadmin	Group 'Operations' modified by user 'kadmin'.
2013-02-08 16:46:28	Modify	kadmin	Group 'Operations' modified by user 'kadmin'.

Editing Gateways

(selected gateway) > Edit

The **Edit gateway** page configures the properties of a gateway node. Gateways nodes share many of the same properties as **groups** (page 44). Gateway nodes have additional, specialized properties and **commands** (page 32) for managing a gateway installed on a network.

- **Basic properties tab** (page 39) - Gateways, groups, and assets display a **Basic properties** edit tab.
- **Advanced tab** (page 39) - Gateways, groups, assets, and monitors display an **Advanced** edit tab.
- **Authentication tab** (page 40) - This edit tab displays with gateways, groups, and assets.
- **NOC tab** (page 41) - This edit tab displays with gateways, groups, and assets.

Basic properties edit tab - gateways

Gateways, groups, and assets display a Basic properties edit tab.

Basic properties

- **Name** - Enter a name for the gateway.
- **Description** - A longer description of the gateway.

Alert and recovery settings

- **Inherit notification group** - Sets the notification group for this node. For gateways, groups, and asset nodes you can override the default notification *user group* messages are sent to. Monitor nodes use the notification group specified by their parent asset node and cannot be overridden.
- **Inherit alarm messages** - Sets the **Alarm Messages** (page 65) format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** (page 56) of this node.

Advanced edit tab - gateways

Groups, gateways, assets, and monitors display an Advanced edit tab.

Map and location settings

- **Inherit map settings** - If checked, **map settings** (page 34) are inherited from the parent node and the other three map options remain hidden. Uncheck to specify your own map settings.
 - **Map setting** - Use google maps. This is the only option available at this time.
 - **Google map display** - Checking these options determines whether gateways, groups and assets are shown on the map.
 - **Geographic location** - Enter the *name of a location* or *GPS coordinates* using decimal notation, such as `-33.469048, -70.642007`.
- **Time zone** - Monitors display their real time charts in the asset's local time.
- **Inherit time zone** - If checked, inherits time zone settings from the parent node. Uncheck to specify you own time zone settings.

Group dependency settings

- **Select dependency monitor / Selected monitors** - Enter text to display the names of monitors in the **Select dependency monitor** list that match the text entered. Select one or more monitors in the list, then click the **Add** button to add the monitors to the **Selected monitors** list. You can also click the **Select** button to browse for target monitors. To remove a monitor, select it and click the **Remove** button.

Receive Syslog messages

- **Syslog server** - If checked, enables Syslog messages intercepted on the gateway's network to be forwarded to the server. Once checked, intercepted syslog messages display on the Network Monitor > Tools > **Syslog message** (page 97) page.
- **Port** - Defaults to 514.

Receive SNMP traps

- **SNMP trap** - If checked, enables SNMP trap messages received from the gateway's network to be forwarded to the server. The **SNMP trap** (page 132) monitor requires this checkbox be enabled. Once checked, received trap messages display on the Network Monitor **Tools > Trap messages** (page 99) page. You can create SNMP trap monitors directly from the **List syslog message** pages, based on selected messages.
- **IP** - The host name or IP number of the receiver of the traps.

Management Interface

- **Port** - Port number that the trap receiver listens to.
- **Community filter** - SNMP trap community string.
- **Agent IP range filter** - Filters the forwarding of SNMP trap messages by IP address.

Misc settings

- **Sync MIBs** - If checked, **Network Monitor** automatically updates this gateway with MIB files added to the server.
- **Notification group** - Group that is notified by email if the gateway does not connect in a timely fashion.
- **Disable auto update** - If checked, disables auto update. If blank, this gateway is automatically updated with the latest version of **Network Monitor** when the server is updated.

Authentication edit tab

This edit tab displays with gateways, groups, or assets.

The **Authentication** edit tab stores credentials used by **Network Monitor** to authenticate access to network assets. Credentials are managed *using inheritance*. That means you can set credentials for a single gateway or group in the monitor tree and all child assets and monitors will make use of them. Moreover you can be certain these same credentials will never be confused with other credentials set for other branches in the tree.

The screenshot shows the 'Authentication' tab in the Network Monitor interface. On the left is a tree view of the network hierarchy, with 'Germany' selected. The main panel is titled 'Edit gateway' and contains several sections for different authentication types: 'Windows domain credentials', 'SSH/Telnet credential', 'SNMP credential', 'VMware credential', and 'Additional credentials'. Each section has an 'Inherit credentials' checkbox and a 'From' dropdown menu. The 'Additional credentials' section includes a dropdown menu for 'CIM account' and an 'Add credential' button. At the bottom right are 'Save' and 'Cancel' buttons.

For any one type of authentication, if **Inherit credentials** is checked, the credentials are inherited from a higher level node. If the checkbox is unchecked, enter credentials for this type of authentication. These credentials will be used by this node and all lower level nodes that inherit this type of authentication. *If the name of specified credentials does not display in parentheses next the name of the higher level node, it means that credentials are not yet defined at the higher level node.*

Types of authentication include:

- **Windows domain credentials** - Specifies Windows local or domain credentials. Leave the **Domain or Computer** field blank or enter `localhost` to specify localhost credentials. Applies to multiple **monitors using Windows authentication** (page 174).
- **SSH Telnet credentials** - Specifies SSH and Telnet credentials.
- **SNMP credentials** - Specifies SNMP credentials. The required parameters depend on the version of SNMP used to connect to the asset:
 - **SNMP v1 or SNMP2c** - Enter the **Read community** name and **Write community** name.
 - **SNMP v3** - If authentication is required
 - ✓ **SNMPv3 Context ID** - Optional. A string matching one or several context IDs specified by the SNMP agent on the asset to limit the data returned.
 - ✓ **Auth method** - The algorithm used for authentication: `None`, `HCMA-MD5`, or `HCMA-SHA1`.
 - ✓ **SNMPv3 username** - The name of the SNMP manager used to access the SNMP agent on the remote asset.
 - ✓ **SNMPv3 Passphrase** - A sequence of words, similar to a password.
 - ✓ **SNMPv3 Encryption** - The algorithm used to ensure privacy using data encryption: `None`, `DES` or `AES-128`.
 - ✓ **SNMPv3 Crypto key** - The string used for data encryption.
- **VMware credentials** - Specifies VMware credentials.
- **Additional credentials** - You can add additional credentials for the following.
 - CIM account
 - Exchange account
 - FTP account
 - HTTP account
 - IMAP account
 - LDAP account
 - MySQL account
 - ODBC account
 - Oracle account
 - POP3 account
 - RADIUS account
 - SMTP account
 - SQL server account

NOC edit tab

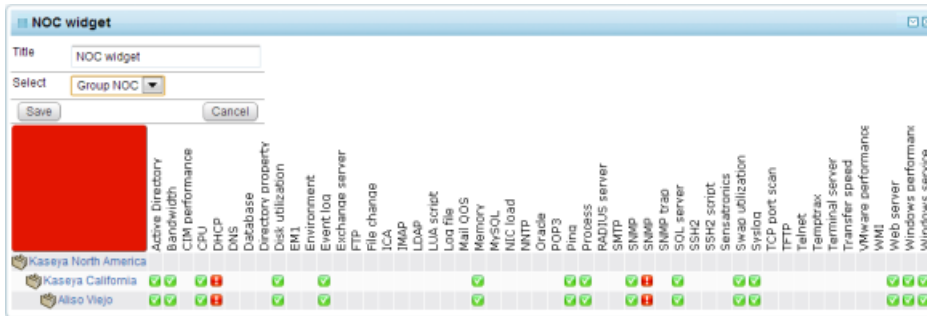
This edit tab displays with groups, gateways, or assets.

The **NOC** edit tab assigns a group, gateway or asset node to a *NOC view*.

Network Operation Center (NOC) widgets are compact, full-screen information views that display the status of a collection of networks and assets. They are normally displayed on dedicated monitors.

Management Interface

NOC views display group, gateway and asset status hierarchically, in a matrix format. All groups, gateways and assets are listed vertically, with the status for each monitor type horizontally. The overall status is shown in the large colored rectangle at the left.



Configuring a NOC view and widget

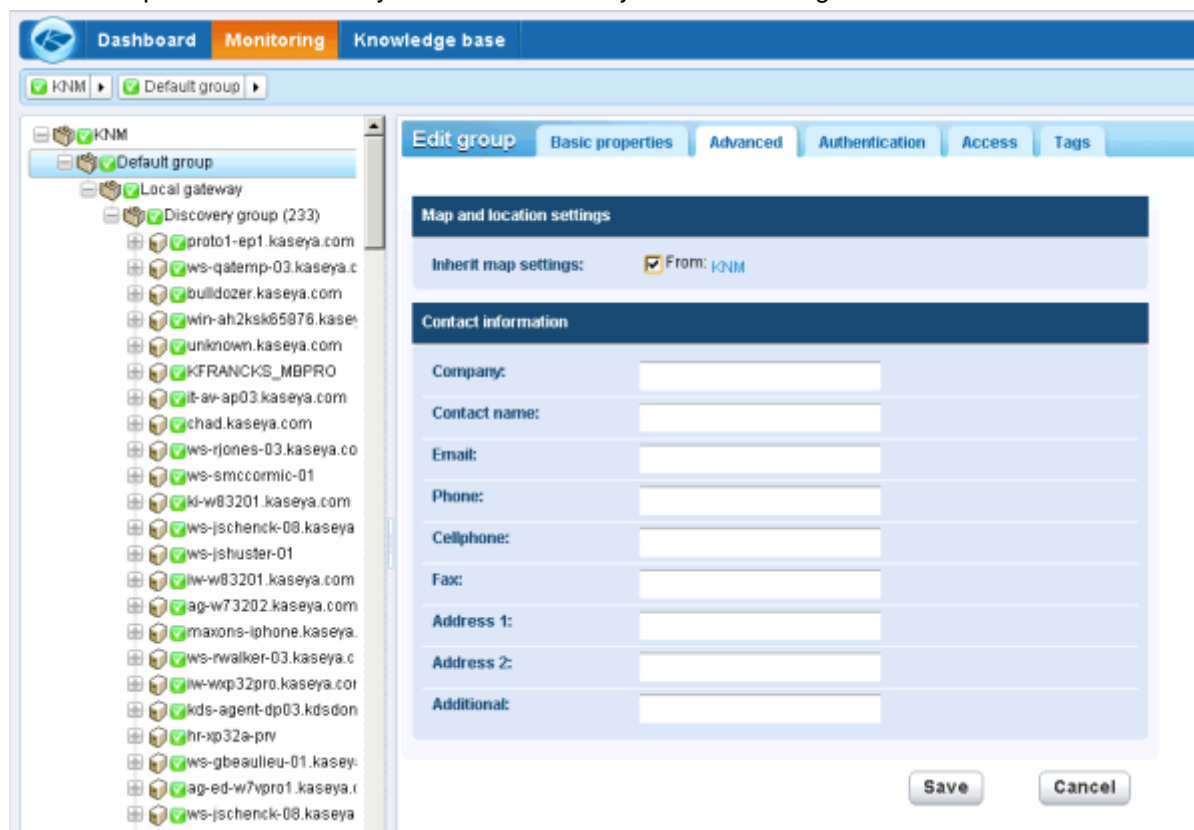
1. Define one or more NOC views using the Network Monitor Settings > **NOC configuration** (page 103) page.
2. A **gateway node** or **group node** must be assigned to at least one NOC view using the Edit > **NOC** tab.
3. Select Dashboard > Add widget > **NOC widget**.
4. Select the ☒ icon on the right side of the widget title bar to configure the following settings.
 - **Title** - The title displayed with the NOC widget on the dashboard.
 - **Select** - Select the default **Group NOC** or any other NOC view that you have created to display that NOC view.

Groups

Groups are "container" nodes used to group other nodes in the monitor tree.

- **Logical Business Units** - A group can represent a logical business unit. Rename the group to reflect the name of the business unit. When you **Edit** any group, click the **Advanced** tab. You'll notice contact information can be entered for the business unit a group represents. If an asset requires on-site intervention, display the asset's closest parent in the monitor tree for the contact information you need.

- **Specialized Service Requirements** - Even if assets don't represent a distinct business unit, you might have to deliver specialized services to a set of assets within a single subnet. It's easiest to distinguish these assets by grouping them together. In this case you might rename the group by the department name or by the set of services you are delivering.



Inheritance by Group

The power of groups goes far beyond organizing and labeling. When you edit a group you'll find it includes many properties, such as alert settings, authentication, access and map locations. This allows you to set properties for all the child assets of the group using inheritance. This can include nested groups, assets, and monitors.

If you take the time to organize the assets you manage by group and use the inheritance feature, it can greatly reduce the amount of time spent configuring assets individually.

The Root Node

The top-level node—called **KNM** by default—is really a "super" group node. Group properties set for the root node can be *inherited* by lower level nodes, just like any group you create. From the root node, settings can be potentially inherited *by every other node in the monitor tree*.

In This Section

Group Commands and Views	43
Adding / Editing Groups	44

Group Commands and Views

Commands

These same commands display when a group node is selected, regardless of the tab selected at the

top.

- **Edit** - Edits the **properties** (page 44) of a group.
- **Add a subgroup** - Creates a **new subgroup** (page 44) as a child node.
- **Move to other group** - Moves the currently selected group to another group.
- **Delete group** - Deletes the currently selected group.
- **Add asset** - Adds an asset manually. Specify an asset name, IP address and asset type. Optionally specify a machine group.
- **Add new scheduled event** - Adds a **scheduled event** (page 36).
- **Create a report** - Creates a **report** (page 69).

Views

Gateways and groups share the same set of views.

- **Assets tab** (page 33) - This tab displays with groups and gateways.
- **Monitors tab** (page 33) - This tab displays with gateways, groups, and assets.
- **Map tab** (page 34) - This tab displays with groups and gateways.
- **Toplist tab** (page 34) - This tab displays with gateways, groups, and assets.
- **Schedules tab** (page 36) - This tab displays with groups and gateways.
- **Actions tab** (page 56) - This tab displays with gateways, groups, assets and monitors.
- **Knowledge tab** (page 38) - This tab displays with gateways, groups, and assets.
- **Audit tab** (page 38) - This tab displays with gateways, groups, assets and monitors.

Adding / Editing Groups

(selected group or gateway) > Add a subgroup

(selected group) > Edit

The **Edit group** page configures the properties of a group node. Since groups are "container" nodes, most of the properties can only be used when inherited by lower level nodes.

- **Basic properties tab** (page 44) - Gateways, groups, and assets display a **Basic properties** edit tab.
- **Advanced tab** (page 45) - Groups, gateways, assets, and monitors display an **Advanced** edit tab.
- **Authentication tab** (page 40) - This edit tab displays with groups, gateways, or assets.
- **NOC tab** (page 41) - This edit tab displays with groups, gateways, or assets.
- **Tag tab** (page 45) - This edit tab displays with groups and assets.

Basic properties edit tab - groups

Gateways, groups, and assets display a **Basic properties edit tab**.

Basic properties

- **Name** - Enter a name for the group. Oftentimes a group corresponds to a logical business unit of a customer.
- **Description** - A longer description of the group.

Alert and recovery settings

- **Inherit notification group** - Sets the notification group for this node. For gateways, groups, and asset nodes you can override the default notification *user group* messages are sent to. Monitor nodes use the notification group specified by their parent asset node and cannot be overridden.
- **Inherit alarm messages** - Sets the **Alarm Messages** (page 65) format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** (page 56) of this node.

Advanced edit tab - groups

Groups, gateways, assets, and monitors display an Advanced edit tab.

Map and location settings

- **Inherit map settings** - If checked, **map settings** (page 34) are inherited from the parent node and the other three map options remain hidden. Uncheck to specify your own map settings.
 - **Map setting** - Use google maps. This is the only option available at this time.
 - **Google map display** - Checking these options determines whether gateways, groups and assets are shown on the map.
 - **Geographic location** - Enter the *name of a location* or *GPS coordinates* using decimal notation, such as `-33.469048, -70.642007`.
- **Time zone** - Monitors display their real time charts in the asset's local time.
 - **Inherit time zone** - If checked, inherits time zone settings from the parent node. Uncheck to specify you own time zone settings.

Contact information

Enter contact information for the business unit a group represents. If an asset requires on-site intervention, display the assets's closest parent in the monitor tree for the contact information you need.

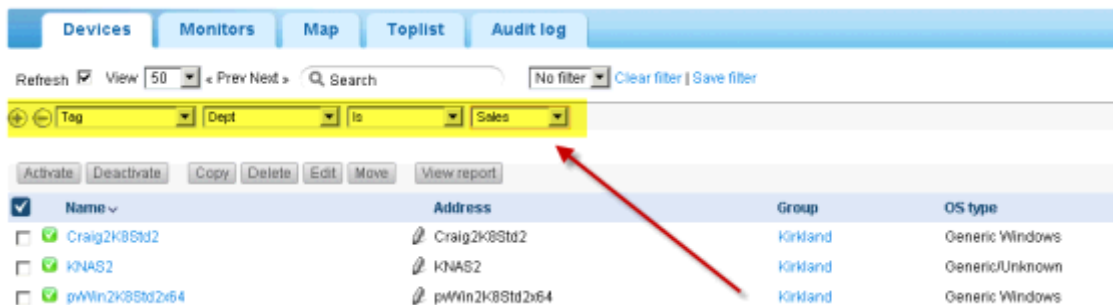
- **Company**
- **Contact name**
- **Email**
- **Phone**
- **Cellphone**
- **Fax**
- **Address 1**
- **Address 2**
- **Additional**

Tags edit tab

This edit tab displays with groups and assets.

The **Tags** edit tab creates, edits and assigns user-defined tags. You can create a tag using any node that displays a Tag tab. From then on the tag is available to assign to that node or nodes matching the tag's scope of assignment.

For example, you could classify assets by the department they belong to. You could create a **DEPT** tag with multiple values: Sales, Accounting, Marketing, Development, Manufacturing, Distribution. View lists can be subsequently filtered or reported on by their assigned tags. An example is shown in the image below.



For example, to create and assign tags to a node in the monitor tree, select a group or asset. Then click

Management Interface

Edit, then the **Tags** tab.

Tags

Available tags: Dept Attach tag

Name: Dept

Scope: ☐ Global ☒ Device

Data: ☐ None ☐ Text ☒ Choice ☐ Date

Choice text: Add choice

Current choices: Accounting Marketing Production Sales Remove choice

Store tag Cancel

Attached tags

Save Cancel

There are two types of **Scope** for a tag. The scope determines what other types of nodes can use the tag.

- **Global** - Any type of record can use the tag.
- **Asset** or **Group** - If an asset node has been selected, only other assets can use the tag. If a group node has been selected, only other groups can use the tag.

You must also specify the type of **Data** entry required for a tag, when a user assigns a tag to a node.

- **None** - No data is required. For example, you might simply assign a tag called `InMaintenance` and leave it at that.
- **Text** - The user can enter any kind of string. For example, a tag called `Note` allows the user to enter whatever they want.
- **Choice** - The user selects one of several fixed values. For example, a `LicenseStatus` tag could be set to one of three fixed values: `Licensed`, `Unlicensed` or `TrialEvaluation`.
- **Date** - The user selects a date. For example, a tag called `RepairDueDate` could represent the expected date of repair for an asset.

Deleting a Tag

- Click the red X next to an assigned tag to delete the assignment.

Assets

Network Monitor monitors assets. An **asset** represents a computer or any other type of network device that can be accessed by an IP number or host name. Each asset managed by **Network Monitor** displays as a separate node in the monitor tree. The parent node of an asset is either a gateway or a group. A selected asset node provides a list view of all the monitors assigned to that asset.

The screenshot shows the Network Monitor interface. At the top, there are tabs: Monitors, Actions, Knowledge, Toplist, Audit, and State change log. Below the tabs is a search bar and a 'Refresh' button. A row of buttons includes 'Activate', 'Deactivate', 'Acknowledge alarm', 'Copy', 'Delete', 'Edit', and 'View report'. The main table lists monitors for the asset 'dev-av-win0d' (10.10.32.6). The table has columns: Name, Type, Alarms, Status, and Next test. The right sidebar shows an 'Overview' section with details like OS type (Windows 2008 R2), Group (Operations), Time zone (GMT-12), Active status (Yes), and Active notification user group (Administrators). Below this is a 'Commands' section with options like Edit, Add new monitor, Deactivate device, Inspect now, Move device, Delete device, Apply template, Save as template, Create a report, and Open MIB browser. At the bottom of the sidebar is a 'Tags' section.

Name	Type	Alarms	Status	Next test
<input checked="" type="checkbox"/> Bandwidth utilization	Bandwidth utilization	0	0.0 / 0.0 %	0h 0m 37s
<input checked="" type="checkbox"/> CPU utilization	CPU utilization	0	10 %	0h 0m 9s
<input checked="" type="checkbox"/> Disk utilization	Disk utilization	0	7535 MB	0h 0m 15s
<input checked="" type="checkbox"/> Memory utilization	Memory utilization	0	3379 MB	0h 0m 37s
<input checked="" type="checkbox"/> Page faults/sec	Windows performance	0	305.20	0h 0m 9s
<input checked="" type="checkbox"/> Page reads/sec	Windows performance	0	3.00	0h 0m 9s
<input checked="" type="checkbox"/> Page writes/sec	Windows performance	0	0.00	0h 0m 9s
<input checked="" type="checkbox"/> Pages/sec	Windows performance	0	3.00	0h 0m 9s
<input checked="" type="checkbox"/> Ping check	Ping	0	1 ms	0h 0m 42s
<input checked="" type="checkbox"/> Security events	Eventlog	0	No matching event records found	0h 0m 27s
<input checked="" type="checkbox"/> SNMP	SNMP	0	2478.16	0h 0m 42s
<input checked="" type="checkbox"/> SNMP Table	SNMP Table	176		0h 0m 15s
<input checked="" type="checkbox"/> SQL Server	SQL Server	0	Operational	0h 0m 42s
<input checked="" type="checkbox"/> Web server	Web server	0	Request completed	0h 0m 42s
<input checked="" type="checkbox"/> Windows service status - Print spool service	Windows service status	119	Spooler not running	0h 0m 15s

Asset Commands and Views

Commands

These commands display when an asset node is selected, regardless of the view tab selected at the top.

- **Edit** - Edits the **properties** (page 49) of the asset.

Note: **Network Monitor** does not support adding or deleting assets manually within the Network Monitor module. An asset must be **discovered by Discovery** (page 25) for you to work with it in **Network Monitor**.

- **Add new monitor** - Adds a new monitor (page 59) to the asset.
- **Deactivate asset** - Deactivates the asset.
- **Inspect now** - Inspects an asset to determine the appropriate **pre-configured monitors** (page 60) for the asset. You may want to run **Inspect Now** if the credentials or configuration of the asset have changed. After running **Inspect Now**, click **Add New Monitor** to see the list of pre-configured monitors.
- **Apply template** - Applies an **asset template** (page 52).
- **Save as template** - Saves the set of monitors as an **asset template** (page 52).
- **Create a report** - Views, emails or publishes a **report** (page 69).
- **Open MIB browser** - Displays the list of OIDs supported by an asset that can be monitored using SNMP. An asset must be SNMP enabled to display OIDs.

Views

- **Monitor tab** (page 48) - This tab displays with gateways, groups, and assets.
- **Actions tab** (page 56) - This tab displays with gateways, groups, assets and monitors.
- **Knowledge tab** (page 38) - This tab displays with gateways, groups, and assets.
- **Toplist tab** (page 34) - This tab displays with gateways, groups, and assets.
- **Audit tab** (page 38) - This tab displays with gateways, groups, assets and monitors.
- **State change log tab** (page 48) - This tab displays with assets and monitors.

Monitor tab

This tab displays with gateways, groups, and assets.

Actions

These are the actions available at the top of the list view when one or more monitors are selected.

- **Acknowledge alarm - Acknowledges alarms** (page 68) on selected monitors.
- **Activate** - Activates selected monitors.
- **Deactivate** - Deactivates selected monitors.
- **Copy** - Creates selected monitors to selected assets.
- **Delete** - Deletes selected monitors.
- **Edit - Edits a selected monitor** (page 61). If multiple monitors are selected, edits shared **standard monitor properties** (page 63) of these monitors.
- **View report** - Generates a report for selected assets.

Table Columns

- **Name** - The name of the monitor.
- **Type** - The **type of monitor** (page 109).
- **Alarms** - The **alarm count** (page 53). This column is only displayed on asset nodes.
- **Status** - The latest result returned from the monitor.
- **Next test** - The next time the test is scheduled to be run.

State change log tab

This tab displays with assets and monitors.

The **State change log** tab displays whenever an asset node or monitor node is selected. This tab lists the status changes for each monitor assigned to an asset.

Note: Searches are case sensitive.

Monitors Actions Knowledge Toplist Audit State change log				
View 50 < Prev Next > Search				
Time	Delta	Monitor	State	Message
2013-02-11 14:10:46	4d 5h 5m	SNMP Table	Alarm	No Such Name
2013-02-11 10:22:13		Windows service status - Print spool service	Ok	Monitor 'dev-ar-win0d - Windows service status - Print spool service' is now in ok status.
2013-02-08 15:32:07		Uptime of Connection (minutes)	Ok	Monitor 'dev-ar-win0d - Uptime of Device (minutes)' is now in ok status.
2013-02-08 10:58:36	0h 7m 9s	<Deleted monitor>	Ok	Monitor 'dev-ar-win0d - SNMP trap' is now in ok status.
2013-02-08 10:51:27		<Deleted monitor>	Ok	Monitor 'dev-ar-win0d - SNMP trap' is now in ok status.
2013-02-07 17:11:15	0h 47m 55s	Memory utilization	Ok	Monitor 'dev-ar-win0d - Memory utilization' is now in ok status.
2013-02-07 16:23:20		Memory utilization	Alarm	Test failed, Access denied. User may lack remote launch and remote activation permission.
2013-02-07 16:12:04	4h 27m 7s	Security events	Ok	Monitor 'dev-ar-win0d - Security events' is now in ok status.
2013-02-07 11:44:57	0h 2m 1s	Security events	Ok	Monitor 'dev-ar-win0d - Security events' is now in ok status.

Editing Assets

<selected asset> > Edit

The **Edit asset** page displays the following property tabs.

- **Basic properties tab** (page 49) - Gateways, groups, and assets display a **Basic properties** edit tab.
- **Advanced tab** (page 50) - Gateways, groups, assets, and monitors display an **Advanced** edit tab.
- **Authentication tab** (page 40) - This edit tab displays with groups, gateways, and assets.
- **NOC tab** (page 41) - This edit tab displays with gateways, groups, and assets.
- **Tag tab** (page 45) - This edit tab displays with gateways, groups, and assets.

Basic properties edit tab - assets

Gateways, groups, and assets display a **Basic properties edit tab**.

Basic properties

- **Name** - The name for the asset. This property is set in **Discovery** module.
- **Address** - The DNS name or IP address of the asset. This property is set when an asset is discovered using the **Discovery** the module.
- **Operating system** - Select the asset's system type. The **operating system** (page 109) determines the type of monitors that can be added to this asset. If you do not know what system type the asset is or the system type is unavailable, select the **Other/Unidentified** option. For Windows performance monitors to work properly, it is essential that the system type be specified correctly.
- **Asset type** - Classifies the type of hardware asset. For reference purposes only.
- **Description** - The description field can be used to describe the asset in greater detail. For example, the type of hardware or physical location.
- **Free text** - The free text field can be used to include other information about the asset and can also be included in alarm notifications.

Alert and recovery settings

- **Inherit notification group** - Sets the notification group for this node. For gateways, groups, and asset nodes you can override the default notification *user group* messages are sent to. Monitor nodes use the notification group specified by their parent asset node and cannot be overridden.
- **Inherit alarm messages** - Sets the **Alarm Messages** (page 65) format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** (page 56) of this node.

Advanced edit tab - assets

Gateways, groups, assets, and monitor display an **Advanced edit tab**.

Advanced

- **Active** - If checked the asset is considered active. Active assets test their monitors. This option is checked by default.
- **SSH2 connect. sharing** - If checked, enables persistent SSH2 connections for this asset. Normally only one connection is opened and then shared among all monitors using SSH2 with this asset. Disabling the SSH2 connection sharing results in more logons on the SSH server, but can be useful if you experience any problems with your connections.
- **Enable inspection** - Enables automated inspection on this asset. Normally **Network Monitor** performs a an asset inventory of all assets regularly, to discover hardware and attached assets.
- **Use WMI** - If an asset is a Windows system type, the following monitor types use WMI when the asset flag **Use WMI** is checked. If you experience issues with these monitor types, try unchecking this checkbox.
 - **WMI Query monitor** (page 141) - Always uses WMI.
 - **Active directory monitor** (page 110) - Always uses WMI.
 - **Bandwidth utilization monitor** (page 111)
 - **CPU utilization monitor** (page 114)
 - **Disk utilization monitor** (page 117)
 - **Event log monitor** (page 118)
 - **Memory utilization monitor** (page 125)
 - **Swap file utilization monitor** (page 135)

Note: See **Windows Management Instrumentation (WMI)** (page 178) for more information.

Map and location settings

- **Inherit map settings** - If checked, **map settings** (page 34) are inherited from the parent node and the other three map options remain hidden. Uncheck to specify your own map settings.
 - **Map setting** - Use google maps. This is the only option available at this time.
 - **Google map display** - Checking these options determines whether gateways, groups and assets are shown on the map.
 - **Geographic location** - Enter the *name of a location* or *GPS coordinates* using decimal notation, such as -33.469048, -70.642007.
- **Time zone** - Monitors display their real time charts in the asset's local time.
- **Inherit time zone** - If checked, inherits time zone settings from the parent node. Uncheck to specify you own time zone settings.

Asset dependency settings

- **Inherit dependency** - This setting determines the currently selected node's **dependency** (page 51) on one or more specified monitors. If checked, this node inherits it dependency from the parent node.

If blank, you can define a dependency based on a different set of monitors *within the same gateway branch of the monitor tree* or leave no monitors specified to ensure this node has no dependencies.

- **Select dependency monitor / Selected monitors** - Enter text to display the names of monitors in the **Select dependency monitor** list that match the text entered. Select one or more monitors in the list, then click the **Add** button to add the monitors to the **Selected monitors** list. You can also click the **Select** button to browse for target monitors. To remove a monitor, select it and click the **Remove** button.

Simple maintenance

These settings provide a quick method of specifying a maintenance period for a *single* asset.

Note: Use [Network Monitor > Schedules > Asset maintenance](#) (page 89) to specify maintenance schedules for *multiple* assets.

- **Start time / (end time)** - The range of time during the day when this asset down for maintenance.
- **Day of week** - The days of the week this asset is down for maintenance.
- **Maintenance mode** - Stop test during maintenance. This is the only asset available during a maintenance period.

Dependency Testing

Dependencies are configured using the **Advanced** (page 50) edit tab of an assets node.

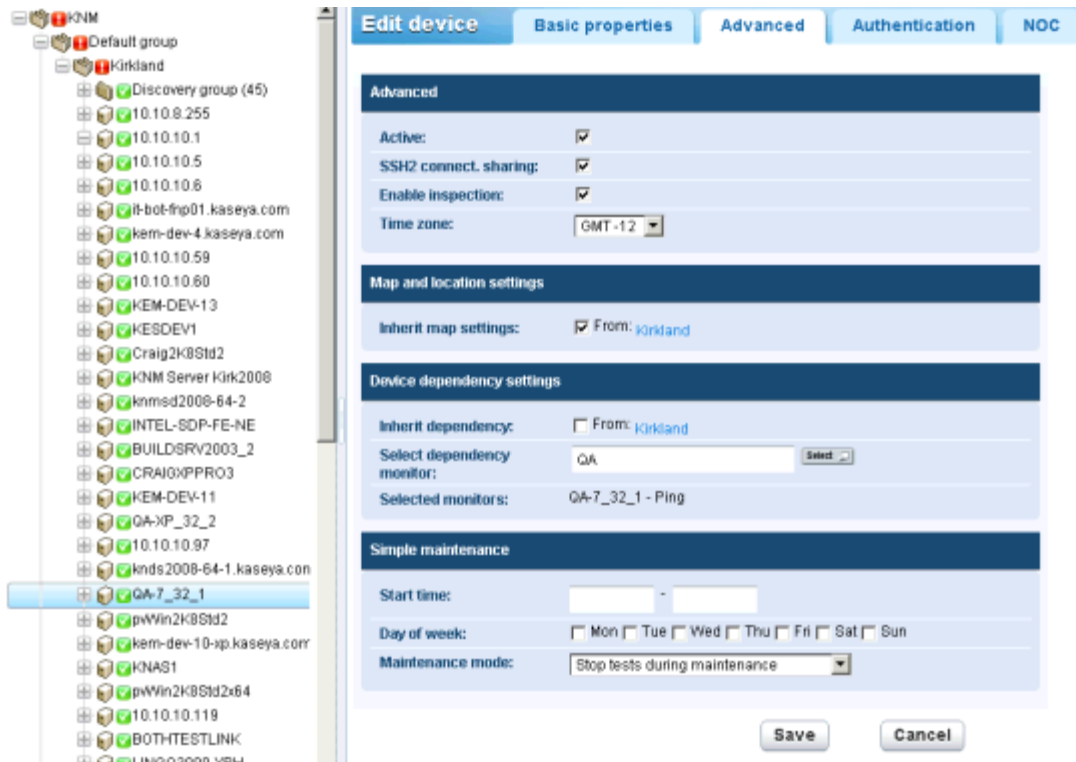
The alert status of one monitor can be made dependent on the alert status of *any node that is a member of the same gateway*.

Imagine monitoring a router for a single network. If the router goes down the monitor you've set up to test that router will correctly change, first to a *Failed* state, then to an *Alarm* state. Unfortunately all the other assets on that same network depend on that same router. When the router fails to connect, those dependent assets can't help but fail to connect as well. An entire branch of the monitor tree reports monitoring failures even though the problem is really a single asset. Those dependent assets are just a distraction at this point. Using dependency relationships you can prevent **Network Monitor** from triggering a cascade of unnecessary *Alarm* states when the *Alarm* state for a single critical monitor will serve the same purpose.

Another example is making all monitors on a single asset dependent on the **Ping check** monitor. If the network connection to the asset fails, then only one alarm will be created for the **Ping check**, but not for all the other monitors assigned to that asset.

Management Interface

Click **Edit** for any gateway, group or asset node, then click the **Advanced** tab. Use **Asset dependency settings** to select the monitor this node should be dependent on. All descendants of this node set to inherit will be dependent on the same monitor you select.



Asset Templates

Asset templates are configured using **Network Monitor > Settings > Asset templates**

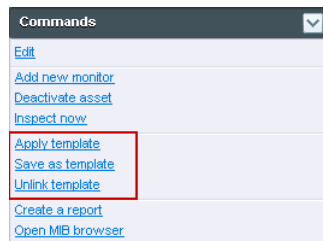
Configuring one monitor at a time for thousands of assets isn't practical. Instead configure a *set of monitors* using an **asset template** (page 101), then apply the asset template to the appropriate asset. You should have an asset template for each type of asset you manage.

System and Custom Asset Templates

Many asset templates are provided with **Network Monitor**. These can be applied but cannot be edited. You can also configure your own *custom* asset templates by configuring an asset with the monitors you need, then clicking the **Save as template** command.

Applying Asset Templates to Assets

Once you have configured an asset template, you only have to select an asset and click the **Apply template** option. Then select the asset template. All the monitors in the asset template will be assigned to the selected asset and begin returning data. If necessary, you can customize the settings of monitors assigned by asset template.



Reapplying Asset Templates

Assets remain *linked* to the asset template after the monitors are assigned. *Changes to an asset template are not automatically propagated to linked assets.* You have to re-apply the changed template to each asset again. When re-applying a changed template to assets, you have the option of over-riding asset-specific settings on selected assets, or leaving asset-specific settings unchanged.

Unlinking Asset Templates

You can unlink an asset from a template. When you unlink an asset template, the monitors remain assigned to the asset.

Monitors


A **monitor** tests a specific function in an asset. Most monitors are capable of collecting various statistical data for reporting purposes. When a monitor test fails consecutively a specified number of times, the monitor enters an *Alarm* state and executes a set of **actions** (page 56).

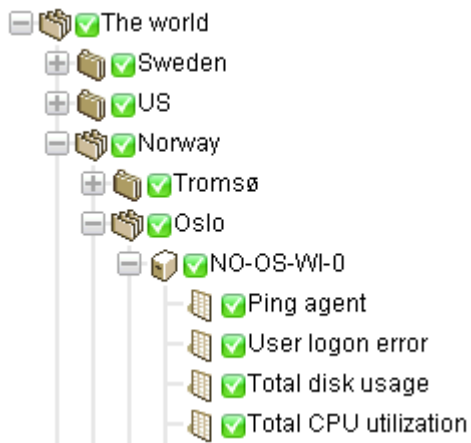
The alert status of each monitor—along with all other active monitors—is reported all the way up the monitor tree. If you are managing hundreds or thousands of monitors, this feature can quickly help you identify the individual monitor that is failing.

Alarm Status Progression



OK Status

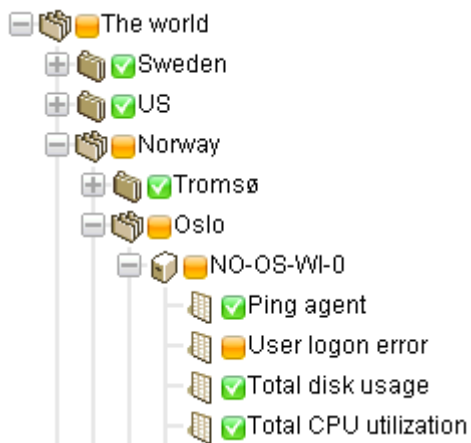
Management Interface

During normal operation, when a monitor is in the *OK* state, a green status  icon displays next to the monitor in the monitor tree. Here is what the monitor tree looks like when all monitors are in the *OK* state.





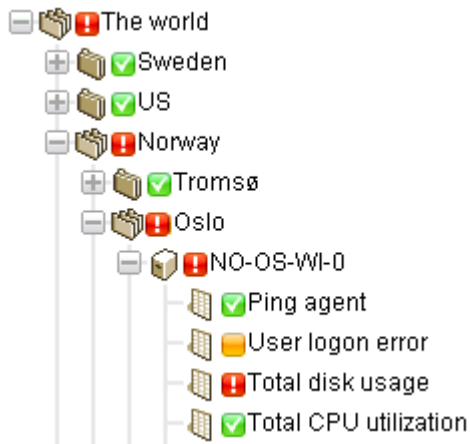
Failed Status

When a monitor fails its test, it changes to a *Failed* state, and an orange status  icon displays next to the monitor in the monitor tree. The *Failed* status has precedence over the *OK* state. In this case the  icon is reported all the way up the monitor tree.




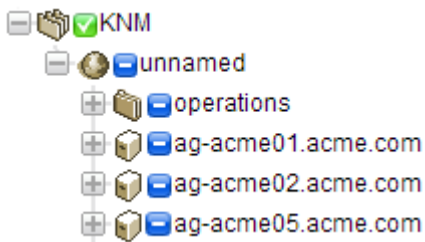
Alarm Status

When a monitor keeps failing tests, it eventually changes to an *Alarm* state, and a red status  icon displays next to the monitor in the monitor tree. The number of failed tests required to change a monitor to the *Alarm* state—known as the *alarm count*—is set to five for most monitors. This is the default and can be changed. Since the *Alarm* state has precedence over the *Failed* state and *OK* state, the  icon is reported all the way up the monitor tree.



Disconnected Status

A special  icon displays whenever a gateway is disconnected from the server. In this case the gateway and all lower level nodes are unable to report their data back to the server.



In This Section

Monitor Commands and Views	55
Adding Monitors	59
Adding Preconfigured Monitors	60
Editing Monitors	61
Alarm Messages	65
Format Variables	66
Acknowledging Alarms	68

Monitor Commands and Views

Commands

These commands display when a monitor node is selected, regardless of the view tab selected at the top.

- **Edit** - Edits the **properties** (page 49) of the asset.
- **Deactivate** - Deactivates the monitor.
- **Copy** - Copies the monitor to selected assets.
- **Delete** - Deletes the monitor.
- **Create a report** - Views, emails or publishes a **report** (page 69).

- **Test now** - Tests the monitor immediately.

Views

- **Summary tab** (page 48) - This tab displays with monitors.
- **Actions tab** (page 56) - This tab displays with gateways, groups, assets, and monitors.
- **Audit tab** (page 38) - This tab displays with gateways, groups, assets, and monitors.
- **State change log tab** (page 48) - This tab displays with assets and monitors.
- **Simulate alarm tab** (page 59) - This tab displays with monitors.

Summary tab

This tab displays with monitors.

The **Summary** tab of a active monitor displays the latest data returned. There are usually three sections to this view.

- **Monitor status** - Displays the latest value and the threshold to trigger a *Failed* state.
- **Live data** - A chart of the latest test values returned by the monitor. The time period the chart is set when you configure the monitor.
- **Monitor Log** - A log of every test value returned by the monitor.

Actions tab

This tab displays with gateways, groups, assets and monitors.

The **Actions** tab displays a set of actions. Actions are defined directly or by *inheritance*. Each action is executed in response to a specific *alarm count*. It is possible—and common—to define several actions for the same alarm count.

Note: Notice we're saying *alarm count* and not *Alarm state*. You can execute a series of actions using any *alarm count* you want. It doesn't have to match the count for the *Alarm state*.



Default Ticket Action

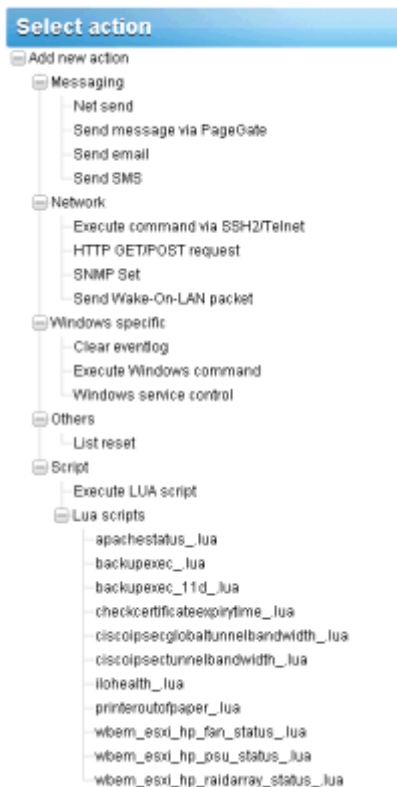
When **Network Monitor** is installed, the **Ticket** action is already added to the KNM root node. By default, the **Ticket** action is inherited by every other node in the monitor tree. This enables tickets to be created automatically in the **Ticketing** module or **Service Desk** module.

Recovery Actions

An administrator may have to intervene to correct an asset in an *Alarm* state, or the asset may enter an *Alarm* state temporarily and recover on its own. Either way, when a monitor recovers, **Network Monitor** can optionally execute a set pf *recovery actions*. **Recovery actions are executed when a monitor changes back to an OK state.** When the monitor recovers, all recovery actions displayed on the monitor's **Actions** tab are executed, regardless of the alarm number.

Adding Actions to the Actions tab

1. Click the **Add actions** button at the top of the **Actions** tab.
2. Select an action from the **Add new action** tree in the middle panel.
3. Select the **Add action** command in the right side panel.
4. Edit **Action properties** for the specific action selected. Here is the **list of actions** (*page 143*) you can select.



Managing Hierarchies of Actions and Recovery Actions

All nodes have an **Actions** tab. The **Actions** tab displays all **actions** and **recovery actions** that apply to the currently selected node. The **Inherited from** column identifies actions inherited from all higher level nodes. You can add additional actions and recovery actions to the currently selected node. All actions and recovery actions on this tab apply to any child nodes that are configured to inherit actions and recovery actions.

The screenshot shows the 'Actions' tab in the Management Interface. At the top, there are tabs for 'Summary', 'Actions', 'Audit', 'State change log', and 'Simulate alarm'. Below the tabs are buttons for 'Add action' and 'Delete'. The main area contains a table with columns 'Alarm number', 'Action', and 'Inherited from'. The table lists three actions: 'SNMP Set: 1.3.6.1.4.1.6876.2.4.1.2.3 on Device', 'Ticket', and 'Send SMS to user group (short message)'. Below the table are buttons for 'Add recovery action' and 'Delete'. At the bottom, there is a section for 'Action' and 'Inherited from' with a checkbox and a dropdown menu.

Alarm number	Action	Inherited from
1	SNMP Set: 1.3.6.1.4.1.6876.2.4.1.2.3 on Device	
1	Ticket	Operations
1	Send SMS to user group (short message)	Also View
1	Send email to user group	Kaseya North America

Disabling Inheritance of Actions and Recovery Actions

You can disable the inheritance of actions and recovery actions for the currently selected node. *Disabling inherited actions and recovery actions applies to any child nodes that are configured to inherit actions and recovery actions.* In edit mode—on either the **Basic properties** or **Advanced** tabs—an **Alert and recovery settings** section displays. Uncheck **Inherit actions** to remove all inherited actions and recovery actions from the currently selected node. After saving this change, re-display the **Actions** tab for the currently selected node. You'll notice inherited actions and inherited recovery actions no longer display.

The screenshot shows the 'Alert and recovery settings' section. It contains two rows: 'Inherit alarm messages:' and 'Inherit actions:'. Each row has a checkbox and a dropdown menu. The dropdown menus are set to 'From: dev-qv-wth03'.

Alert and recovery settings	
Inherit alarm messages:	<input checked="" type="checkbox"/> From: dev-qv-wth03
Inherit actions:	<input checked="" type="checkbox"/> From: dev-qv-wth03

Managing Customer-Specific Actions and Recovery Actions

You might find it easiest to manage and customize sets of actions and recovery actions at the "customer" level of the monitor tree. For example, you could create customer-specific alarm messages and alarm actions using the gateway node representing a single network. From then on these customer-specific settings could be *inherited* by every monitor below that gateway node in the monitor tree.

Actions on Gateways

Actions work slightly different for monitors assigned to a gateway. The following actions are always executed on the server:

- Send email
- Send SMS
- Paging via Pagegate

All other actions are executed on the gateway.

Simulate alarm tab

This tab displays with monitors.

The **Simulate alarm** tab generates a report that describes what happens when a particular monitor enters the *Alarm* state. To better understand how alarm escalation works in **Network Monitor**, the report contains verbose information about the progress of the escalation. Time specified in the report is relative to the first alarm generated.

Below is a sample report produced by the **Simulate alarm** function for a **Free disk space** monitor with default actions assigned.

Summary Actions Audit State change log Simulate alarm	
Monitor	SQL Server
Monitor type	SQL Server
Device	dev-av-win0d
Test procedure	Tests every 60 seconds. Alarm generated after 5 consecutive failed tests. In alarm state the monitor will test every 600 seconds.
Alarm number 1 (Executed 5 minutes after first failed test)	
Action type	Send email to user group
Subject	KNM - Alarm - dev-av-win0d - SQL Server
===== Time: 2012/12/21 13:20:16 Device: dev-av-win0d (10.10.32.6) Monitor: SQL Server ===== Status: Alarm Operational Body %[system.charts] ===== Distribution list: kadmin (noreply@kaseya.com)	
Extra recipients	
End of report	

Note: The **Simulate alarm** feature does not work correctly if the system administrator has disabled all actions.

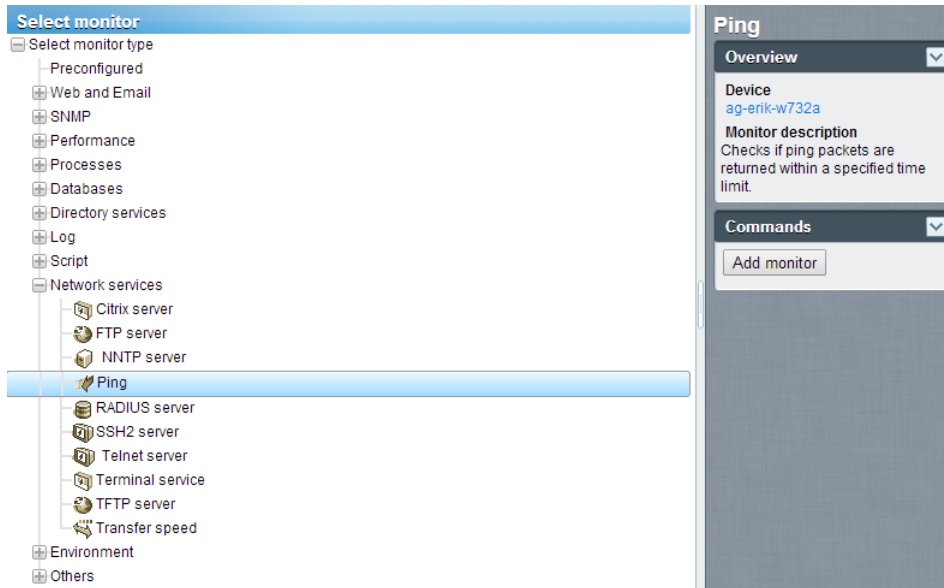
Adding Monitors

<selected asset > > **Add new monitor**

To add a monitor to an asset:

1. Select any asset node in the monitor tree.
2. Select the **Add new monitor** command.

- A list of list of **monitor types** (page 109)—more than 40 and growing—displays. See **Monitor Reference** (page 109) to identify which operating systems support which monitors.



3. Select a category and monitor type.
4. Select the **Add monitor** command.
5. Configure the monitor by **editing the monitor's property tabs** (page 61).

Note: Adding preconfigured monitors (page 60) is even faster!

Adding Preconfigured Monitors

Network Monitor can determine the appropriate *preconfigured monitors* for an asset. Typically you add preconfigured monitors just after a new asset is discovered. It's also recommended if the credentials or configuration of the asset has changed.

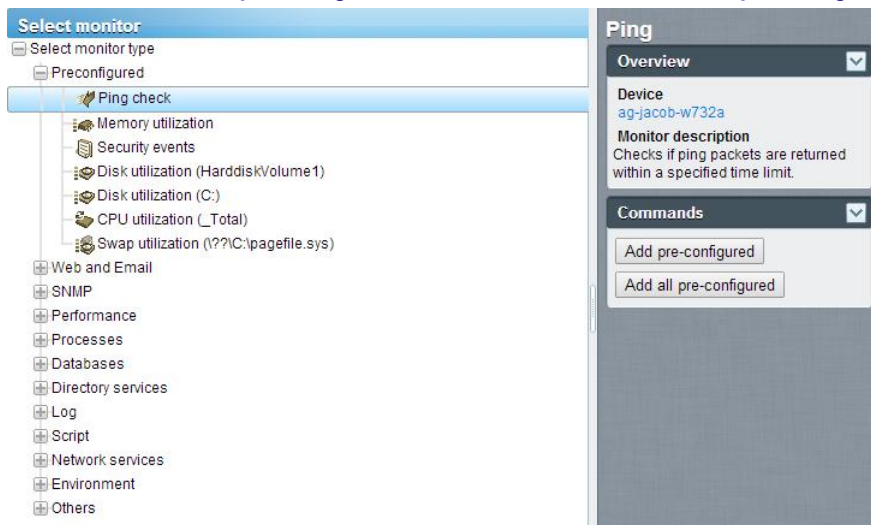
To add preconfigured monitors to an asset:

1. Click the **Inspect now** command for the asset. Wait for inspection to finish.

Note: You can also run *Inspect now for multiple assets at the same time*, using the **More > Inspect now** option on the **Assets** tab (page 33).

2. Click **Add New Monitor** to see a list of preconfigured monitor types.
3. Click any of the **Preconfigured** monitor types in the list.

4. Click either the **Add pre-configured** command or click the **Add all pre-configured** command.



Editing Monitors

<selected monitor> > Edit

The **Edit monitor** tab sets the properties for monitors assigned to assets.

- **Basic tab** (page 63) - This edit tab displays with monitors.
- **Advanced tab** (page 63) - Gateways, groups, assets, and monitors display an **Advanced** edit tab.
- **Alarm filtering tab** (page 64) - This edit tab displays with monitors.
- **Statistics tab** (page 64) - This edit tab displays with monitors.

Example

Let's take a look at the properties you can set if you select the **Performance > Memory utilization** monitor.

*Note: The following **standard monitor settings** display on most monitors. See the **Monitor Reference** (page 109) for **monitor-specific settings**.*

Edit monitor Basic Advanced Alarm filtering Statistics

Basic monitor settings

Device: QA-7_32_1 (Generic Windows)
 Type: Memory utilization
 Name: Memory utilization
 Test interval: 60

Threshold settings

Free memory: 50
 Unit: MB
 Process report: ☐

Windows domain credentials

Inherit credentials: ☒ From: QA-7_32_1 (Administrator)

Minimum free main memory in the specified unit.

Save Cancel

- The **Test interval** value in the **Basic Properties** section shows how much time must elapse between tests *before the first alarm is generated*.
- The **Threshold setting** section specifies the minimum **Free memory** required by this monitor, as described by the tooltip.

Edit monitor Basic Advanced Alarm filtering Statistics

Alert settings

Alarm generation: 5
 Alarm test interval: 600
 Active: ☒

Statistics and chart settings

Store statistics: ☒
 Chart resolution: 24 hours
 Group channels: Group 4 channels
 Chart layout: 1



Simple maintenance

Start time: -
 Day of week: ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun
 Maintenance mode: Stop tests during maintenance

Alert and recovery settings

Inherit alarm messages: ☒ From: QA-7_32_1
 Inherit alarm actions: ☒ From: QA-7_32_1

Save Cancel

- The **Alarm generation** value specifies the minimum number of *consecutive* "tests" that must fail to generate an alarm.
- The **Alarm test interval** value shows how much time must elapse between tests *after the first alarm is generated*. This interval is usually much longer than the **Test interval**, to give you time to respond to the original alarm.
- After the first alarm count, each additional, consecutive test that fails will increase the alarm count by one.
- As described in **Alarm Status Progression** (page 53):
 - The first time a monitor fails a test it begins displaying a warning  icon next to the monitor in the monitor tree.
 - When the number of failed tests—the *alarm count*—matches the number in the **Alarm generation** field, the monitor enters an *Alarm* state. An alarm  icon starts displaying next to the monitor in the monitor tree.
 - The monitor will remain in its alarm state until any *one* of the following occurs:
 - ✓ The test no longer fails, at least once, in a continuing series of consecutive tests.
 - ✓ The alarm is acknowledged by a user. An acknowledged alarm means a user knows about it and is acting to correct it.
 - ✓ The monitor is edited.

Basic edit tab - monitors

This edit tab displays with monitors.

Note: The following *standard monitor settings* display on most monitors. See the **Monitor reference** (page 109) for *monitor-specific settings*.

Basic tab

- **Asset** - The name of the asset.
- **Type** - The type of monitor. The identified **operating system** (page 109) determines the type of monitors that can be added to an asset.
- **Name** - The unique name of the monitor. Defaults from the monitor type name.
- **Test interval** - The interval to wait if the last test was *OK*. Typically the interval is longer if the last test *Failed*, as specified using the **Alarm test interval** on the **Advanced** tab.

Advanced edit tab - monitors

Groups, gateways, assets, and monitors display an **Advanced edit tab**.

Note: The following *standard monitor settings* display on most monitors. See the **Monitor reference** (page 109) for *monitor-specific settings*.

Alert settings

- **Alarm generation** - Specifies the minimum number of *consecutive* "tests" that must fail to generate an alarm.
- **Alarm test interval** - Specifies how much time must elapse between tests *after the first Failed alarm is generated*. This interval is usually much longer than the **Test interval** on the **Basics** tab, to give you time to respond to the original alarm. After the first alarm count, each additional, consecutive test that fails increases the alarm count by one.
- **Active** - If checked, this monitor is active. A monitor that is not active does not perform any tests. This option is checked by default.

Statistics and chart settings

- **Store statistics** - If checked, data collected is stored to disk.
- **Chart resolution** - The duration displayed by the chart.
- **Group channels** - The number of channels of data allowed on a single chart if a monitor returns multiple channels of data. This is mainly useful for monitors such as the Environment monitor that store separate statistics data for different external sensors.

Simple maintenance

These settings provide a quick method of specifying a maintenance period for a *single* monitor.

Note: Use **Network Monitor > Schedules > Monitor maintenance** (page 90) to specify maintenance schedules for *multiple* monitors.

- **Start time / (end time)** - The range of time during the day when this monitor is down for maintenance.
- **Day of week** - The days of the week this monitor is down for maintenance.
- **Maintenance mode** - Stop test during maintenance. This is the only mode available during a maintenance period.

Alert and recovery settings

- **Inherit alarm messages** - Sets the **Alarm Messages** (page 65) format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** (page 56) of this node.

Alarm filtering edit tab - monitors

This edit tab displays with monitors.

Note: The following *standard monitor settings* display on most monitors. See the **Monitor reference** (page 109) for *monitor-specific settings*.

This tab enables you to filter out categories of alarms for a monitor. For example, if a monitor is causing false alerts due to an unstable network connection, uncheck **Network errors** to ignore these types of errors. By default, all types of errors are alerted on.

- **Network errors** - Alerts on network connection error conditions.
- **Threshold errors** - Alerts on monitor threshold error conditions.
- **Other errors** - Alerts on unclassified error error conditions.

Statistics edit tab - monitors

This edit tab displays with monitors.

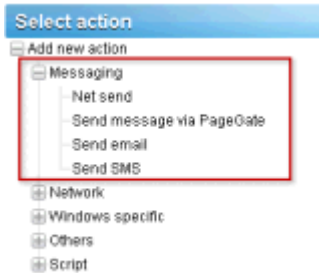
Note: The following *standard monitor settings* display on most monitors. See the **Monitor reference** (page 109) for *monitor-specific settings*.

This tab contains display settings for each type of statistical data recorded by the monitor. If checked, the specified data is shown in the real time charts on the monitor information view.

Alarm Messages

Alarm messages can be specified for gateways, groups, assets, and monitors.

Several of the actions you can execute when an alarm fails a consecutive number of tests is the sending of messages.



The default format used by all message types is specified by the *root node* at the top of the monitor tree, named the KNM node by default. All other descendant nodes *inherit* this message format unless you choose to override it. There is a separate format for action messages and for recovery action messages. See the list of [Format Variables](#) (page 66) available to use.

Edit group Basic properties Advanced Authentication NOC Access

Basic properties

Name:

Description:

Alert and recovery settings

Notification group:

Alarm subject:

Alarm message:

Recover subject:

Recover message:

Management Interface

To override the inherited default format, click either the **Basic properties** or **Advanced** tab, depending on the type of node you've selected. Then uncheck the **Inherit alarm messages** checkbox.

The screenshot shows the 'Edit device' interface with the 'Basic properties' tab selected. Below the 'Basic properties' section is the 'Alert and recovery settings' section. In this section, the 'Inherit alarm messages' checkbox is highlighted with a red box. The checkbox is currently unchecked. Other settings include 'Inherit notification group' (checked, From: Stockholm), 'Alarm message' (text area), 'Alarm subject' (text field), 'Recover message' (text area), 'Recover subject' (text field), and 'Inherit alarm actions' (checked, From: Stockholm). At the bottom are 'Save' and 'Cancel' buttons.

Format Variables

All outgoing messages in **Network Monitor** can include formatting variables in the text of the message. The format variables are resolved before the messages are processed and sent to recipients. Most of these format variables are context sensitive. For example, the format variable `%[monitor.error]` only resolves when an alarm is triggered by a monitor action. This same format variable will not resolve into anything if used in a **Send mail** scheduled event.

<code>%[system.time]</code>	current time
<code>%[system.time_hour]</code>	24 hours formatting
<code>%[system.time_hour2]</code>	12 hours formatting
<code>%[system.time_minute]</code>	including minutes
<code>%[system.time_second]</code>	including seconds
<code>%[system.date]</code>	current date
<code>%[system.date_year]</code>	current date with full year
<code>%[system.date_year2]</code>	year without century
<code>%[system.date_month]</code>	month as number 01 - 12
<code>%[system.date_day_of_month]</code>	day of the month 01 - 31
<code>%[system.date_weekday]</code>	0 - sunday, 6 = saturday

%[system.date_day_of_year]	day of the year 1 - 366
%[group.name]	name of group
%[group.path]	full path of group
%[group.id]	group unique id
%[group.url]	link to group
%[group.kb_article_url]	link to articles for the current group
%[group.company]	group/company name
%[group.additional]	group/company additional line 1
%[group.additional]	group/company additional line 2
%[group.contact]	group/company contact name
%[group.email]	group/company email
%[group.phone]	group/company phone
%[group.cellphone]	group/company cell phone
%[group.fax]	group/company fax
%[group.address1]	group/company address1
%[group.address2]	group/company address 2
%[asset.local_time]	asset local time
%[asset.name]	name
%[asset.id]	unique id of asset
%[asset.free_text]	
%[asset.address]	
%[asset.ip]	
%[asset.description]	
%[asset.notification_group]	
%[asset.mac]	
%[asset.url]	link to asset
%[asset.kb_article_url]	link to articles for the current asset
%[monitor.name]	
%[monitor.id]	
%[monitor.error]	
%[monitor.error2]	
%[monitor.type]	
%[monitor.current_status]	
%[monitor.time_last_ok]	
%[monitor.time_last_ok_local_time]	
%[monitor.time_last_failed]	
%[monitor.time_last_failed_local_time]	
%[monitor.dependency_status]	
%[monitor.url]	
%[user.current]	name of the user, used in acknowledge alarm
%[user.on_duty]	name of "on duty" user as defined by a user work schedule

Management Interface

%[user.distribution_list]	list of users who get the e-mail
%[report.name]	
%[report.description]	
%[monitor.list]	used in acknowledge alarm, monitors that were acknowledged

Acknowledging Alarms

Acknowledge an alarm by selecting the [Acknowledge](#) button at the top of any **Monitors** view tab on a gateway, group, or asset node.

A user can acknowledge the alarm state of one or more monitors to notify other users that the alarms are being investigated. When acknowledging an alarm, the user has two choices:

- **Clear alarm status** - This clears the alarm state and returns the monitor to its *Ok* state.
- **Deactivate the monitors** - This deactivates the monitors, with a checkbox to automatically [reactivate the monitors after N minutes](#). If the reactivate checkbox is unchecked, the monitors stays deactivated until being manually activated.

Acknowledge alarm

Acknowledge alarm for the following monitors:

Device	Monitor
QA:XP_32_2	CPU utilization

Modify the selected monitors:

Deactivate the monitors

☒ and reactivate the monitors after: 30 minutes

User notification

You can send a message to all users responsible for the selected monitors:

```
=====
Time: %[system.time]
User %[user.current] has acknowledged alarm for the following monitors:
=====
%[monitor.list]
```

Send the message by: ☒ Email: ☐ SMS: ☐ PageGate:

Acknowledge alarm Cancel

Acknowledge Notification Format

The format of the acknowledge notification message is *not inherited down the monitor tree*. Instead, the default notification format is specified using the Network Monitor Settings > SMS > **Default messages** (page 107) tab and applies to all nodes.

Note: The **Format Variables** (page 66) topic lists the format variables you can include in an acknowledgment notification message.

Reports

Network Monitor is capable of generating statistical reports from recorded monitor data. All reports are constructed using a common set of design elements such as charts, toplist, downtime information, data tables, comments and images. The overall style and color settings of the reports are controlled by style templates, which makes it easy to add your company color-scheme or logotype to the finished reports.

This section introduces how to view and publish different types of reports.

Viewing Report Templates

<Select a node> > Create a report > View in Browser

The **View report** page enables you to view two types of report.

- **Report templates**
- **Quick reports**

Typically you select groups, assets or monitors *first*, then select the type of report to view.

1. Select any node in the monitor tree, typically a gateway or group. Depending on the type of node, either assets or monitors are listed in the middle pane.
2. Click the **View Report** button or select the **Create a Report > View in Browser** command to display the **View report** page.

Report settings

The **Report settings** tab on the **View report** page displays three initial options:

- **Period** - Selects the period of the report.
 - Current day, week, month, quarter, year
 - Last day, week, month, quarter, year
 - User defined period
 - Offset in days
- **Run a report template** - Select from a list of predefined reports templates. **Network Monitor** comes pre-configured with a set of useful **Report templates**. You can customize these or create your own. The type of data and design elements are already selected in a report template, so the only choice you have to make is which report template to run.
- **Configure a quick report** - We recommend you select specific monitors before selecting this option. If you do, the **quick report** (page 70) includes a set of compatible design elements by default for the monitors you have selected. If no monitors are selected before selecting this option, you must add each design element manually.

Selection

Use the **Selection** tab on the **View report** page to override the default selection of gateway or group,

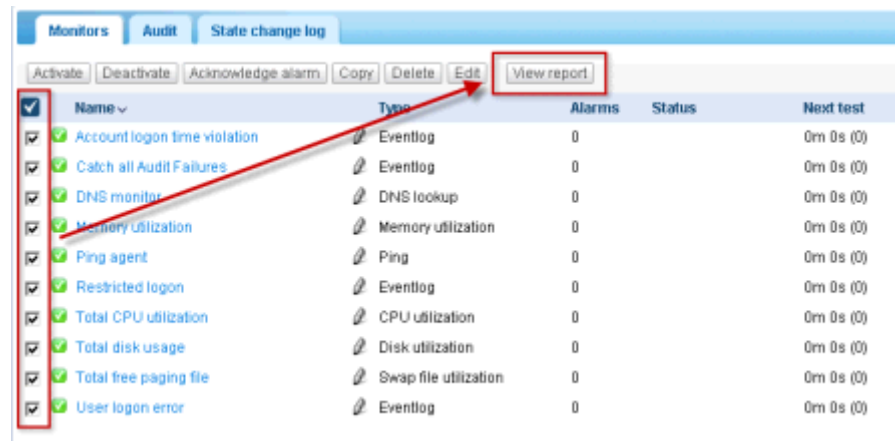
assets and monitors selected for either type of report.

Viewing Quick Reports

<Select a node> > <select monitors> > View report

Once assets are assigned different types of monitors, run a **Quick report** to *compare data from different types of monitors*. When multiple assets are selected, data for the same monitor type is grouped together on the same graph.

The fastest way to configure a quick report is from the list view of a **Monitors** tab of a single asset. Select all the monitors for that asset on the **Monitors** tab. Click the **View report** button at the top of the monitor list.



Click the **Configure a quick report** option. The **Report settings** tab lists a series of configuration sections, one or more for each type of monitor you selected earlier.

The screenshot shows the 'Report settings' tab with three sub-tabs: 'View report', 'Report settings', and 'Selection'. The 'Report settings' sub-tab is active. Under 'Report settings', there is a 'Period:' dropdown set to 'Current day' and a 'Please select:' section with two radio buttons: 'Run a report template' and 'Configure a quick report'. The 'Configure a quick report' option is highlighted with a red rectangle. Below this is the 'Configure a quick report' section, which contains a 'Please select:' dropdown set to 'Databases' and an 'Add' button. Below this are several configuration sections for different metrics, each with a red 'X' icon to its right:

- CPU utilization:** Unit: Percent, Chart: Display averages, Group 4 monitor(s), Datatable: No datatable, Interval average.
- Disk utilization:** Unit: Percent, Chart: Display averages, Group 4 monitor(s), Datatable: No datatable, Interval average.
- Ping roundtrip time:** Unit: Milliseconds, Chart: Display averages, Group 4 monitor(s), Datatable: No datatable, Interval average.
- Ping packetloss:** Unit: Percent, Chart: Display averages, Group 4 monitor(s), Datatable: No datatable, Interval average.
- Memory utilization:** Unit: Percent, Chart: Display averages, Group 4 monitor(s), Datatable: No datatable, Interval average.
- Swap utilization:** Unit: Percent, Chart: Display averages, Group 4 monitor(s), Datatable: No datatable, Interval average.

At the bottom of the form are two buttons: 'View report' and 'Cancel'.

Click the **View report** button at the bottom of the page. Monitor data displays in chart format for each of the sections configured on the **Report settings** tab.

Note: To display the report in a new tab or window, set the Network Monitor > User > My settings > Interface options tab > View reports drop-down list to Open reports in a new window.

Using this same page you can:

- Add new sections using the **Add** button at the top the **Report settings** tab.
- Select a different time **Period**.
- Use the **Selection** tab to select multiple groups, assets and monitors.

Note: You can also select the **Run a report template** option to run a report with a pre-defined layout for the assets you selected.

Viewing Customized Reports

Customized reports are good for defining reports whose content does not change. A customized report is also the only way to create a report that contains data for different time periods in the same report.

Customize reports are designed just like report templates, *but are bound to specific groups, assets and monitors*. For that reason customized reports are not run by first selecting a node in the monitor tree. *Instead you both create and run customized reports by selecting Network Monitor > Reports >*

Customized reports (page 77).

Note: Since the design and running of customized reports are so similar to report templates, you should familiarize yourself with configuring **report templates** (page 78) first. Customized reports simply provide additional fields that require you to specify groups, assets and monitors.

Emailing and publishing reports

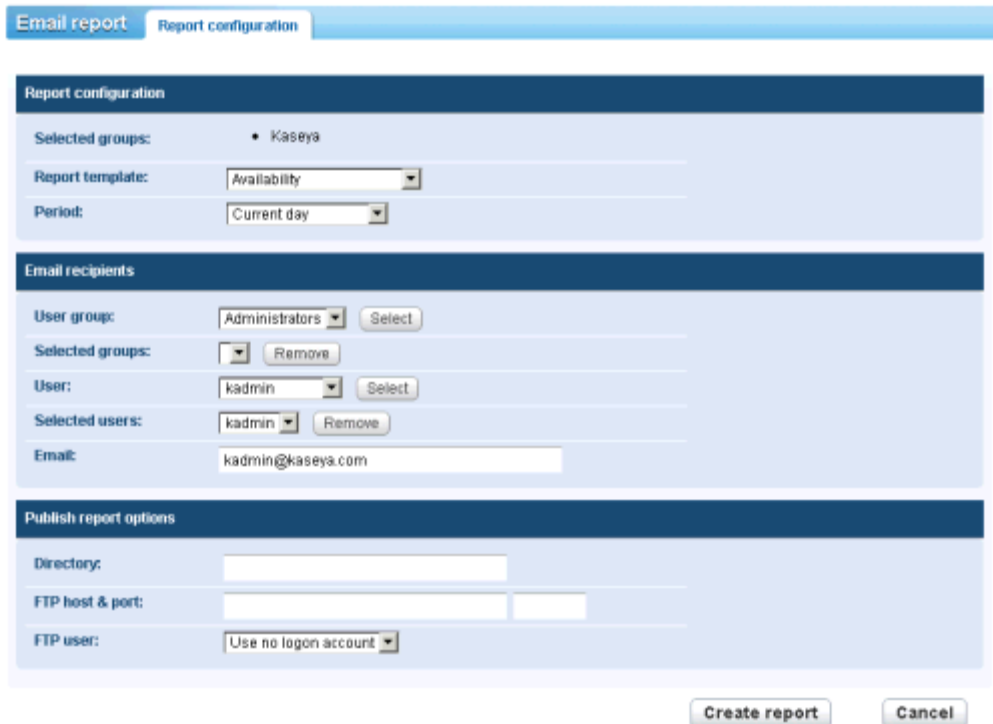
<Select a node> > Create a report > Email or publish

Network Monitor > Reports > Customize reports > (click the )

The **Email report** page distributes a selected report template or customized report as an attachment to an email, or populates a file location. You do not preview the report before generating it.

Select groups, assets or monitors *first*.

1. Select any node in the monitor tree, typically a group. Depending on the type of node, either assets or monitors are listed in the middle pane.
2. Click the **View Report** button or select the Create a Report > **Email or publish** command to display the **Email report** page.



Email report | Report configuration

Report configuration

Selected groups: • Kaseya

Report template: Availability

Period: Current day

Email recipients

User group: Administrators

Selected groups:

User: kadmin

Selected users: kadmin

Email: kadmin@kaseya.com

Publish report options

Directory:

FTP host & port:

FTP user: Use no logon account

Report configuration

- **Selected groups** - Displays the selected group node.

- **Report template** - Select a report template.
- **Period** - Selects the period of the report.
 - Current day, week, month, quarter, year
 - Last day, week, month, quarter, year
 - User defined period
 - Offset in days

Email recipients

- **Select assets / Selected assets** - Enter text matching any part of the name of the asset. Select one or more assets from the **Select assets** list and click the **Add** button. To remove one or more user groups from **Selected groups**, select a user group and click the **Remove** button.
- **User / Selected users** - Select one or more VSA users from the **Users** list and click the **Select** button. To remove one or more users from the **Selected users** list, select users and click the **Remove** button.
- **Email** - Specify individual email addresses as recipients. Separate multiple entries with a comma.

Publish report options

Instead of emailing a report, you can save it to a network location.

- **Directory** - The generated report is published on a network folder as an HTML document. Specify the path to this folder. Optionally include the following formatting variables when specifying the filename.
 - `%[system.date]` - the current full date
 - `%[system.date_year]` - current year
 - `%[system.date_month]` - current month
 - `%[system.date_day_of_month]` - current day in the month
 - `%[system.time]` - current full time
 - `%[system.time_hour]` - current hour
 - `%[system.time_minute]` - current minute
 - `%[system.time_second]` - current second
- **FTP host & port** - The generated report can be published on a FTP server as a HTML document. Specify the host name and port number. Defaults to 21.
- **FTP user** - Select the logon account to be used for authenticating against the FTP server here.

Scheduling reports

Scheduling the automatic generation of reports is done with the scheduled events feature. Details on how to work with scheduled events can be found in the **Scheduled events** (page 36) section.

Documentation for the **Generate report** (page 153) event specifically can be found in the **Scheduled event reference** section.

Chapter 3

Navigation Panel Reference

The navigation pane for **Network Monitor** provides module settings and functions that are independent of any one node in the monitor tree.

In This Chapter

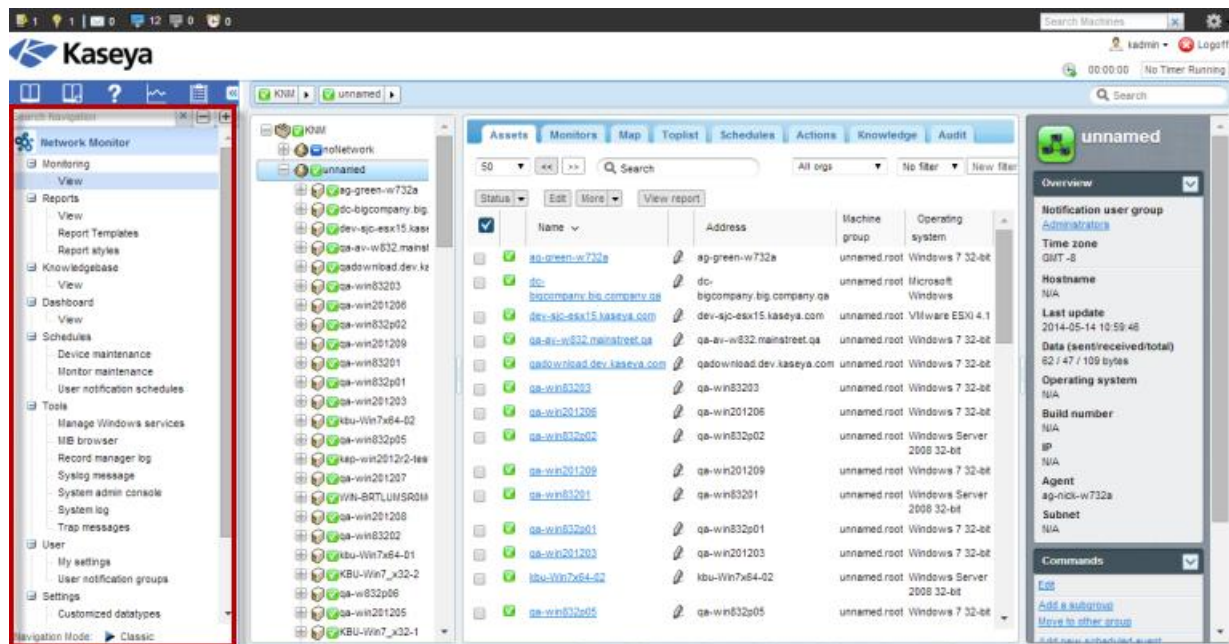
Navigation Panel Overview	75
Customized reports	77
Report templates	78
Knowledge Base Articles	86
Dashboard	88
Asset maintenance	89
Monitor maintenance	90
User notification schedules	91
Windows service list	92
MIB Browser	93
Record manager log	96
Syslog message	97
System administrator console	97
System log	99
Trap messages	99
My settings	99
User notification groups	100
Customized data types	101
Asset templates	101
Log settings	102
NOC settings	103
Other system settings	104
SMS settings	104
Default messages	107

Navigation Panel Overview

The **Network Monitor** navigation panel provides different views of content and enables you to configure module-level settings.

Navigation Panel Reference

Note: The navigation panel takes the place of the "K menu" in earlier, standalone releases of **Network Monitor**.



These functions are detailed in the [Navigation Panel Reference](#) (page 75) included with this documentation. The following is a summary description of each option in the navigation panel.

Functions	Description
Monitoring > View (page 16)	Selects the monitoring view (page 16).
Reports > View (page 77)	Configures customized reports that are bound to selected sets of nodes.
Report Templates (page 78)	Configures report templates that can be applied to any set of nodes.
Report styles (page 79)	Configures the overall look of reports, report templates and customized reports.
Knowledgebase > View (page 86)	Selects the Knowledge base view.
Dashboard > View (page 88)	Selects the Dashboard view.
Asset maintenance (page 89)	Configures asset maintenance schedules.
Monitor maintenance (page 90)	Configures monitor maintenance schedules.
User notification schedules (page 91)	Configures Network Monitor user work schedules.
Management Windows services (page 92)	Selects the Management Windows services view.
MIB browser (page 93)	Selects the MIB browser view.
Record manager log (page 96)	Selects the Record manager log.
Syslog message (page 97)	Selects the Syslog messages view.
System admin console (page 97)	Selects the System admin console view.
System log (page 99)	Displays log entries created by the Kaseya Network Monitor service.
Trap messages (page 99)	Selects the SNMP Trap messages view.
My settings (page 99)	Selects the Edit my settings view.

User notification groups (page 100)	Maintains user groups. Asset notifications are sent to all members of the notification user group assigned to that asset.
Customized datatypes (page 101)	Creates customized data types for use with monitors capable of storing generic data.
Asset templates (page 101)	Configures sets of monitors that can be applied to an asset in one step.
Log settings (page 102)	Sets log policies for Network Monitor.
NOC configuration (page 103)	Creates customized NOC (Network Operations Center) views.
Other system settings (page 104)	Specifies additional settings for alerts and other events.
SMS (page 104)	Sets SMS message settings.

Customized reports




Network Monitor > Reports > View

The **Customized reports** page maintains all customized reports. **Customized reports** are good for defining reports whose content does not change. A customized report is also the only way to create a report that contains data for different time periods in the same report. Customized reports are designed just like report templates, *but are bound to specific groups, assets and monitors*. For that reason customized reports are not run by first selecting a node in the monitor tree. *Instead you both create and run customized reports by selecting Network Monitor > Reports > View.*

The following subtopics describe both **report templates** (page 78) and customized reports. Certain fields apply to customized reports only and are identified in each topic.

- **Report properties** (page 78)
- **Style templates** (page 79)
- **Report info** (page 79)
- **Report data types** (page 80)
- **Graphs** (page 81)
- **Data tables** (page 82)
- **Downtime report** (page 83)
- **Comments** (page 84)
- **Images** (page 84)
- **Toplists** (page 84)

Actions

- **Delete** - Deletes the selected report.
- **New customized report (or  to edit)** - Edits the **properties** (page 78) of the report.
- **(Edit details)** - Click the **underlined name of the report** (page 79) to add or edit the list of design elements in the report.
- **(View report)** -  - Displays the selected customized report in a browser.
- **(Email or publish)** -  - **Distributes the report** (page 72) as an email attachment or saves the report to a network location.

Report templates

Network Monitor > Reports > Report Templates




The **Report templates** page maintains all report templates. A report template has a predefined layout, a set of data objects and design elements. Report templates are global and can be applied anywhere. You can select any node in the monitor tree and click the **Create a report > View in browser** command to generate a report from a selected report template. By default the report includes all assets and monitors included in the selected node. You can also run them from the **Report templates** page itself.

Many predefined report templates are included with **Network Monitor**. You can customize these or create your own.

The following subtopics describe both report templates and **customized reports** (page 77). Certain fields apply to customized reports only and are identified in each topic.

- **Report properties** (page 78)
- **Style templates** (page 79)
- **Report info** (page 79)
- **Report data types** (page 80)
- **Graphs** (page 81)
- **Data tables** (page 82)
- **Downtime report** (page 83)
- **Comments** (page 84)
- **Images** (page 84)
- **Toplists** (page 84)

Actions

- **Delete** - Deletes the selected report.
- **New report template (or  to edit)** - Edits the **properties** (page 78) of the report.
- **(Configure report)** - Click the **underlined name of the report** (page 79) to configure the design elements in the report.
- **(View report) ** - **Displays the selected report template in a browser** (page 69).
- **(Email or publish) ** - **Distributes the report** (page 72) as an email attachment or saves the report to a network location.

Report properties

Network Monitor > Reports > Report Templates > (click the  icon of a report template)
 Network Monitor Reports > View > (click the  icon of a customized report)

The **Report properties** page specifies basic properties of the report template or customized report.


- **Name** - Enter a name for the report. The name identifies the report in list views.
- **Description** - A longer description of the report and its function.
- **Report category** - Select the category of the report. Reports are grouped by category throughout the user interface.
- **Style** - Select the **style template** (page 79) of the report.
- **Favourite** - If checked, the item is marked as a favourite for the current user. The current user's favourite items can be displayed on a dashboard using the favourites widget.
- **Visibility** - *Applies to Customized reports only.*
 - **Private** - If selected, only the current user can see the customized report in list views.
 - **System administrators** - If selected, you and any system administrator can see the customized report in list views.

Report styles

Network Monitor > Reports > Report styles

Style templates control the overall look of the report. A style template is made up of a number of different elements that are common for all reports using the same style template. Both **Report templates** (page 78) and **Customized reports** (page 77) can use a style template.

Actions

- **Delete** - Deletes the selected style template.
- **New style template (or  to edit)** - Adds or edits a style template. The **Color settings** tab only displays in edit mode.

Basic properties

- **Name** - This is the name of the template. The name is used to identify the template in lists.
- **Description** - A longer description of the style template.
- **Header** - The header is displayed on top of every generated report. The following parameter can be included in the header.
 - `%[system.time]` - the current time
- **Footer** - The footer displayed in the bottom of every generated report. The following parameter can be included in the footer.
 - `%[system.time]` - the current time
- **Logotype** - It is possible to include an image, such as a logotype, in every generated report using this template. Logotype images should be placed in the `KNM\reports\images\logo` folder of the KNM host machine.
- **Logotype placement** - Specify the placement of the logotype image.
- **Default** - Check this option to set this style template as the default for new reports.

Color settings

Specified all colors using hexadecimal `RRGGBB` color format.

- **Color scheme** - Select a pre-defined color scheme. To customize your own color scheme, select **Custom**.
- **Background 1 and 2** - Enter the color for backgrounds in graphs.
- **Grid color** - Enter the color for the grid in graphs.
- **Text color** - Enter the color for text and values in graphs.
- **Line color 1 to 8** - Enter the color for each specific monitor in graphs.


Report info

Network Monitor > Reports > Report Templates > (click name of report template)



Network Monitor > Reports > View > (click name of customized report)

The **Report info** page defines the details of the report template or customized report. This includes the layout, design elements, and **report data types** (page 80) used.

Commands

- **Edit** - (or click the  icon) - Edits the selected item.
- **Copy** - Copies a selected item.
- **Delete** - Deletes selected items.
- **Add availability** - Adds an **availability item** (page 83).

Navigation Panel Reference

- **Add comment** - Adds a **comment item** (page 84).
- **Add data table** - Adds a **data table item** (page 82).
- **Add graph** - Adds a **graph item** (page 81). Click the hyperlink of a graph item to specify the monitors included in the graph.
- **Add image** - Adds an **image item** (page 84).
- **Add toplist** - Adds a **toplist item** (page 84).
- ( or ) - Moves an item up or down in the list.

Report data types

The following types of types of data can be selected when defining a graph or data table in a report.

- Availability
 - Report downtime for assets
 - Report downtime for monitors
- Databases
 - Buffer cache hit ratio
 - SQL query value
- Environmental
 - Temperature
 - Humidity
 - Wetness
 - Voltage
 - Electric current
 - Fan speed
 - Luminosity
 - Relative airflow
 - Switch/dry contact
 - Electric power
- File System
 - Disk utilization
 - Free disk space
 - Directory size
 - Directory file count
 - Swap utilization
- Network
 - Bandwidth utilization
 - Bandwidth usage
 - Ping roundtrip time
 - Pink packetloss
 - Transfer speed
 - Unspecified SNMP data
 - Unspecified SSH script data
 - Connections
 - Requests
 - Requests / sec
 - Connections / sec
 - Users
- Others
 - Unspecified LUA data
 - Latency
- Performance

- CPU utilization
- Disk utilization
- Free disk space
- Memory utilization
- Free memory
- Swap utilization
- Unspecified Windows performance data
- Unspecified WMI data
- Unspecified VMware performance data
- Unspecified CIM performance data
- User Defined
 - (none)
- Web and email
 - Mail roundtrip time
 - Webpage fetch time

Graphs

Network Monitor > Reports > Report Templates > (click the name of a report template) > Add graph or click the  icon for a graph item

Network Monitor > Reports > View > (click the name of a customized report) > Add graph or click the  icon for a graph item

Graphs display a chart of recorded monitor data over a specific period. Each graph can contain data from up to 8 individual monitors. Every monitor is coded with a specific color. The color is specified in the relevant **Style template** (page 79).

Basic properties

- **Period** - Specifies the period for this item. *Applies to Customized reports only.*
 - Current day, week, month, quarter, year
 - Last day, week, month, quarter, year
 - User defined period
 - Offset in days

Note: Report templates specify the time period when the report template is run.

- **Data type** - Selects the **type of data** (page 80) and unit of measure to include in the report.
- **Header** - Specifies header text for the graph. Optionally include the following parameter in the header.
 - %graph_type - Displays the report data type in the graph.
- **Footer** - Specifies footer text for the graph.



Advanced properties

- **Data option** - average (default), min, max - Defines how data is presented when there are more recorded samples for a given position in time. Affects visual presentation only.
- **Separate monitors** - If checked, each monitor is graphed separately.
- **Fill** - If checked, the graph is filled. Ignore if more than one monitor is included in the graph.
- **Legend** - If checked, include a legend after the graph. This contains a reference to all monitors included in the graph, as well as their extreme values over the period.
- **Data filter** - Optionally specify a **min** and **max** range for visible data. Data outside the range is ignored.
- **Custom scale** - Optionally limit the graph to a certain range in the Y-axis. Normally, this is controlled automatically by the type of the data.

- **Graph dimension** - Specify the dimension of the graph image. The default value is 1000 x 152 pixels.

Customize report fields only

For **Customize reports**, click the *hyperlink* of a graph item to display a **Monitor list** page. specify the monitors included in the graph.

- **Add monitor** - Displays an **Add monitors to graph** page.
 - **Select monitor / Selected monitors** - Enter text to display the names of monitors in the **Select monitor** list that match the text entered. Select one or more monitors in the list, then click the **Add** button to add the monitors to the **Selected monitors** list. You can also click the **Select** button to browse for target monitors. To remove a monitor, select it and click the **Remove** button.
 - Only monitors storing data of the type specified in the graph can be selected.
- **Delete** - Deletes a selected monitor.
- ( or ) - Moves an item up or down in the list.

Data tables

Network Monitor > Reports > Report Templates > (click the name of a report template) > Add data table or click the  icon for a data table item

Network Monitor > Reports > View > (click the name of a customized report) > Add data table or click the  icon for a data table item

Data tables can display tabular data in both horizontal and vertical tables. This makes it possible to display readings in a textual format. The number of rows or columns depends on the report time period.

Data table properties

- **Header** - Header text describing the item in the report.
- **Select asset / Selected assets** - Enter text to display the names of assets in the **Select asset** list that match the text entered. Select one or more assets in the list, then click the **Add** button to add the assets to the **Selected assets** list. You can also click the **Select** button to browse for target assets. To remove an asset, select it and click the **Remove** button. *Applies to Customized reports only.*
- **Select monitor / Selected monitors** - Enter text to display the names of monitors in the **Select monitor** list that match the text entered. Select one or more monitors in the list, then click the **Add** button to add the monitors to the **Selected monitors** list. You can also click the **Select** button to browse for target monitors. To remove a monitor, select it and click the **Remove** button. *Applies to Customized reports only.*
- **Period** - Specifies the period for this item. *Applies to Customized reports only.*
 - Current day, week, month, quarter, year
 - Last day, week, month, quarter, year
 - User defined period
 - Offset in days

Note: Report templates specify the time period when the report template is run.


- **Resolution** - The frequency within the **Period** to collect data. *Applies to Customized reports only.*
- **Layout** - Select between a horizontal layout, where the time is presented as going from left to right, or a vertical layout where time is listed as going from up to down.

Data table configurations

A single data table in a report includes one or more data table configurations. After selecting a **Data type** and **Data table mode**, click the **Add** button to add the configuration to the list of configurations. To remove a configuration, select it from the list and click the **Remove** button.

- **Data type** - Selects the **type of data** (page 80) and unit of measure to include in the report.
- **Data table mode**
 - **Snapshot** - The closest data sample to the cell. For example, if you have a **Daily** report and there are two samples at **14:59** and **15:02**, the data shown for the cell at **15:00** is the sample at **14:59**.
 - **Interval average** - Averages all samples within each period and uses that value for the respective cell.
 - **Min** - Smallest data sample within each period.
 - **Max** - Largest data sample within each period.

Downtime report

Network Monitor > **Reports** > **Report Templates** > (click the name of a report template) > **Network Monitor** > **Reports** > **View** > (click the name of a customized report) > (click the  icon for an item)

Downtime report items—also call *availability*—can show the downtime of one or more selected assets or individual monitors. A downtime report can also be filtered by time of day and types of monitors. For example, you could calculate downtime using **Ping** monitors only.

Downtime report properties

All values are reported as percentages of the report period.

- **Group / Selected groups** - Enter text to display the names of groups in the **Group** list that match the text entered. Select one or more groups in the list, then click the **Add** button to add the groups to the **Selected groups** list. You can also click the **Select** button to browse for target groups. To remove a group, select it and click the **Remove** button. *Applies to Customized reports only.*
- **Period** - Specifies the period for this item. *Applies to Customized reports only.*
 - **Current day, week, month, quarter, year**
 - **Last day, week, month, quarter, year**
 - **User defined period**
 - **Offset in days**

Note: Report templates specify the time period when the report template is run.

- **Downtime reporting**
 - **Report downtime for assets** - Displays individual assets and their contribution to downtime.
 - **Report downtime for monitors** - Displays each monitor in each asset and its contribution to downtime.
- **Report uptime** - The time the monitor was in a normal state.
- **Report downtime** - The total time the monitor was in the alarm state.
- **Report unknown time** - Unknown is the time **Network Monitor** did not know the status of the monitor, for example if the **Network Monitor** service was stopped for a couple of hours. If left blank:
 - **Consider unknown time as uptime**
 - **Leave unknown time as unknown time**
- **Include assets and monitors with no downtime in the report** - If blank, eliminates assets from the report that have no downtime issues.

Advanced properties

- **Downtime calculation**

- **Sum** - Sums downtime values in the report.
- **Avg** - Provides average downtime values in the report.
- **Time limit** - Limits downtime data to a daily range of hours.
- **Monitor limit** - Limits downtime data to specified **types of monitors** (page 109).

Comments

Network Monitor > Reports > Report Templates > (click the name of a report template) > Add comment or click the  icon for a comment item

Network Monitor > Reports > View > (click the name of a customized report) > Add comment or click the  icon for a comment item

Comments can be included in your reports. They can also be used to include signature fields for occasions when a report has to be reviewed and signed by someone.

- **Comment** - The comment text to be included in the report.
- **Font options** - The font size and alignment of the text of the comment.
- **Signature field** - If checked, a horizontal line displays in the report where a signature can be written.

Images

Network Monitor > Reports > Report Templates > (click the name of a report template) > Add image or click the  icon for an image item

Network Monitor > Reports > View > (click the name of a customized report) > Add image or click the  icon for an image item

The **Report image** page adds custom images to your reports. Supported image files must be placed in the `KNM\reports\images` folder of the KNM host machine. After that they can be selected from this page and viewed in reports.

- **Image** - Select the desired image from the list.
- **Placement** - Specify the placement of the image in the report.

Toplists

Network Monitor > Reports > Report Templates > (click the name of a report template) > Add toplist or click the  icon for an toplist item

Network Monitor > Reports > View > (click the name of a customized report) > Add toplist or click the  icon for an toplist item

The **Toplists** report item inserts or more **toplists** (page 34) in your reports.

Toplist configurations

A single toplist item in a report includes one or more toplist configurations. After selecting **Type**, **Sorting mode**, **Entries** and **Data** values, click the **Add** button to add the configuration to the list of configurations. To remove a configuration, select it from the list and click the **Remove** button.

- **Header** - Header text describing the item in the report.
- **Period** - Select the toplist to include in the report.
 - Current day
 - Current week
 - Current month
 - Last day
 - Last week
 - Last month

- **Type** - Select the type of data.
 - Bandwidth usage
 - Bandwidth utilization
 - CPU utilization
 - Disk utilization
 - Fan speed
 - Free disk space
 - Free memory
 - Humidity
 - Luminosity
 - Memory utilization
 - Ping packetloss
 - Ping roundtrip time
 - Relative airflow
 - Swap utilization
 - Temperature
 - Transfer speed
 - Webpage fetch time
 - Wetness
- **Sorting mode**
 - Lowest entries first
 - Highest entries first
- **Entries** - Number of entries to display.
- **Data**
 - Sampled min value
 - Sampled max value
 - Period average
- **Add / Selected / Remove** - To add a toplist configuration, click the **Add** button. The selected configuration is added to the **Selected** list. To remove a configuration, select it and click the **Remove** button.

Report templates fields only

- **Filter by selection** - If checked, assets and monitors are selected when viewing the report template in the report. This option is selected by default.

Customize report fields only

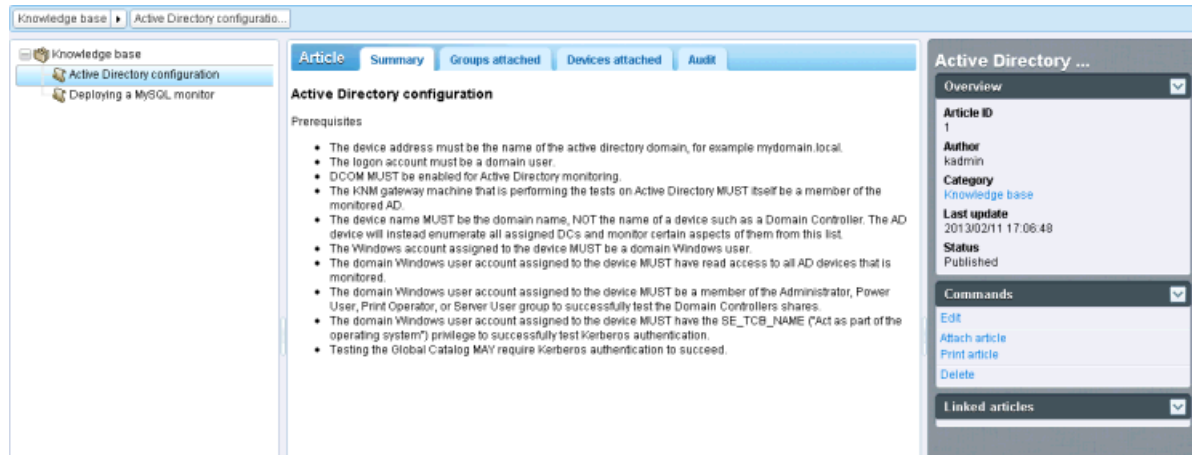
The following fields only display for Customized reports.

- **Group / Selected groups** - Enter text to display the names of groups in the **Group** list that match the text entered. Select one or more groups in the list, then click the **Add** button to add the groups to the **Selected groups** list. You can also click the **Select** button to browse for target groups. To remove a group, select it and click the **Remove** button.
- **Select asset / Selected assets** - Enter text to display the names of assets in the **Select asset** list that match the text entered. Select one or more assets in the list, then click the **Add** button to add the assets to the **Selected assets** list. You can also click the **Select** button to browse for target assets. To remove an asset, select it and click the **Remove** button.

Knowledge Base Articles

Network Monitor > Knowledgebase > View

The **Knowledge base** enables you to create a shared set of "how to" articles that can be assigned to any group, gateway, asset or monitor. This provides you with instant access to the exact reference material you need to troubleshoot and manage assets. Click any group, gateway or asset node and select the **Knowledge** (page 38) tab to see the list of **Knowledge base** articles assigned to that node.



Related Topics

- **Knowledge tab** (page 38)
- **Knowledge Base Categories** (page 87)

View tabs

- **Summary** - Displays the article.
- **Groups attached** tab - Lists the groups attached to the current article. Optionally attaches or detaches the current article to groups and assets.
- **Assets attached** tab - Lists the assets attached to the current article. Optionally attaches or detaches the current article to groups and assets.
- **Audit** tab - Shows the log of users who have updated the article.

Commands

- **Edit** - Edits the selected article.
- **Attach article** - Attaches the current article to groups and assets.
- **Print article** - Printed the current article.
- **Delete** - Deletes the current article.











Edit tabs

- **Basic properties** tab - Edits the title and body of an article. Use the following toolbar buttons to add special formatting to the text:



The more advanced toolbar buttons are described below.

- - Source - Enables you to edit the HTML tags controlling the format of the article.
- - Preview the display of text and images.
- - Pastes content copied from a Word document.

-  - Find and replace.
-  - Remove formatting.
-  - Links and unlinks text to a URL, an anchor or an element ID. Links are only supported within the same article.
 - ✓ Insert an named anchor  at a location in the article text. Then add a link that jumps the article to that named anchor when you click the link.
 - ✓ Use the Source  icon to display HTML tags and add an ID attribute to an element. Then add a link that jumps the article to that element ID when you click the link.
-  - Inserts a table at the cursor location. Table properties include number of rows and columns, caption, border width, header, cell spacing, alignment.
-  - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
-  - Insert an emoticon.
-  - Insert a symbol.
-  - Insert a page break. Used when printing an article.
- **Advanced** tab
 - **Link categories / Linked categories** - Explicitly links an article to one or more categories. A category is a knowledge base folder containing other categories or knowledge base articles. Clicking a category lists all the articles linked to that category.
 - **Add related articles / Related articles** - Links an article to other related articles. Related articles are listed in the right side panel when an article is being viewed.

See also:

- **Knowledge Base Categories** (page 87)
- **Knowledge tab** (page 38)

Knowledge Base Categories

A knowledge base **category** is a knowledge base folder containing other categories or knowledge base articles. Clicking an category in the knowledge base tree lists all the articles in the middle panel that are either descendants of that category or *explicitly linked* to that category. Articles are explicitly linked to categories using the **Advanced** (page 86) edit tab when editing an article.

Related Topics

- **Knowledge Base Articles** (page 86)
- **Knowledge tab** (page 38)

Actions

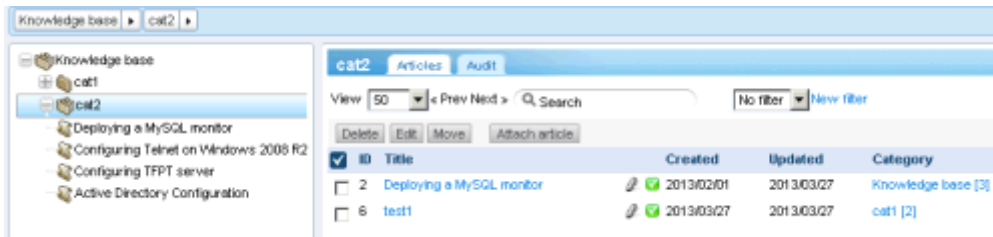
- **Delete** - Deletes a selected article
- **Edit** - Edits one or more selected articles. If multiple articles are edited, only shared properties can be edited.
- **Move** - Moves selected articles to a different position in the knowledge base tree. *This does not affect explicit links between articles and categories.*
- **Attach article** - Assigns an article to selected groups and assets.

Commands

- **Edit** - Edits a selected article.
- **Add a subcategory** - Adds a subcategory to the current category.
- **Delete category** - Deletes the current category.

Navigation Panel Reference

- **Create a new article** - Creates a new article subordinate to the current category.



Edit tabs

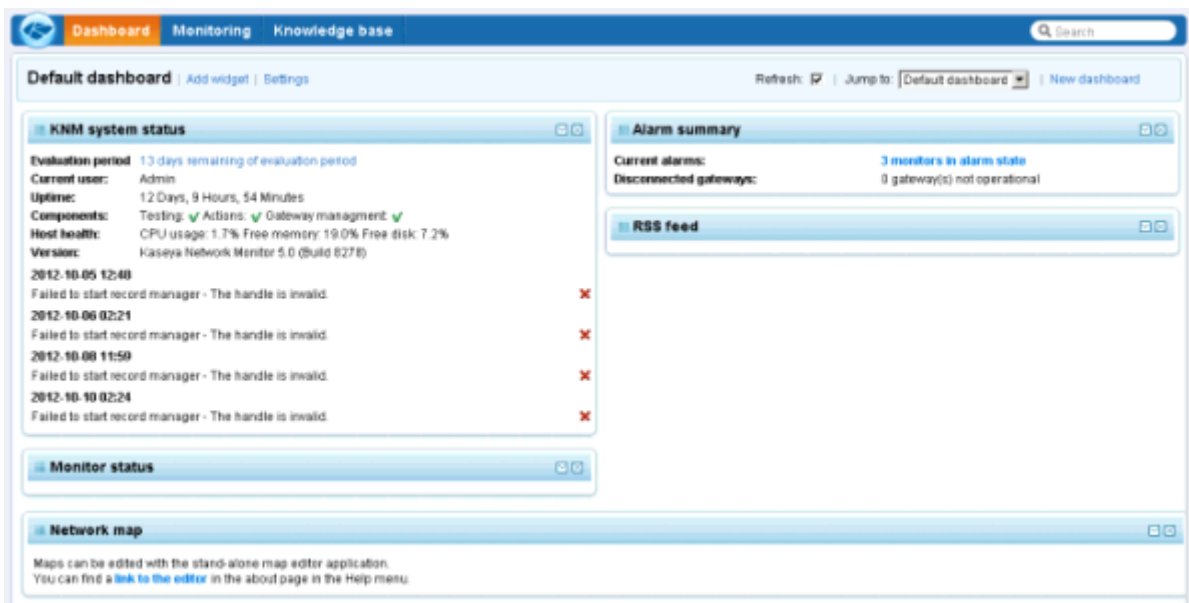
Basic properties tab

- **Name** - The name of the category.
- **Description** - A one line description of the category.

Dashboard

Network Monitor > Dashboard > View

The **Network Monitor** dashboard is a user configurable view, comprising one or more *widgets*. Each widget displays a different type of real time information.



A number of useful widgets are included with **Network Monitor**. This includes:

- Status widgets
 - Monitor status
 - Asset status
 - Group status
 - Gateway status
 - User status
 - System status
 - Alarm summary

- NOC widget
- Map widgets
 - Network map
 - Network map, small
- Misc widgets
 - Web page
 - Web page, small
 - Favourited items
 - Log entries
 - Toplists
 - Notepad
 - RSS feed

Click [Settings](#) to create or edit a dashboard. Click [Add widget](#) to add widgets to a dashboard.


Asset maintenance

[Network Monitor](#) > [Schedules](#) > [Asset maintenance](#)

The [Asset maintenance](#) page schedules "downtime" maintenance periods for assets. During a scheduled maintenance period no monitors are tested. Maintenance schedules can be either a single maintenance period or a recurring maintenance period with many flexible scheduling options.

Actions

Shift-click to select multiple rows.

- [Delete](#) - Deletes selected schedules.
- [\(Edit\)](#) - Click the  properties icon to edit a single row.
- [New schedule](#) - Creates a [new schedule](#) ([page 89](#)).

Edit asset maintenance

[Network Monitor](#) > [Schedules](#) > [Asset maintenance](#) > [New Schedule or Edit](#)

The [Edit asset maintenance](#) page specifies a single maintenance schedule that can be applied to *multiple* assets. The schedule can be for a single period or recurring periods.

Note: Simple maintenance for a *single* asset can be specified on the [Advanced](#) ([page 50](#)) tab of an asset node.

Maintenance settings

- [Select assets](#) - Enter a string in the edit box to list all asset names matching the string. Then click the [Add](#) button. Alternatively use the [Select](#) button to browse for assets.
- [Selected assets](#) - Lists selected assets. To remove items, select items in the list, then click [Remove](#).
- [Start Time](#) - Specifies the time of day to start the maintenance period.
- [Maintenance period](#) - Specifies the duration of the maintenance period, in hours and minutes.
- [Maintenance mode](#) - [Stop tests during maintenance](#). This is the only mode supported at this time.
- [Expires](#) - If checked, the maintenance schedule is automatically deleted once the maintenance period is over.
- [Description](#) - Describes the maintenance schedule.
- [Schedule type](#)

➤ Single maintenance

- ✓ **Start date** - Specifies the date to activate the maintenance schedule. Specify the date using a YYYY-MM-DD format.

➤ Repeated maintenance

- ✓ **Active between** - Specifies the date range the maintenance schedule is active. Specify the range using a YYYY-MM-DD format. If these fields are left empty the maintenance schedule is always active.
- ✓ **Day of week** - By checking a day, the maintenance schedule is active only on selected days of the week.
- ✓ **Every N:th day** - If specified, the maintenance schedule is active every Nth day from the specified start date. This option requires a specified date range in the **Active between** fields.
- ✓ **Last in month** - If checked, the maintenance schedule is active the last day of every month.
- ✓ **Days in month** - If checked, maintenance schedule is active on specific days of the month. Specify days separated with a comma.


Monitor maintenance

Network Monitor > Schedules > Monitor maintenance

The **Monitor maintenance** page schedules "downtime" maintenance periods for *monitors*. During a scheduled maintenance period no monitors are tested. Maintenance schedules can be either a single maintenance period or a recurring maintenance period with many flexible scheduling options.

Actions

Shift-click to select multiple rows.

- **Delete** - Deletes selected schedules.
- **(Edit)** - Click the  properties icon to edit a single row.
- **New schedule** - Creates a **new schedule** (page 90).

Edit monitor maintenance

Network Monitor > Schedules > Monitor maintenance > New Schedule or Edit

The **Edit monitor maintenance** page specifies a maintenance schedule that can be applied to *multiple* monitors. The schedule can be for a single period or recurring periods.

Note: Simple maintenance for a *single* monitor can be specified on the **Advanced** (page 63) tab of a monitor node.

Maintenance settings

- **Select assets** - Enter a string in the edit box to list all asset names matching the string. Then click the **Add** button. Alternatively use the **Select** button to browse for assets.
- **Selected assets** - Lists selected assets. To remove items, select items in the list, then click **Remove**.
- **Start Time** - Specifies the time of day to start the maintenance period.
- **Maintenance period** - Specifies the duration of the maintenance period, in hours and minutes.
- **Maintenance mode** - Stop tests during maintenance. This is the only mode supported at this time.
- **Expires** - If checked, the maintenance schedule is automatically deleted once the maintenance period is over.

- **Description** - Describes the maintenance schedule.
- **Schedule type**
 - **Single maintenance**
 - ✓ **Start date** - Specifies the date to activate the maintenance schedule. Specify the date using a YYYY-MM-DD format.
 - **Repeated maintenance**
 - ✓ **Active between** - Specifies the date range the maintenance schedule is active. Specify the range using a YYYY-MM-DD format. If these fields are left empty the maintenance schedule is always active.
 - ✓ **Day of week** - By checking a day, the maintenance schedule is active only on selected days of the week.
 - ✓ **Every N:th day** - If specified, the maintenance schedule is active every Nth day from the specified start date. This option requires a specified date range in the **Active between** fields.
 - ✓ **Last in month** - If checked, the maintenance schedule is active the last day of every month.
 - ✓ **Days in month** - If checked, maintenance schedule is active on specific days of the month. Specify days separated with a comma.


User notification schedules

Network Monitor > Schedules > User notification schedules

The **User work schedules** page schedules *active* periods for *users*. This prevents operators from receiving notifications unnecessarily during their off hours.

Actions

Shift-click to select multiple rows.

- **Delete** - Deletes selected user work schedules.
- **(Edit)** - Click the  properties icon to **edit** (page 92) a single row.
- **New schedule** - Creates a new schedule.

Related Topics

- **Edit user work schedule** (page 91)
- **Schedule blocks** (page 92)

Edit user work schedule

Network Monitor > Schedules > User notification schedules > New Schedule or Edit

The **Edit user work schedule** page specifies a single user work schedule. You define active days, hours and users associated with a schedule using the **Schedule blocks** (page 92) page.

Schedule properties

- **Name** - The name of the user work schedule.
- **Description** - A longer description of the user work schedule.
- **Active** - The start date and end date when the user work schedule is active.
- **Expires** - If checked, the schedule is cleared from **Network Monitor** after the active end date.

Schedule blocks

Network Monitor > Schedules > User notification schedules > Click <name of schedule>

User work schedules (page 91) are specified using *blocks* and *rules*.

- **Blocks** - A user work schedule is divided into one or more blocks. A block represents a shorter period of time within the schedule. Add blocks to create a sequence of blocks. You can move the blocks up and down in the sequence. The sequence of blocks is continuously repeated as a *rolling schedule* from the active start date to the active end date of the schedule.
- **Rules** - Users selected for a rule are "active" during the days and hours specified by a rule. They can receive notifications during these active time periods. You can specify one or more rules for each block. Rules can overlap each other and specify different users.


Example

1. Create a user work schedule for one month.
2. Create 1 block with a length of 7 days.
3. Create two rules for this single block: a weekday block and a weekend block. Set days, hours and users as appropriate for each rule.

Commands

- **Edit** - Edits the name, start date and end date of the **user work schedule** (page 91).
- **Copy** - Creates a new schedule by copying the currently selected schedule.
- **Delete** - Deletes the currently selected schedule.

Block Actions

- **Add block** (or  to edit) - Adds or edits a block.
 - **Length** - Enter the length of the block in days. For example, specifying 7 creates a block 7 days in length.
- **Delete** - Deletes selected blocks.

Rule Actions

- **Edit Rule** - Click to edit the following options.
 - **Day of week** - Days of the week this rule is active.
 - **Active between** - Start and end time of the day this rule is active.
 - **Available users** - Users available to select.
 - **Selected users** - Selected users are active during the days and hours specified by this rule and can received notifications.
- **Delete Rule** - Deletes selected rules.

Windows service list

Network Monitor > Tools > Manage Windows services

The **Windows service list** provides direct access to the list of available services on a Windows computer. Only assets identified as Windows computers and that have **Windows authentication logon accounts** (page 40) are available to select.

Displaying a Windows Service List

Enter text in the **Select asset** field to display the names of assets that match the text entered. Select one asset. Click the **Update** button to add the asset to the **Selected asset** list. You can also click the **Select** button to browse for target groups.

Actions

Select one or more services in the list and then perform one of the following actions.

- **Start** - Start selected services.
- **Stop** - Stop selected services.
- **Restart** - Restart selected services.
- **Pause** - Pause selected services. Not all services can be paused.
- **Continue** - Resume the running of paused services.

See Also

- **Windows service control** (page 149) (action)
- **Windows service control** (page 157) (scheduled event)
- **Windows service status** (page 141) (monitor)

MIB Browser

Network Monitor > Tools > Mib browser

(asset name) > Open MIB browser command

(asset name) > Add new monitor > SNMP > OID [...]

(asset name) > Add new monitor > SNMP trap > OID include/exclude filters [...]

The **MIB Browser** page displays a MIB tree you can navigate to select **OID values** (page 93). *The MIB Browser must be able to successfully connect to the SNMP agent on the remote asset or computer to retrieve and select OID values in this dialog.*

Five filter fields are used to specify OID values and their corresponding values on a remote asset. If the connection is successful and the remote asset supports the selected OID, the OID value displays in the upper right corner when you click an OID item in the tree.

- **Hostname** - The name of the asset.
- **Port** - Defaults to 161.
- **Gateway** - The gateway used by the asset.
- **SNMP version** - The version of SNMP protocol used to connect to the SNMP agent on the asset: v1, v2c, v3
- **Read community** - The SNMP read community name assigned to the asset you are connecting to. Displays when v1 and v2c is selected.

Note: See **Compiling custom MIB files** (page 94) to modify the MIB tree displayed in this dialog.

Selecting an OID

1. Click any OID in the tree displayed in the left pane to display the OIDs properties in the right pane.

Note: OID values are only returned if a connection is made to the asset and the asset supports the selected OID request.

2. Click the **Select OID** button.

MIB Objects

Each SNMP-enabled asset 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 manufacture in the form of a **MIB file**, so OIDs are usually called **MIB objects**. The MIB files can be imported into a "MIB aware" application, such as **Network Monitor**. The **Network Monitor** comes pre-installed with many popular sets of MIB objects, so **compiling custom MIB files** (page 94) is usually only required for devices with specialized MIB objects.

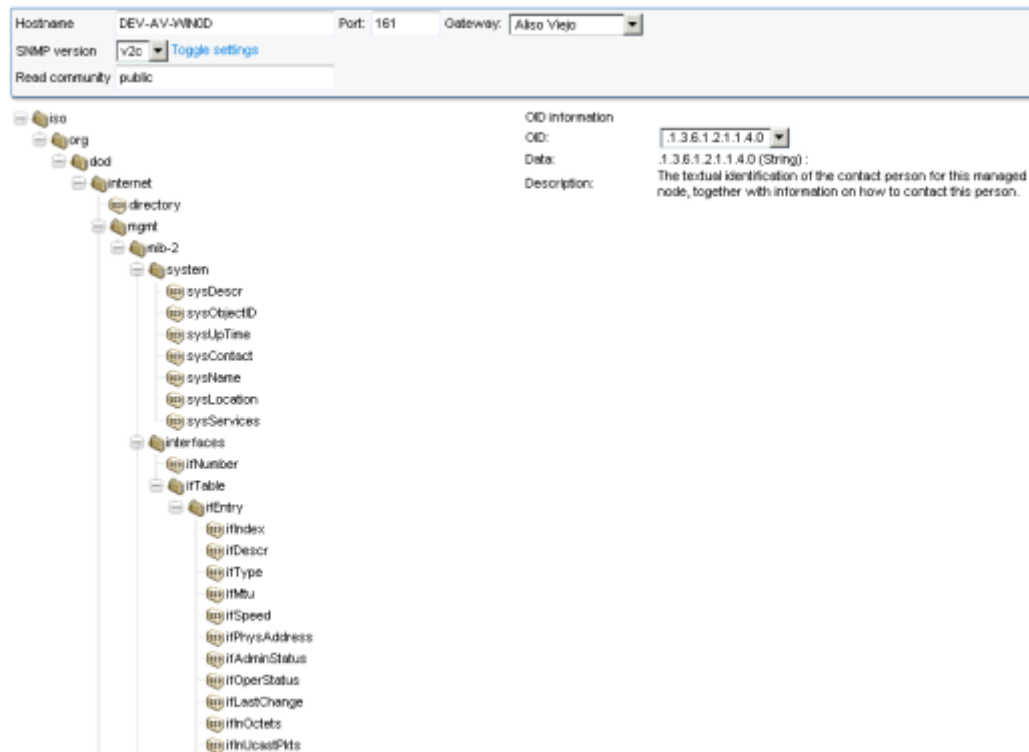
MIB Tree

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.

Network Monitor displays the MIB tree in a MIB browser. The MIB browser can be displayed using any of the following methods of access:

- Network Monitor > Tools > MIB browser
- <asset name> > Open MIB browser command
- <asset name> > Add new monitor > SNMP > OID [...]
- <asset name> > Add new monitor > SNMP trap > OID include/exclude filters [...]

The same tree displays at all times, based on the **MIB files installed on the server** (page 94). Below is an example of the MIB browser dialog.



Compiling Custom MIB Files

By using the MIB compiler you can compile text MIB files into a binary format that **Network Monitor** can read. Compiling MIB files requires understanding about how MIB files work as well as a general understanding of SNMP and **MIB objects** (page 93). A number of different RFC documents outline the fundamental base that all other MIB files are based on.

Note: The community name, SNMP version, and port used by **Network Monitor** to connect to an SNMP asset is set on the **Authentication** (page 40) tab of an asset node. The asset node may inherit this setting from a parent node. See the **Installation Checklist** (page 9).

As an example, this is the compile order of a CISCO ® product MIB.

1. SNMPv2-SMI.mib
2. SNMPv2-TC.mib
3. SNMPv2-MIB.mib
4. RFC1213-MIB.mib
5. IF-MIB.mib
6. CISCO-SMI.mib
7. CISCO-PRODUCTS-MIB.mib
8. CISCO-TC.mib

The first 5 files in this example are common for most product MIB files, and are included in the default knm.mib binary MIB file.

Warning: All of these files must be compiled at the same time, otherwise the MIB compiler fails due to unresolved symbols.

Contents of the default KNM MIB file

The default knm.mib file included in the installation contains the following base OIDs (object identifiers).

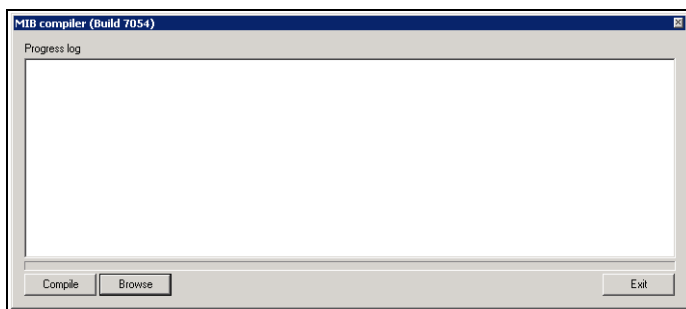
- iso.org.dod.internet.directory
- iso.org.dod.internet.mgmt
- iso.org.dod.internet.experimental
- iso.org.dod.internet.private
- iso.org.dod.internet.security

The file is located in the \<Kaseya_Installation_Directory>\KNM\mibs directory.

Download and Run the MIB Compiler

1. Navigate to the Network Monitor > Tools > [Utility downloads](#) page.
2. Click the [MIB compiler](#) link to download the utility to your local machine.
3. Run the utility.

Compiling a MIB file



1. Start the <Kaseya_Installation_Directory>\knm\mibcompiler.exe.
2. Click the [Browse](#) button to select one or more *.mib files.
 - Locate the default knm.mib file in the KNM\mibs folder of the **Network Monitor** host machine and double click it to select it.

- Select any additional *.mib files you want to include for compiling.
- 3. Click the **Compile** button.
- 4. Specify where you want to save the compiled *.dat file.
- 5. Click the **Browse** button to select the *.dat file that was just compiled. An interactive MIB tree displays in the main window. You can use it to navigate through the different OIDs.
- 6. Move or copy the compiled *.dat file to the KNM\mibs folder.

Record manager log

Network Monitor > Tools > Record manager log

The **Record manager log** page displays log entries created by the Kaseya Record Manager service. This service is installed when **Network Monitor** is installed. Record Manager provides statistical storage and query functions for **Network Monitor**. It based on the same service class as the Kaseya Network Monitor service so the same install/uninstall commands work with both.

Folders

Record Manager has one base directory specified in the rminit.cfg file. This directory contains one folder for each day and a folder called realtime. The realtime folder contains X number of records per monitor to serve as a quick access cache. This file can be rebuilt.

rminit.cfg

Record Manager has an "init" file called rminit.cfg containing the following parameters:

```
# Record manager configuration file
bind_if=
listen_port=3030
storage_path=rmstorage
service_name=Kaseya Record Manager
display_name=Kaseya Record Manager
```

RPC

Record Manager communicates with **Network Monitor** using RPC on port 3030 (default) using TCP/IP protocol. By default Record Manager is installed in the same directory as KNM. If necessary, Record Manager can be installed on a different machine.

The KNM init.cfg parameters must be modified to reflect this.

```
RECORDMGR_HOST=host_name_or_ip
RECORDMGR_PORT=3030
```

System admin console related commands

Command	Switch	Description
Status	-recordmgr	Prints record manager status messages.
recordmgr-rebuild	YYYY-MM-DD	Rebuilds the file for the specified date, ex. 2012-09-01.
recordmgr-rebuild	-all	Rebuilds all final files. Should be used with extreme care. This operation may take hours to complete. During this time reports may not deliver the correct result.

Syslog message

Network Monitor > Tools > Syslog message

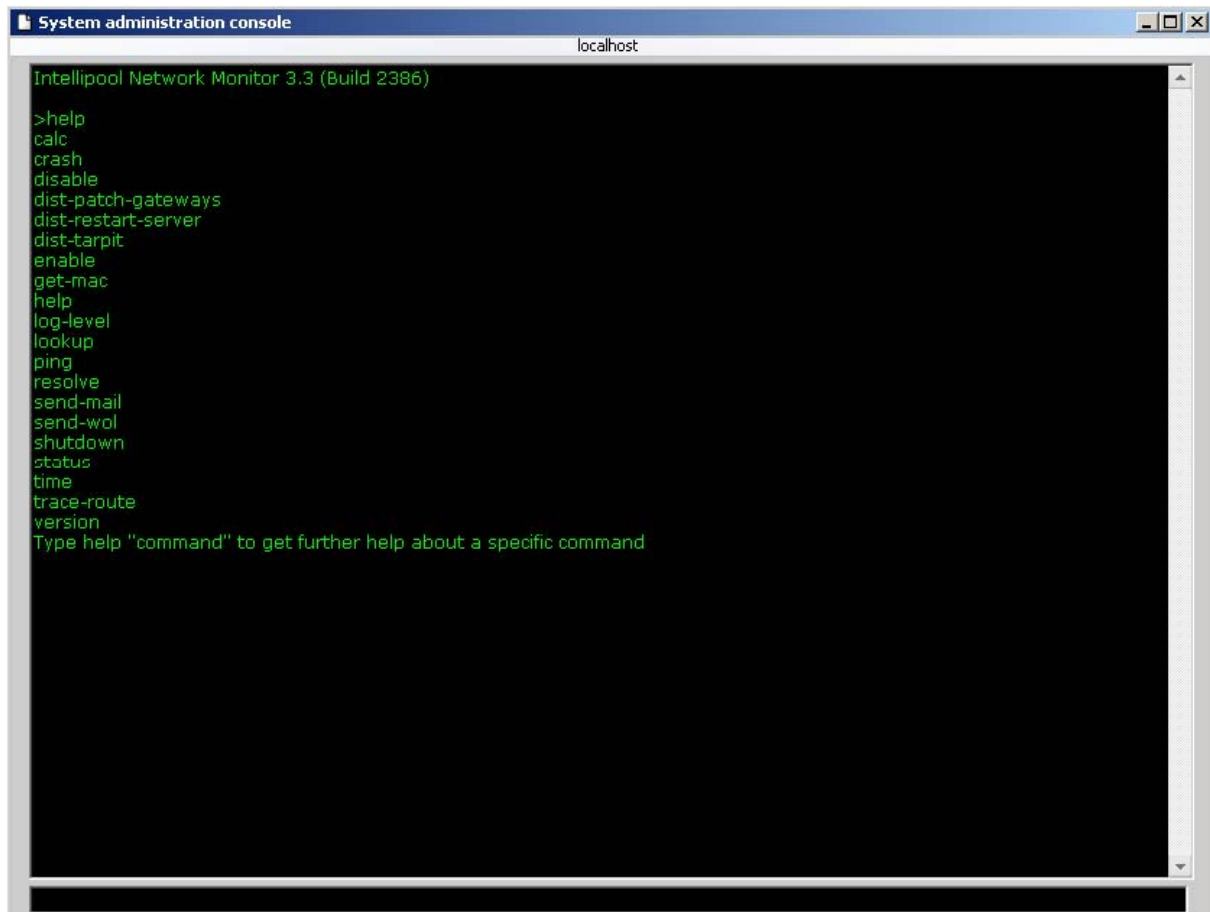
The [50 latest syslog messages](#) page displays the 50 latest syslog messages sent to **Network Monitor** by all **Syslog** (page 136) monitors that are members of the same gateway.

You must activate syslog message collection for each gateway separately, by checking the Network Monitor > (selected gateway) > Edit > **Advanced tab** (page 39) > **Syslog server** checkbox.

System administrator console

Network Monitor > Tools > System admin console

The purpose of the **System administrator console** is to provide an easy way to perform recurring system administrative tasks. The interface is a normal Command Line Interface (CLI) that most system administrators are familiar with. Only users flagged as system administrators can access the console.



The system administrator console

Commands

- **calc** - A built-in calculator for simpler calculations. Usage example:

```
calc 41+1
```

- **disable** - Disables a feature in **Network Monitor**.
 - **-all** - Disables all the listed features.

Navigation Panel Reference

- `-testing` - Disables testing.
- `-actions` - Disables execution of actions.
- `-statistics` - Disables statistical storage.
- `-login` - Disables login for normal users, but system administrators can login.
- `dist-patch-gateways` - Starts patching all gateways that require patching.
- `dist-restart-server` - Restarts the **Network Monitor** distributed testing server.
- `dist-tarpit` - Add or removes IP numbers from the tar pit. The tar pit protects the server from brute force login attempts and DOS attacks.
 - `-block` - Blocks the specified IP number.
 - `-unblock` - Unblocks the specified IP number.
 - `-list` - Lists all IP numbers in the tar pit.
 - `-blocktime` - Sets the default block time, in minutes. Defaults to 20.

`dist-tarpit -block 192.168.0.1`

- `enable` - Enables a feature in **Network Monitor**.
 - `-all` - Enables all the listed features.
 - `-testing` - Enables testing.
 - `-actions` - Enables actions.
 - `-statistics` - Enables statistical storage.
 - `-login` - Enables login for normal users.
- `get-mac` - Retrieves the MAC address for a certain IP number. Only IPs on the local area network of the **Network Monitor** host machine are likely to return a MAC address.

`get-mac 192.168.42.1`

- `help` - Displays help information for the different commands in the console. Type `help <command>` to display command specific help.
- `log-level` - Adjusts the log level. When **Network Monitor** restarts, it defaults to the log level specified in the `init.cfg` file. The available values are 0, 1 and 2.
- `lookup` - Queries a DNS server for information about a domain.

`lookup kaseya.com`

- `ping` - Pings an IP number or host name.
- `resolve` - Resolves a host name to an IP number.

`resolve www.kaseya.com`

- `send-mail` - Sends an email to the specified address using the **Network Monitor** built in email client.

`send-mail myaddress@test.com , "Testing KNM" , "This is a test mail"`

- `send-wol` - Sends a Wake on Lan packet to the specified host.

`send-wol 192.168.42.1`

- `shutdown` - Shuts down **Network Monitor** and flushes all un-saved settings to disk.
- `status` - Displays feature status information.
 - `-thread` - Displays current total number of threads that **Network Monitor** is using.
 - `-threadpool` - Displays the total number of threads in a thread pool.
 - `-memory` - Displays the current **Network Monitor** memory usage.
 - `-cpu` - Displays the current **Network Monitor** CPU usage.
 - `-handle` - Displays the current **Network Monitor** handle usage.
 - `-feature` - Displays the status of **Network Monitor** features.
- `time` - Prints the local date and time of the **Network Monitor** host machine.
- `trace-route` - Performs a trace route to the specified host.

- **version** - Prints the version of **Network Monitor**. Can also be used to check if a new version of **Network Monitor** is available.

version -check

System log

Network Monitor > Tools > System log

The **System log** page displays log entries created by the Kaseya Network Monitor service. Mainly used when a problem has occurred. You can enable verbose logging by setting `LOG_LEVEL = 2` in the `Init.cfg` (page 159) file. The verbose system log is kept in a separate text file:

`<Kaseya_Installation_Directory>\Logs\Services\KaseyaNetworkMonitor.log`.

Trap messages

Network Monitor > Tools > Trap messages

The **50 latest SNMP traps** page displays the 50 latest SNMP trap messages received by each gateway. Use this page to ensure SNMP trap messages are being received by **Network Monitor**. **SNMP trap** (page 132) monitors cannot respond to an SNMP trap message unless that SNMP trap message displays on this page. You can also use this page to create SNMP trap monitors for one or more assets.

50 latest SNMP traps						
<div>Also View <input type="button" value="Update from gateway"/></div> <div><input type="button" value="Create monitor"/></div>						
<input checked="" type="checkbox"/>	Source IP	Agent IP	Enterprise OID	Community	Time	Message
<input type="checkbox"/>	10.10.32.6	10.10.32.6	1.3.6.1.6.3.1.1.5.5	public	2013-03-26 15:16:12	.1.3.6.1.2.1.1.3.0 TimeTicks:4255091 .1.3.6.1.6.3.1.1.4.1.0 OID: 1.3.6.1.6.3.1.1.5.5 .1.3.6.1.6.3.18.1.3.0 IP Address:10.10.32.6 .1.3.6.1.6.3.18.1.4.0 String:public .1.3.6.1.6.3.1.1.4.3.0 OID: 1.3.6.1.4.1.311.1.1.3.1.2
<input type="checkbox"/>	10.10.32.6	10.10.32.6	1.3.6.1.6.3.1.1.5.5	public	2013-03-26 15:16:12	.1.3.6.1.2.1.1.3.0 TimeTicks:4255091 .1.3.6.1.6.3.1.1.4.1.0 OID: 1.3.6.1.6.3.1.1.5.5 .1.3.6.1.6.3.18.1.3.0 IP Address:10.10.32.6 .1.3.6.1.6.3.18.1.4.0 String:public .1.3.6.1.6.3.1.1.4.3.0 OID: 1.3.6.1.4.1.311.1.1.3.1.2
<input type="checkbox"/>	10.10.32.6	10.10.32.6	1.3.6.1.6.3.1.1.5.5	public	2013-03-26 15:16:12	.1.3.6.1.2.1.1.3.0 TimeTicks:4255090 .1.3.6.1.6.3.1.1.4.1.0 OID: 1.3.6.1.6.3.1.1.5.5 .1.3.6.1.6.3.18.1.3.0 IP Address:10.10.32.6 .1.3.6.1.6.3.18.1.4.0 String:public .1.3.6.1.6.3.1.1.4.3.0 OID: 1.3.6.1.4.1.311.1.1.3.1.2

Actions

- **Update from gateway** - Select a gateway from the drop-down list and click **Update from gateway** to display the list of SNMP trap messages received by that gateway.
- **Create monitor** - Create **SNMP trap** (page 132) monitors for one or more assets based on a received SNMP trap message.

My settings

Network Monitor > Tools > My settings

The currently logged on user can change basic settings of their own user record. Properties are organized into the following tabs:

- **Basic properties tab** (page 100)
- **Interface options tab** (page 100)

Basic properties tab

Network Monitor > Tools > My settings > Basic properties tab

Basic properties

- **User group** - Displays the user groups the currently logged on user is a member of.
- **API Key** - A numerical string, associated with the user record, used to authenticate logons by third party utilities connecting to the **Network Monitor** server. A new, randomly-generated string can be generated by clicking the **New** button. The API key is used by the **Gizmo** (page 188) utility.
- **SMS number** - SMS alerts for this user are sent to this SMS phone number.

Interface options tab

Network Monitor > Tools > My settings > Interface options tab

Interface options

- **Refresh** - Specifies the refresh time in seconds for pages in the management interface.
- **View reports** - Open reports in same window or Open reports in a new window.
- **Follow current node** - If checked, all other open nodes close when a node is selected. If unchecked, all other open nodes remain open when a node is selected.


User notification groups

Network Monitor > User > User notification groups

The **User group list** maintains user group notifications. Asset notifications are sent to all members of the user group assigned to that asset using the **Notification user group** setting on the **Basic properties tab** (page 49) of the asset.

Actions

Shift-click to select multiple rows. Enter a string in the search box to filter the list of records displayed.

- **Delete** - Deletes selected users groups.
- **(Edit)** - Click the  properties icon to edit a single row.
- **New group** - **Create a new user group** (page 100).

Create a new user group

Network Monitor > User > User notification groups > New group or Edit

The **Edit user group** page assigns users to a user group.

User Group properties

- **Name** - The name of the user group. It should be a descriptive name.
- **Description** - A longer description of the user group.

Group members

- **User** - All available users in the VSA partition are listed in this field. To add a user to the user group, select it from the list and click the **Select** button.
- **Current members** - Lists all users that are currently added to this user group. To remove a user from the user group, select it from the list and click the **Remove** button.

- **Group manager** - The group manager specifies one user to be assigned as manager for the user group. When using user schedules to schedule user working hours, the group manager is the default contact when no other user is available.

Customized data types

VSA > Network Monitor > Settings > Customized datatypes

The **Customized data types** page creates customized data types for use with monitors capable of storing generic data. These monitors are:

- CIM performance monitor
- Database monitors (Database server, Oracle, MySQL, SQL Server)
- Powershell script monitor
- SNMP monitor
- SSH2 script monitor
- VMware performance monitor
- Windows performance monitor
- WMI monitor

Network Monitor comes pre-configured with many different data types and knows how to handle those data types when it comes to reporting and presentation. In some cases it is useful to define your own data types, for example when you are dealing with proprietary data.

Basic properties

- **Name** - The name of the data type.
- **Description** - Enter a description for the data type.
- **Toplist** - If checked, the data type is included as a selectable item in **toplist** (*page 84*) report items.
- **Compatible monitors** - The monitor types compatible with this data type. Select a monitor type from the list and click the **Select** button. A selected monitor type can be removed from the selected list, by selecting it and clicking the **Remote** button.
- **Stored unit** - If the data type uses one or more units, you must specify the base unit used by monitors.
- **Compatible units** - Select and add units from the list that you want to include with this data type. This is useful for reporting when you want to display proprietary data in different units.

Presentation settings


- **Decimals** - Enter the number of decimals to use when this data type is displayed and reported.
- **Clipping** - Optionally enter low or high clipping values for this data type.

Asset templates

Network Monitor > Settings > Asset templates

The **Asset templates** page specifies the properties of multiple monitors, similar to an asset. The asset template is then applied to one or more assets. Configuring one monitor at a time for thousands of assets isn't practical. Instead select a pre-defined asset template or configure your own, then assign the asset template to the appropriate asset. You should have an asset template for each type of asset you manage. See **Asset Templates** (*page 52*) for more information.

Actions


- **Edit** - **Edits an hyperlinked asset template** (page 102). Applies only to *custom* asset templates created using the **Save as template** (page 52) command when an asset is selected.
- **Import** - Import an asset template from an external XML file.
 - An asset template configuration can be exported from one instance of **Network Monitor** and imported into another instance of **Network Monitor**. This enables the community of **Network Monitor** users to share monitoring solutions.
 - A Windows performance monitor set or SNMP set can be exported from the VSA and be converted on import into an asset template configuration.
- **Delete** - Deletes selected asset templates.
-  - Edits the name and description of an asset template.

Editing asset templates

Network Monitor > Settings > Asset templates

The **Monitor configuration** page configures the list of monitors in the asset template.

Actions

- **Delete** - Deletes selected monitors.
- **(Click  to edit the monitor)** - Monitors within an asset templates are defined using most of the same properties as an unlinked monitor. Refer to the **Monitor reference** (page 109) for a description of each monitor's properties.

Commands

- **New monitor** - Adds a new monitor.
- **Export to XML** - Exports the asset template to an external XML file. Exported asset template data never contains any private information, such as usernames or passwords. The information included in the exported data is for monitor configurations, but excludes authentication settings.
- **Update from XML** - Updates the asset template from an external XML file.

Log settings

VSA > Network Monitor > Settings > Log settings

The **Log settings** page sets log policies for **Network Monitor**. **Network Monitor** is continuously writing a system log containing information about various system events and other status information. **Network Monitor** can also be configured to send log information to various services.

Log policies are set using the following tabs.

- **Windows event log**
- **Syslog**
- **SNMP traps**
- **Retention**

Windows event log tab

- **Windows event log** - If checked, **Network Monitor** stores log information in the Windows Event log in the **Application** log folder.

Syslog tab

- **Syslog** - If checked, **Network Monitor** sends log information to a syslog daemon. Specify the address and port number to a host with a running syslog server. The **Network Monitor** syslog client uses the UDP protocol and port 514 by default.
- **Syslog server** - The address of the syslog server receiving the log information.
- **Syslog port** - The port number of the syslog server.

SNMP trap tab

- **SNMP trap** - If checked, **Network Monitor** sends all log information as SNMP traps to a remote trap console.

Note: Kaseya has created a custom MIB file that can be imported by the software receiving traps from **Network Monitor**. You can find the MIB file, named knm.mib, in the \mibs directory.

- **Trap receiver** - The host name or IP number of the receiver of the traps.
- **Trap port** - Port number that the trap receiver listens to.
- **Community** - SNMP trap community string.

Note: Use the **Advanced** tab of a **gateway node** (page 38) to receive SNMP trap messages on a network.

Retention

Specifies how long to keep data—Forever, Month, Quarter, Year—for the following. Month, quarter and year settings represent a count of days from the current day: 30, 90 and 365 days.

- **Log retention**
- **Record retention**
- **Toplist retention**

NOC settings

Network Monitor > Settings > NOC configuration

The **NOC settings** page creates customized NOC (Network Operations Center) views. These views are normally viewed on a full screen monitor.

See the **NOC tab** (page 41) for instructions on how to display a NOC view.

Generic settings tab

- **NOC view mode** - This is a global setting affecting all NOC views. If set to View all monitor types all monitor types are visible in the NOC matrix. If Hide unavailable monitor types is selected, only monitor types included in a specific NOC view configuration are shown when the NOC view is displayed.

View configuration tab

NOC views are configured using this tab. To create a new NOC view, click the **New view** button. To edit an existing NOC view, select the view from the list and click the **Edit** button. The following properties can be set for a NOC view.

- **View title** - This is the title of the NOC view and displays on top of the NOC view.
- **Group by** - Specifies if the NOC view displays networks, assets, or assets followed by monitors.
- **Monitor type filter** - Filters the monitors displayed by monitor type.

Other system settings

Network Monitor > Settings > Other system settings

The **Other system settings** page specifies additional settings for alerts and other events, using the following tabs:

- **Monitor defaults**
- **Date & week formats**
- **PageGate integration**
- **Other settings**

Monitor defaults

This tab contains default settings for monitor parameters related to monitoring and storage of statistical data.

- **Test interval** - The default poll interval for new monitors.
- **Alarm gen.** - The default alarm generation value for new monitors.
- **Alarm test interval** - The default alarm test interval for new monitors.
- **Telnet prompt** - Enter the command prompts, separated by a comma. Whenever **Network Monitor** logs into a telnet server, it needs to know what the command prompt looks like.
- **Telnet login prompt** - Enter the login prompts, separated by a comma. Whenever **Network Monitor** logs into a telnet server, it needs to know what the login prompt looks like.
- **Telnet pass prompt** - Enter the password prompts, separated by a comma. Whenever **Network Monitor** logs into a telnet server, it needs to know what the password prompt looks like.

Date & week formats

This tab contains settings for date and week formats in **Network Monitor**.

- **Date format** - Specifies the date format preferred when displaying a date in the management interface and alert messages.
- **Week format** - Specifies the week format preferred.
- **Week numbering** - Specifies the week numbering method used in your region.

PageGate integration

This tab contains settings for PageGate integration in **Network Monitor**. PageGate is a paging gateway application developed by NotePage (<http://www.notepage.net> (*http://www.notepage.net*)).

- **Interface method** - Select the interface method to communicate with the PageGate software. Currently the only supported method is the `GetAscii` method.
- **Polling directory** - Specify the polling directory used for the `GetAscii` method. Please see the documentation for the PageGate software for more details.

SMS settings

Network Monitor > Settings > SMS > SMS settings

Network Monitor can send SMS through a modem connected to the **Network Monitor** host machine. The modem can either be a GSM phone or a modem capable of sending SMS via a fixed line service provider. The **SMS settings** tab configures the logical settings required to enable the connection.

- **GSM phone port** - Select the port used to connect to the phone from the list of available COM ports.
- **Baud rate** - Baud rate is the speed **Network Monitor** reads and writes to the modem. Refer to the modem's documentation to specify the correct value. A setting of 2400 is recommended, if you're not sure what to select. *Selecting the wrong baud rate can result in sporadic failures when sending SMS messages.*

- **PIN Code** - Optional PIN code field. Some GSM phones requires **Network Monitor** to send a PIN code before sending a message. Enter the 4 digit PIN code in this field.

Configuring the modem

1. Select the serial port the GSM modem is connected to.
2. Select the baud rate. Defaults to **9600**.
3. (Optional) Enter the PIN code to unlock the SIM card.
4. Click the **Save** button to store the new settings.

User phone number

An SMS phone number must be specified for each user receiving SMS notifications from **Network Monitor** using either of the following:

- Network Monitor My settings > **Basic properties tab** (page 100) > **SMS number** field

Tested SMS assets

- Falcom Samba
- Falcom Swing
- Falcom Twist
- Nokia 30
- Z-text fixed line SMS modem

Along with this list, almost all modern GSM phones and modems work. The asset must support Text mode SMS and be able to connect to a COM port. An asset may also connect to an USB port but the asset driver must be able to emulate a standard serial port so it can be discovered by **Network Monitor**.

SMS modem installation checklist

The asset should be connected to a serial port, or USB port with serial emulation, on the **Network Monitor** host machine.

1. Connect the phone cable to the **Network Monitor** host machine.
2. Install the modem driver for your phone (if required).
3. With a terminal program connect to the phone.
4. Try to send a SMS by typing the following.
 - **ATZ**
 - **KNM SMS TEST**
 - **Press CTRL-Z**
 - **AT+CMGF=1**
 - **AT+CMGS="<PHONENUMBER>"**
5. The SMS should now be sent. Remember to replace **<PHONENUMBER>** with the number of the receiving phone and keep the quote signs (e.g. **"0068455"**). On the last line you should press the **CTRL-Z** key combination.
6. The phone should answer with CMGS followed by a number indicating the ID of the sent SMS.
7. The phone is now ready for use by **Network Monitor**.

CMS Error codes

8	Operator determined barring
10	Call barred
21	Short message transfer rejected
27	Destination out of service

Navigation Panel Reference

28	Unidentified subscriber
29	Facility rejected
30	Unknown subscriber
38	Network out of order
41	Temporary failure
42	Congestion
47	Resources unavailable, unspecified
50	Requested facility not subscribed
69	Requested facility not implemented
81	Invalid short message transfer reference value
95	Invalid message, unspecified
96	Invalid mandatory information
97	Message type non-existent or not implemented
98	Message not compatible with short message protocol state
99	Information element non-existent or not implemented
111	Protocol error, unspecified
127	Interworking, unspecified
128	Telematic interworking not supported
129	Short message Type 0 not supported
130	Cannot replace short message
143	Unspecified TP-PID error
144	Data coding scheme (alphabet) not supported
145	Message class not supported
159	Unspecified TP-DCS error
160	Command cannot be actioned
161	Command unsupported
175	Unspecified TP-Command error
176	TPDU not supported
192	SC busy
193	No SC subscription
194	SC system failure
195	Invalid SME address
196	Destination SME barred
197	SM Rejected-Duplicate SM
198	TP-VPF not supported
199	TP-VP not supported
208	D0 SIM SMS storage full
209	No SMS storage capability in SIM
210	Error in MS
211	Memory Capacity Exceeded
212	SIM Application Toolkit Busy
213	SIM data download error
255	Unspecified error cause

300	ME failure
301	SMS service of ME reserved
302	Operation not allowed
303	Operation not supported
304	Invalid PDU mode parameter
305	Invalid text mode parameter
310	SIM not inserted
311	SIM PIN required
312	PH-SIM PIN required
313	SIM failure
314	SIM busy
315	SIM wrong
316	SIM PUK required
317	SIM PIN2 required
318	SIM PUK2 required
320	Memory failure
321	Invalid memory index
322	Memory full
330	SMSC address unknown
331	No network service
332	Network timeout
340	NO +CNMA ACK EXPECTED
500	Unknown error
512	User abort

Default messages

Network Monitor > Settings > SMS > Default messages tab

The **Default messages** page sets the default format for acknowledge notification messages. *This format is not inherited down the monitor tree.*

Note: The **Alarm Messages** (page 65) topic lists the format variables you can include in an acknowledgment notification message.

The **Report Subject** line specifies the default format for an email subject line when a generated report is emailed to recipients.

Monitor Reference

This chapter contains a reference for *monitor-specific settings*. See [Editing Monitors](#) (page 61) for *standard monitor settings*.

Monitors by Operating System

The types of monitors you can add to an asset depends on the asset's identified **Operating system**. Typically the **Operating system** for an asset is identified during **Network Discovery** (page 25). You can change the **Operating system** (page 49) identified for an asset manually. The following table shows you which types of operating systems support each monitor.

	Windows	Linux/Unix	VMWare	Cisco IOS based	Other/ Unidentified
Active Directory (page 110)					
Bandwidth utilization (page 111)					
CIM monitor (page 112)					
Citrix server (page 113)					
CPU utilization (page 114)					
Database server (page 114)					
Datastore utilization (page 115)					
DHCP query (page 115)					
Directory property (page 116)					
Disk utilization (page 117)					
DNS lookup (page 117)					
Environment monitor (page 118)					
Eventlog (page 118)					
Exchange Server (page 119)					
File Change (page 120)					
FTP server (page 120)					
IMAP4 server (page 121)					
JVM performance (page 121)					
LDAP query (page 122)					
Log file (page 123)					
Lua script (page 124)					
Mail server QOS (page 124)					
Memory utilization (page 125)					

MySQL (page 125)					
NNTP server (page 127)					
Oracle (page 127)					
Ping (page 128)					
POP3 server (page 129)					
Process status (page 129)					
RADIUS server (page 129)					
Salesforce query (page 130)					
SMTP server (page 131)					
SNMP (page 131)					
SNMP trap (page 132)					
SQL Server (page 133)					
SSH2 script (page 135)					
SSH2 server (page 135)					
Swap file utilization (page 135)					
Syslog (page 136)					
TCP port scan (page 136)					
Telnet server (page 137)					
Terminal service (page 137)					
TFTP server (page 137)					
Transfer speed (page 138)					
Vmware performance (page 138)					
Web server (page 139)					
Windows performance (page 140)					
Windows service status (page 141)					
WMI Query (page 141)					

Active Directory monitor

The **Active Directory** monitor is capable of monitoring several key aspects of an Active Directory server, including replication latency, domain controller time variance and verification of Kerberos authentication.

- System type: Windows
- Category: Directory service

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor prerequisites

- The asset address must be the name of the active directory domain, for example `mydomain.local`.
- The logon account must be a domain user.
- DCOM MUST be enabled for Active Directory monitoring.
- The KNM gateway machine that is performing the tests on Active Directory MUST itself be a member of the monitored AD.
- The asset name MUST be the domain name, NOT the name of an asset such as a Domain Controller. The AD asset will instead enumerate all assigned DCs and monitor certain aspects of them from this list.
- The Windows account assigned to the asset MUST be a domain Windows user.
- The domain Windows user account assigned to the asset MUST have read access to all AD assets that is monitored.
- The domain Windows user account assigned to the asset MUST be a member of the Administrator, Power User, Print Operator, or Server User group to successfully test the Domain Controllers shares.
- The domain Windows user account assigned to the asset MUST have the SE_TCB_NAME ("Act as part of the operating system") privilege to successfully test Kerberos authentication.
- Testing the Global Catalog MAY require Kerberos authentication to succeed.

Monitor specific properties

- **Logon account** - The logon account contains the credentials to use when testing the active directory server. The account must be a domain user or the test fails.
- **Kerberos authentication** - If checked, tests if the Active Directory can perform a Kerberos authentication successfully. Any authentication error is written to the error report, and an alarm is raised.
- **Global catalog** - If checked, tests if the Global Catalog Domain Controller is found. Any error is written to the error report, and an alarm is raised.
- **DC:s published in DNS** - If checked, tests if the Domain Controller's service DNS SRV records are found in the DNS ("`_ldap._tcp.DOMAIN.`", "`_kerberos._tcp.DOMAIN.`", "`_ldap._tcp.dc._msdcs.DOMAIN.`", "`_kerberos._tcp.dc._msdcs.DOMAIN.`", "`_ldap._tcp.Default-First-Site._sites.DOMAIN.`", etc.)
- **Replication** - If checked, tests if the last replication attempt was successful.
- **Max DC time variance** - Measure the time variance in seconds between domain controllers. If the time difference between the domain controllers are above this value the test fails.

LDAP query option

An optional LDAP query statement can be executed and its output compared to a predefined value using a compare operation.

- **LDAP query** - LDAP query to perform.
- **Compare value** - Value to compare query result with.
- **Value type** - Type of value that is compared with the retrieved value from the database.
- **Operation** - Operation to evaluate the returned query result and the compare value to determine if the test succeeded or failed.

Bandwidth utilization monitor

Bandwidth utilization monitors bandwidth on a network interface. It can be configured with or without threshold settings. On Windows assets, the methods for measuring bandwidth can be *SNMP* or *WMI* or *Windows performance counters*. For all other types of assets, SNMP is the method used. **Always**

consider using **SNMP for monitoring bandwidth** since it is much faster and leaner on resources than WMI or Windows performance counters.

- For WMI or Windows performance counters, a Windows user with permissions to read the registry on the monitored asset is required.
- When using Windows performance counters, the service “Remote Registry” must be enabled and started on the monitored asset.
- If you experience issues with this monitor type on Windows machines, try unchecking the **Use WMI** checkbox on the **Advanced tab** (page 50) of the asset node.
- The community name, SNMP version, and port used by **Network Monitor** to connect to an SNMP asset is set on the **Authentication** (page 40) tab of an asset node. The asset node may inherit this setting from a parent node. See the **Installation Checklist** (page 9).
- System type: All
- Category: Performance

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Interface name** - Select the interface to monitor.
- **Interface speed** - Optional parameter to manually set the interface speed. This can be useful if you are monitoring a NIC that is connected to a slower connection such as a ADSL line. The speed is always entered in Kbps.
- **Force SNMP** - Displays if SNMP is detected on the asset. If checked, SNMP is used, even if the asset is a Windows system type.
- **Check link status** - If checked, monitoring of Up or Down status. SNMP is the only method that enables you to select the **Check link status** checkbox.
- **Unit** - Unit to record and display bandwidth utilization data in. This cannot be changed once the monitor has been created.
- **Threshold** - The upper threshold in the selected unit.
- **Inherit credentials** - Specifies the Windows domain credential, if one is required. If checked, inherited. If blank, overrides the Windows domain credential set for the asset on the **Authentication** (page 40) tab of an asset node.

CIM monitor

The **CIM monitor** can query a CIM agent (CIMOM) configured on any hardware platform that supports CIM and has the agent and providers configured. Refer to your hardware manual for how to configure the CIMOM.

The monitor can query a CIM performance counter for a CIMOM (agent) and compare it to a value using a compare operation. If the compare operation evaluates to false the monitor fails the test. Supports most performance counters assets, such as hosts, datastores, memory, CPU, etc.

- System types: Linux/UNIX, VMware
- Category: Performance

Note: For an introduction to CIM monitoring see the **Kaseya Knowledge Base** (<https://helpdesk.kaseya.com/entries/35975757>).

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Connection settings

- **Use secure HTTP (SSL)** - Use SSL for encrypted traffic (default).

CIM monitor properties

- **Target Namespace** - Defaults to `root/cimv2`. For specific namespaces on your system, refer to your hardware manual. Another common namespace is `root/interop`.
- **Class** - Classes are enumerated, based on the namespace you have chosen so it can look very different between different systems.
- **Property** - The type of property you want to monitor. Properties are enumerated, based on the class you have chosen.
- **Instance** - If there are multiple instances for the chosen class, they are enumerated here.
- **Divisor** - The result is divided by this value. Optional. Defaults to 1.
- **Data type** - The unit of data sampled by the test. This makes it possible to group data from this type of monitor with other monitors such as CPU utilization in reports.

Threshold settings

- **Value type** - Type of value returned.
- **Compare operation** - Operation used to evaluate the returned result and the predefined compare value.
- **Compare value** - User defined compare value. Only numerical values are valid.

CIM account

If you have chosen Other/Unidentified as the asset type, you will have to choose an account here to authenticate against the CIMOM. *Ensure your CIM user has at least read permissions for the specified namespace.*

- **Inherit credentials** - If checked, inherits credentials from the asset. If blank, enter monitor-specific credentials.
- **Username/password** - Credential used to authenticate access for this monitor.
- **Port** - Defaults to 5989 (SSL). The default port for unencrypted traffic is 5988.

References and links

CIM (Common Information Model) is a standard defined and published by Distributed Management Task Force (DMTF). Other standards like Web-Based Enterprise Management (WBEM) defines the implementation of CIM, including protocols for discovering and accessing the implementations.

Windows Management Instrumentation (WMI) is an example of an implementation as well as Standards Based Linux Instrumentation Management (SBLIM). Others are Storage Management Initiative – Specification (SMI-S), Server Management Architecture for Server Hardware (SMASH) and Desktop and mobile Architecture for System Hardware (DASH).

- [http://en.wikipedia.org/wiki/Common_Information_Model_\(computing\)](http://en.wikipedia.org/wiki/Common_Information_Model_(computing))
- http://en.wikipedia.org/wiki/Windows_Management_Instrumentation
- <http://sourceforge.net/projects/sblim>
- http://en.wikipedia.org/wiki/Storage_Management_Initiative_-_Specification
- <http://dmf.org/standards/smash>
- <http://dmf.org/standards/dash>
- <http://h18006.www1.hp.com/storage/smis.html> - Lists HP hardware that supports SMI-S.

Citrix server monitor

The **Citrix server** monitor checks if a Citrix server is responding to connection attempts.

- System type: All
- Category: Network services

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Port number** - Port number of the Citrix service.

CPU utilization monitor

Monitors **CPU utilization** on an asset and triggers an alarm if above the specified threshold.

- System type: All but Other/Unidentified
- Category: Performance

On Windows assets, the methods for measuring CPU utilization is *WMI* or *Windows performance counters*.

- For WMI or Windows performance counters, a Windows user with permissions to read the registry on the monitored asset is required.
- When using Windows performance counters, the service “Remote Registry” must be enabled and started on the monitored asset.

On Unix assets, KNM connects to a monitored asset using SSH2, issuing commands specific to the selected operating system. Ensure the user used for UNIX assets can issue required commands, like *vmstat* or *mpstat*. If required, install the system tools for your system that include the *mpstat* utility to monitor specific CPUs or cores. Otherwise, only overall system load will be monitored.

Note: If you experience issues with this monitor type on Windows machines, try unchecking the **Use WMI** checkbox on the **Advanced tab** (page 50) of the asset node.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Max CPU load** - The maximum CPU utilization in percent.
- **CPU number** - The number of the CPU on the host. This value is usually automatically obtained from the relevant asset. To refresh the list, press the Rescan CPUs link.
- **Detailed error report** (Windows only) - If checked, includes the top 5 processes by CPU usage.
- **Inherit credentials** - Specifies the Windows domain credential, if one is required. If checked, inherited. If blank, overrides the Windows domain credential set for the asset on the **Authentication** (page 40) tab of an asset node.

Database server monitor

Database server monitors a database using ODBC. The test verifies that the ODBC data source can be opened and accessed. The monitor can also execute a SQL query and compare the result to a predefined value.

- System type: All
- Category: Database

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Basic tab

ODBC monitor properties

- **Datasource name** - Name of the ODBC data source to be used to connect to the database. The datasource:
 - Be configured on the system *hosting the gateway node of the target machine*.
 - Must be an ODBC DNS System type data source.
 - Be 32 bit data source.
 - ✓ On 32 bit gateway host systems, run `c:\Windows\System32\odbcad32.exe` to configure the data source.
 - ✓ On 64 bit gateway host systems, run `c:\Windows\SysWOW64\odbcad32.exe` to configure the data source.
- **SQL query** - Optional SQL query to perform.

ODBC account

- **Inherit credentials** - If checked, inherits credentials from the asset. If blank, enter monitor-specific credentials.

Note: For this monitor, uncheck this checkbox and enter monitor-specific credentials.

- **Username/password** - Credential used to authenticate access for this monitor.
- **Fail if no rows** - Check this option to make the monitor fail the test if the query returns no rows.
- **Data type** - `SQL query value` is the only option currently supported.

Threshold settings

- **Value type** - Type of value that the value queried from the database are compared with.
- **Compare operation** - Specify how the queried value and the compare value should relate to each other for a successful test.
- **Compare value** - Value to compare queried result with.

Datastore utilization

Datastore utilization monitors free space on a VMware datastore and automatically enumerates available datastores to monitor on the asset.

- System type: VMware
- Category: Performance

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Datastore name** - The name of the datastore to monitor. The name is automatically obtained from the asset when doing an asset inspection. To refresh the list, press the **Rescan services** link.
- **Free datastore space** - Minimum space free on datastore in the unit selected below.
- **Unit** - Select the unit to use in the test. The **Free datastore space** threshold is given in this unit.

DHCP query monitor

The **DHCP query** monitor verifies that a DHCP server is able to lease IP addresses to clients in the network. At least one address must be free for the test to succeed.

- System type: All

- Category: Directory services

Network Monitor uses the MAC address of the first installed network card on the **gateway host** to request an IP address from the DHCP server.

- The **Network Monitor** host cannot use DHCP for its own network interface if this monitor is used. If the gateway host machine used DHCP the result could be that **Network Monitor** might release the IP address allocated to the host.
- If the DHCP server is on a different network than your **Network Monitor** server, either deploy a gateway on that network or implement DHCP forwarding (UDP helper) on the network where **Network Monitor** is installed.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Directory property monitor

The **Directory property** monitor can test the file count, directory sizes, relative size changes and ages of files in a directory. The test can be limited in scope to files matched by a wildcard.

- System type: Windows
- Category: Others

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Share** - Name of share relative to the asset. *File specification is required.* Accepts wildcard formatting options. For example, `\temp*.?xt`. See below for additional formatting options.
- **Ok if no files** - If checked, the option makes the monitor pass the test if there are no matching files. The test passes without checking the subsequent tests.
- **Logon account** - To override the asset default account, select an account from the list.
- **Max files** - Enter the maximum file count in directory for test to pass. Leave blank to skip this test.
- **Min files** - Enter the minimum file count in directory for test to pass. Leave blank to skip this test.
- **Max age** - Enter the maximum file age of the oldest file in the directory in hours and minutes. For example, `HH:MM`. Leave blank to skip this test.
- **Max age newest** - Enter the maximum file age of the newest file in the directory. Leave blank to skip this test.
- **Rel. threshold** - The relative threshold test enables you to test for relative changes between the current test and the previous test. Select an option that will make the test fail if it evaluates to true.
- **Abs. threshold** - The absolute threshold test can be used to test the directory size against an absolute threshold in MB. The threshold, together with the operation, should evaluate to true for the test to pass.

Path field formatting variables

The following formatting variables can be included when specifying the path of a share. For example, the format

`\sharename*%[system.date_year]-%[system.date_month]-%[system.date_day_of_month].log` matches the filenames: 2013-01-15.log, 2013-02-10.log, 2013-03-06.log.

- `%[system.time_hour]` - Hour in 24-hour format (00 -23)
- `%[system.time_hour2]` - Hour in 12-hour format (01 -12)
- `%[system.time_minute]` - Minute as decimal number (00 -59)
- `%[system.time_second]` - Second as decimal number (00 – 59)

- `%[system.date_year]` - Year with century, as decimal number
- `%[system.date_year2]` - Year without century, as decimal number
- `%[system.date_month]` - Month as decimal number (01 – 12)
- `%[system.date_day_of_month]` - Day of month as decimal number (01 – 31)
- `%[system.date_day_of_year]` - Day of year as decimal number (001 – 366)
- `%[system.date_weekday]` - Weekday as decimal number (0 – 6; Sunday is 0)

Disk utilization monitor

Disk utilization monitors free space on a volume and automatically enumerates available volumes to monitor on the asset.

On Windows assets, the methods for measuring disk utilization is *WMI* or *Windows performance counters*.

- For WMI or Windows performance counters, a Windows user with permissions to read the registry on the monitored asset is required.
- When using Windows performance counters, the service “Remote Registry” must be enabled and started on the monitored asset.
- If a Windows share is monitored instead of a volume or a drive, then the Windows user associated with the asset will need network read access to the share name.

On Unix assets, KNM connects to a monitored asset using SSH2, issuing commands specific to the selected operating system. Ensure the user used for UNIX assets can issue required commands. `df` is the default command.

- System type: All but Other/Unidentified
- Category: Performance

Note: If you experience issues with this monitor type on Windows machines, try unchecking the **Use WMI** checkbox on the **Advanced tab** (page 50) of the asset node.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Use Windows share** - This option only displays for Windows system type assets.
 - If checked, the monitor uses the SMB/CIFS network protocol to obtain disk utilization. Doing so requires you to enter a share name, for example `C$`. Ensure that *File and printer sharing* is running on the asset when you enable this option. Enumeration of disks is not supported when this option is enabled.
 - If blank, the monitor uses the Windows performance registry to obtain disk utilization values.
- **Volume name** - The name of the disk to monitor. The name is automatically obtained from the asset when doing an asset inspection. To refresh the list, press the **Rescan disk volumes** link. If the **Use Windows share** option is selected, a text field replaces the list.
- **Free disk space** - Minimum space free on volume in the unit selected below.
- **Unit** - Select the unit to use in the test. The **Free disk space** threshold is given in this unit.
- **Inherit credentials** - Specifies the Windows domain credential, if one is required. If checked, inherited. If blank, overrides the Windows domain credential set for the asset on the **Authentication** (page 40) tab of an asset node.

DNS lookup monitor

The **DNS lookup** monitor connects to a *DNS server running on the asset* and tries to translate the

Monitor Reference

specified address into another address format. The entered address can be in number form (255.255.255.255) or in name form (www.kaseya.com).

- System type: All
- Category: Directory services

To test reverse DNS lookups, ensure the DNS server used by your KNM host or gateway supports that feature. Test by using the `ping -a` command.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Name** - The address to use for translation test. To test more than one address at the time, separate the addresses with a semi colon in this field.
- **All fail** - Selecting this option indicates that all the addresses must have failed lookups for the agent to go into a failed state.

Environment monitor

The **Environment monitor** is capable of monitoring hardware for environmental monitoring. Various hardware from many different manufacturers are supported, including AKCP, IT Watchdogs, AVTECH, Sensatronics and others.

- System type: All
- Category: Environment

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor configuration

When creating a new **Environment monitor**, the user first has to select the manufacturer and model of the asset. Once the model has been selected, **Network Monitor** automatically fetches the asset configuration.

Monitor specific properties

- **Temperature unit** - The desired temperature unit for specifying the thresholds. This also affects the visual presentation of real time charts for this monitor.
- **Polling method** - This setting chooses the polling method for querying data from the asset. Normally, it does not need to be changed.
- **Port** - Port number for polling data from the asset. Normally this is automatically set by **Network Monitor**.

After these generic settings, the settings for each individual sensor on the asset can be specified. They are logically organized into groups corresponding to how the asset itself has been configured earlier. Each sensor must be enabled, by checking the enabled box for each sensor. Thresholds are not required and can be left empty if the sensor is only used to collect statistics.

Event log monitor

The **Event log** monitor reads the event log and searches for messages that matches the monitor parameters. Only event log entries created after the previous test is included in the current test.

- System type: Windows
- Category: Log

If **Use WMI** is checked on the **Advanced** tab of the parent asset, WMI is used for this monitor. To monitor

event logs under **Applications and Services Logs**, uncheck WMI since WMI is limited when it comes to the log files it can read.

If **Use WMI** is not checked, then two different APIs are used for reading the event logs, depending on Windows version. The API used for Windows Vista/Server 2008 differs from the one used for Windows Server 2003 or Windows XP.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Event Source string** - (Optional) The source of the event.
- **Computer** - (Optional) The computer that registered the log entry.
- **Event ID** - Event ID number to trigger an alarm on. Separate multiple numbers with a comma. To include all event IDs, leave the field blank.
- **Event ID filter** - Event ID number of events to filter out. Separate multiple numbers with a comma.
- **Filter including** - If one or more strings exist in the event record message text, the record is included in the test, assuming all other criteria are met.
- **Filter excluding** - If one or more strings exist in the event record message text, the record is **not** included in the test, assuming all other criteria are met.
- **Event type** - The type of event to search for. If the alternative **all** is selected, all types of events are considered for the test.
- **Include message** - If checked, the message text is include in the error report.
- **Event Log** - Displays a predefined list of log names. Select a log to monitor.
- **Alt. Event Log** - Alternative log name. Enter the name of the log to search. This setting overrides the **Event Log** setting.
- **Logon account** - Overrides the default account selected for an asset.

Exchange server monitor

The **Exchange server** monitor type can monitor I/O activity and mail queue sizes of an Microsoft Exchange 2007 server.

- System type: Windows
- Category: Web and email

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Performance monitoring

- **Disk read bytes/s** - Maximum rate at which bytes are transferred from the disk during read operations.
- **Disk write bytes/s** - Maximum rate at which bytes are transferred to the disk during write operations.

Queue monitoring

Leave these fields blank to not perform these tests.

- **Send queue size (mailbox)** - Maximum allowed number of messages in the **mailbox** send queue.
- **Receive queue size (mailbox)** - Maximum allowed number of messages in the **mailbox** receive queue.
- **Send queue size (public)** - Maximum allowed number of messages in the **public** send queue.
- **Receive queue size (public)** - Maximum allowed number of messages in the **public** receive queue.
- **SMTP categorizer queue length** - Maximum number of allowed messages awaiting processing, such as recipient validation, sorting of local or remote delivery and distribution list recipient expansion.

Large number of waiting messages in this queue can indicate performance problems in other Exchange components or Active Directory.

- **Message queued for delivery** - Maximum number of messages queued for delivery.

File change monitor

The **File change** monitor checks a file for changes in size or modification date.

- System type: All but Other/Unidentified
- Category: Others

Ensure the user credential used has at least read permission for the file being monitored.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Windows specific properties

- **File path** - The absolute path of the file using UNC notation, including the name of the host. This allows you to target a file on a different asset than the asset the monitor is set up on. For example, `\\myhost\c$\test.txt`

Unix specific properties

- **File path** - Path of a file relative to the host. For example, `/home/robert/test.txt`

Monitor specific properties

- **Date** - If checked, triggers an alarm if the file is modified since the last test.
- **Larger size** - If checked, triggers an alarm if the file grows in size since the last test.
- **Smaller size** - If checked, triggers an alarm if the file shrinks in size since the last test.
- **Not change** - If checked, triggers an alarm if the file size or date not have changed since the last test.

Path field formatting flags

The following formatting variables can be included when specifying a path.

- `%[system.time_hour]` - Hour in 24-hour format (00 -23)
- `%[system.time_hour2]` - Hour in 12-hour format (01 -12)
- `%[system.time_minute]` - Minute as decimal number (00 -59)
- `%[system.time_second]` - Second as decimal number (00 – 59)
- `%[system.date_year]` - Year with century, as decimal number
- `%[system.date_year2]` - Year without century, as decimal number
- `%[system.date_month]` - Month as decimal number (01 – 12)
- `%[system.date_day_of_month]` - Day of month as decimal number (01 – 31)
- `%[system.date_day_of_year]` - Day of year as decimal number (001 – 366)
- `%[system.date_weekday]` - Weekday as decimal number (0 – 6; Sunday is 0)

FTP server monitor

The **FTP server** monitor checks if an FTP server accepts new connections.

- System type: All
- Category: Network services

The FTP server monitor can monitor service availability, but logging on also works. Enter an FTP

account for the asset or monitor. If you want to check that anonymous logons work, use the standard “anonymous” account. Most FTP servers will accept any string or your email address as a password.

Note: Only monitor specific settings are documented here. See [Standard monitor settings](#) (page 63).

Monitor specific properties

- **Logon account** - Account used to logon to the FTP server. If no logon account is selected, a simple port check is performed.
- **Port number** - The port number the FTP server is listening on.

IMAP4 server monitor

The **IMAP4 server** monitor tests if it can logon and select a mailbox. The test verifies that the authentication and storage part of the IMAP4 server is working. If no username or password is provided a simple connection test is preformed.

- System type: All
- Category: Web and mai

Add an IMAP4 credential on either the asset or the monitor to confirm that logon works.

Note: Only monitor specific settings are documented here. See [Standard monitor settings](#) (page 63).

Monitor specific properties

- **Username/Password** - Optional credentials to logon and check mail box.
- **Inbox name** - Name of the inbox to check if credentials is given.
- **Port number** - The port number the services listening on.

JVM performance monitor

The **JVM performance** monitor uses JMX to query Java bean objects and their data. The monitor compares Java bean values with a compare value using a compare operation. If the compare operation evaluates to `false` the monitor fails the test. Optionally two performance counters can be queried and combined before being compared with the compare value.

- System type: Windows, Linux/UNIX, Other/Unidentified
- Category: Performance

Monitoring Average CPU Usage

All bean objects and their data use the **Data type** `Java VM performance data`, except for the following combination of settings:

- **Object** - `java.lang.type=OperatingSystem`
- **Counter** - `ProcessCpuTime`
- **Data type** - `CPU utilization`

In this case an average CPU usage—similar to the CPU usage that is displayed in JConsole—is calculated by fetching two samples of the `ProcessCpuTime` counter with a known time delay between them. Optionally displays data in percent.

Configuration

- The Java server must have JMX activated and accessible over the LAN.

- The **Network Monitor** gateway—including the local gateway on the **Network Monitor** server computer—must have the Oracle Java JDK (or at least JRE) for 32-bit applications installed. If any 64-bit Java is installed, remove it entirely, or at least clear it completely from the PATH environment variable. The Java installer can be downloaded from:
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>
(<http://www.oracle.com/technetwork/java/javase/downloads/index.html>).
- If the gateway is running x64 Windows and a 32-bit version of Java JRE (or JDK) has been installed, go to the Control Panel > System > Advanced System Settings and add the following string to the PATH environment variable for the system user.
`;C:\Program Files (x86)\Java\jre7\bin;C:\Program Files (x86)\Java\jre7\bin\client`
- Verify that the %JAVA_HOME%\bin\client folder (where %JAVA_HOME% represents the Java installation folder) contains the important file JVM.DLL, that is the **Network Monitor** interface to JNI and ultimately the Java VM
- Reboot the gateway machine to make sure that the setting is reflected on all running applications and services.
- If the JDK is installed on the gateway, you should verify that the connection to the JMX server is available by executing the JConsole.exe (32-bit) application in the JDK bin folder
- Verify that the gateway, including the KNM local_gateway subfolder, have their own copy of the JAR file jmx_connector.jar, that is found in the KNM installation folder.
- When adding a **JVM performance** monitor, ensure that the JVM account, if any, and port setting is set to the correct values. Then select the **ReScan** link. The **Object**, **Counter**, and **Instance** listboxes will be filled with any available beans and their datafields.

Monitor specific properties

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

- **Object/Counter/Instance** - Name of the primary performance bean to test. These values can be enumerated by using the enumeration function. The instance field is intentionally left blank for some counter types. Click the **Rescan** link to refresh these values
- **Object/Counter/Instance** - Optional. Secondary performance bean. These values can be enumerated by using the enumeration function. The instance field is intentionally left blank for some counter types.
- **Combine operation** - Optional operation used when querying two counters. They can be combined into a final result by using the add, subtract, divide or multiply operation.
- **Divisor** - A value that the retrieved value is divided with before the comparison.
- **Data type** - The unit of data sampled by the test. This makes it possible to group data with other monitors using the same type in reports.
- **Value type** - Type of value that is compared with the retrieved value.
- **Compare Operation** - Operation to use when comparing.
- **Compare value** - Value to compare with the resulting value from the calculation.
- **Inherit credentials** - Specifies the JVM credential, if one is required. If checked, credentials are inherited. If blank, overrides the JVM credential set for the asset on the **Authentication** (page 40) tab of an asset node.
- **Port** - The port number of the JVM service.

LDAP query monitor

The **LDAP query** monitor checks if a LDAP server is responding to directory lookup requests.

- System type: All

- Category: Directory services

Add an LDAP user credential on either the asset or monitor.

Note: Only monitor specific settings are documented here. See [Standard monitor settings](#) (page 63).

Monitor specific properties

- **Username/Password** - Credentials used for lookup. To override the asset's default account, select an account from the list.
- **Domain name** - Name of the domain or workgroup the username is associated with.
- **Port** - Port number that the LDAP server listens to.

Log file monitor

The **Log file** monitor can read a text file and check for *appended lines containing one of the specified strings*. The monitor generates an alarm if the specified search criteria are met. The monitor uses SMB for connecting to an asset. This means that the only credentials configurable are Windows accounts. You will need to set a Windows account even if the target operating system is non-Windows using Samba.

- System type: All
- Category: Log

Note: Only monitor specific settings are documented here. See [Standard monitor settings](#) (page 63).

Monitor specific properties

- **Path** - Absolute path of the the file, including the name of the host. For example, `\\myhost\C$\test.txt`.
- **Search string** - String to search for. Multiple strings can be searched. Separate each sub string with a comma. If multiple substrings are entered, the test performs a logical OR operation on the string.
- **Alert if no change** - If checked, the test fails if the file has not changed since last the test. If checked, search string tests are not performed.
- **Restart** - If checked, the monitor restarts from the top of the log file for each test.
- **Inherit credentials** - If checked, inherits credentials from the asset. If blank, enter monitor-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this monitor.

Path field formatting flags

The following formatting variables can be included when specifying a path.

- `%[system.time_hour]` - Hour in 24-hour format (00 -23)
- `%[system.time_hour2]` - Hour in 12-hour format (01 -12)
- `%[system.time_minute]` - Minute as decimal number (00 -59)
- `%[system.time_second]` - Second as decimal number (00 – 59)
- `%[system.date_year]` - Year with century, as decimal number
- `%[system.date_year2]` - Year without century, as decimal number
- `%[system.date_month]` - Month as decimal number (01 – 12)
- `%[system.date_day_of_month]` - Day of month as decimal number (01 – 31)
- `%[system.date_day_of_year]` - Day of year as decimal number (001 – 366)
- `%[system.date_weekday]` - Weekday as decimal number (0 – 6; Sunday is 0)

Lua script monitor

The **Lua script** monitor executes a **Lua** (page 186) script loaded from the `KNM\script` folder of the KNM host machine.

- System type: All
- Category: Script

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Script** - Select the script from the list. The list is based on the scripts found in the `\script` folder of the KNM host machine.
- **Argument** - Arguments to be passed to the script.
- **Logon account** - Optional credentials for Windows authentication, if the script requires authentication. To override the asset default account, select an account from the list.
- **Do not logon using account** - Check this option if you want to pass the authentication parameters to the Lua script and bypass the default authentication performed by **Network Monitor** before the test starts.

Mail server QOS monitor

The **Mail server QOS** monitor can test the ability of a mail server to send and receive mail. Statistics about round trip time, time to send and login time are stored.

- System type: All
- Category: Web and Email

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Email round trip timeout** - The maximum time in seconds the monitor waits for email to arrive at the POP3 server.
- **SMTP server** - Address of SMTP server to send the test mail through.
- **SMTP port** - Port number of the SMTP server
- **SMTP account** - Optional account to use to authenticate with the SMTP server. Selecting an account with an SMTP server that does not require authentication causes the test to fail. Leave blank if unsure.
- **From address** - Email address used as the From field in outgoing email.
- **Custom EHLO** - Custom EHLO string that is used to greet the remote email server. Must be specified if this monitor is assigned to a gateway.
- **POP3 server** - Is always the address of the asset.
- **POP3 port** - Port number of the POP3 server.
- **Email address** - Email address to be used in test. Note that the email address must exist on the POP3 server and must be accepted by the SMTP server for delivery. The email account should be exclusive to **Network Monitor** since the test erases all emails after each test.
- **POP3 account** - Credentials used to logon to the POP3 server.

Memory utilization monitor

Memory utilization monitor tests free memory and triggers an alarm if it is below the given threshold or if the asset is unavailable.

- System type: All but Other/Unidentified
- Category: Performance

On Windows assets, the methods for measuring memory utilization is *WMI* or *Windows performance counters*.

- For WMI or Windows performance counters, a Windows user with permissions to read the registry on the monitored asset is required.
- When using Windows performance counters, the service “Remote Registry” must be enabled and started on the monitored asset.

On Unix assets, KNM connects to a monitored asset using SSH2, issuing commands specific to the selected operating system. Ensure the user used for UNIX assets can issue required commands. `free -m` is the default command. It may require software installation on your asset.

Note: If you experience issues with this monitor type on Windows machines, try unchecking the **Use WMI** checkbox on the **Advanced tab** (page 50) of the asset node.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Free memory** - The amount of free memory required. If the free memory goes below this value the monitor fails the test.
- **Unit** - The unit of free memory tested. The free memory threshold is specified in this unit.
- **Process report** - If checked, process memory consumption is included in the alarm message.
- **Task Manager approx** - If checked, calculates memory utilization using a method that approximates Windows Task Manager values. If blank, uses a legacy **Network Monitor** method.
- **Inherit credentials** - Specifies the Windows domain credential, if one is required. If checked, inherited. If blank, overrides the Windows domain credential set for the asset on the **Authentication** (page 40) tab of an asset node.

MySQL monitor

This **MySQL** monitor type is capable of monitoring several key aspects of an MySQL database.

- System type: All
- Category: Database

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Prerequisites

The **MySQL Connector/C** (<http://www.mysql.com/downloads/connector/c>) or **MySQL Workbench** (<http://dev.mysql.com/downloads/tools/workbench/5.2.html>) packages must be installed on the **Network Monitor** server or gateway. Download and install the 32-bit client, even if your server is 64-bit. This is because **Network Monitor** is a 32-bit application and requires 32-bit drivers.

After installation ensure the file path to `libMySQL.dll` is in the Windows system path. This is normally taken care of during installation of the administrator package, and might require a reboot of the server. The **Network Monitor** `nmservice.exe` service must be restarted for the change to take effect. If **Network Monitor** cannot access this DLL file, the MySQL monitor fails with an error message specifying that it cannot find the `libMySQL.dll` file.

Monitor Reference

If your MySQL server normally only responds to local queries, ie. your application is on the same server as the database, you may need to follow these simple steps to allow access for KNM to monitor your MySQL database.

- Your MySQL server will need to respond to requests from a remote host. By default, the bind address is 127.0.0.1 so you need to change "bind-address" in your `/etc/mysql/my.cnf` to the correct IP address of your server, or comment out the row with # before the `bind_address` line for the server to listen on all IP addresses of your server.
- By default, your client may not be allowed to connect to your database. To allow the client to connect to the database, follow these steps:
 1. SSH to your MySQL server
 2. `mysql -u root -p`
Enter password
 3. Run the following query:

```
use <database name>
GRANT ALL ON *.* to root@'<ip address of your KNM host/gateway>' IDENTIFIED BY
'<your root password>';
FLUSH PRIVILEGES;
```

Monitor specific properties

These fields are required to connect to the database to perform configured tests.

- **Logon account** - The logon account contains the credentials to use when authenticating with the MySQL database.
- **Port** - Port number which the database server listens to.
- **Database name** - Name of database to connect to.

Performance monitoring options

Leave these fields blank to not perform their tests.

- **Max thread count** - A numeric value that represents the maximum number of running threads, if the number of running threads exceeds this value the monitor fails the test.
- **Max replication latency** - A value in seconds that is the maximum difference in time between master and slave, if this time is exceeded the monitor fails the test.
- **Max slow queries** - A slow query is defined as a query that has been running longer than the average time and exceeded the `long_query_value` time defined in the database configuration. Enter a numeric threshold value to make the test fail if the number of slow queries exceeds this value.
- **Max open tables** - A numeric value that represents the maximum number of allowed open tables.
- **Queries per second average** - A numeric value that represents the maximum number of running queries per seconds allowed.
- **Max users** - Maximum number of users allowed to logon at the same time.

SQL query option

An optional SQL statement can be executed and its output compared to a predefined value using a compare operation.

- **SQL query** - Optional SQL query to perform.
- **No rows fail** - Check this option to make the monitor fail the test if the query returns no rows.
- **Compare value** - Value to compare query result with.
- **Value type** - Type of value that is compared with the retrieved from the database.
- **Operation** - Operation to evaluate the returned query result and the compare value to determine if the test succeeded or failed.

NNTP server monitor

The **NNTP server** monitor connects and checks the status of a NNTP (Network News Transport Protocol) server.

- System type: All
- Category: Network services

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Port number** - The port number the NNTP server is configured to use.

Oracle monitor

This **Oracle monitor** type is capable of monitoring several key aspects of an Oracle database. The monitor uses the native Oracle interface and does not require an ODBC driver installed on the **Network Monitor** host machine.

- System type: All
- Category: Databases

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Prerequisites

Install the **Oracle database instant client**

(<http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html>) on the **Network Monitor** server or gateway. Download and install the 32-bit client, even if your server is 64-bit. This is because **Network Monitor** is a 32-bit application and requires 32-bit drivers.

After installation ensure that the folder where you installed the package is in the Windows system path. This might require a reboot of the server. After altering the system path, restart the **Network Monitor** service for the change to take effect. If **Network Monitor** cannot access the DLL files it requires, the Oracle monitor fails with an error message specifying that it cannot find the DLL files.

Oracle account

These fields are required to connect to the database to perform configured tests.

- **Inherit credentials** - If checked, inherits credentials from the asset. If blank, enter monitor-specific credentials.
- **Username/password** - Credential used to authenticate access for this monitor.
- **Service name** - This is the name of the service defined in the `tnsnames.ora` file. **Network Monitor** uses this information to connect to the Oracle database.
- **Port** - The port number the Oracle database server listens to.

Performance monitoring options

- **Max open cursors** - A numeric value that represents the maximum number of simultaneously opened cursors. If the number of open cursors exceeds this value the monitor fails the test. Leave the field blank to not perform this test.
- **Long op. threshold** - A value in seconds that is the maximum time an operation can execute. If this time is exceeded, the monitor fails the test. Leave the field blank to not perform this test.
- **Buffer cache hit ratio** - The buffer cache hit ratio indicates the percent of total number of requests that have been served without accessing the disk. A higher value translates into better database

performance. Set this value to the lowest acceptable value. If the ratio falls below this value the monitor fails the test. Leave the field blank to not perform this test.

- **Failed logons** - A numeric value that represents the maximum allowed number of failed logons during a day. To test this value, auditing must be enabled. Leave the field blank to not perform this test.

Tablespace monitoring options

A table space is associated with physical files stored on disk, each database can be associated with one or more table spaces for storages of tables and indexes. By monitoring table space usage, you can be warned before the remaining free space in a table space passes below a threshold.

- **Tablespace usage** (any) - A threshold value that sets the maximum percent usage of a table space allowed. This field applies to all table spaces in the database. Subsequent fields can be used to configure exceptions for this rule, for up to five other table spaces. Leave the field blank to not perform this test.
- **Tablespace usage** (1-5) - A threshold value for the maximum usage allowed for a specific table space. These fields override the global table space threshold. Leave the field blank to not perform this test.

SQL query option

An optional SQL statement can be executed and its output compared to a predefined value using a compare operation.

- **SQL query** - Optional SQL query to perform.
- **Fail if no rows** - Check this option to make the monitor fail the test if the query returns no rows.
- **SYSDBA privilege** - If checked, elevates the credential to SYSDBA.
- **Value type** - Type of value that is compared with the retrieved value from the database.
- **Compare operation** - Operation to evaluate the returned query result and the compare value to determine if the test succeeded or failed.
- **Compare value** - Value to compare the query result with.

Ping monitor

Ping monitor uses the ICMP protocol to verify that the asset responds to ping packets within a predefined time. The monitor can also calculate packet loss and round trip time during the test. The monitor only triggers on packet loss level if the round trip time is within the specified range.

Note: The ping protocol is one of the protocols with lowest priority in a network and some hosts do not respond to ping packets by default.

- System type: All
- Category: Network services

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Timeout** - Largest round trip time in milliseconds the monitor waits for the ping packet to return from the host.
- **Packet loss** - Max packets lost when transmitted to the host. Specified in percent of total sent packages.
- **Packets to send** - The number of packets to send each test. A higher value yields a more exact packet loss and round trip time value.
- **Include trace** - Select option to include a trace route log in alarm message.

- **Max hops** - Max number of trace route hops that are performed while in Alarm state. Defaults to 255.
- **Alternative IP** - Secondary IP to test. The monitor can ping an alternative IP number in the same test.
- **Package size** - Total size of the data sent with the packet. Excludes the IP and ICMP header size of 28 bytes. For example, to test an MTU of 1500 enter 1472 here.
- **Don't fragment** - Sets the 'do not fragment' option in the outgoing ping packets.

POP3 server monitor

The **POP3 server** monitor connects to a POP3 mail server and verifies that it can logon to the server and check for mail, without affecting the status of the mailbox. The purpose is to verify that the POP3 authentication and the storage system of the POP3 server is working. If no username or password is provided a simple connection test is performed.

- System type: All
- Category: Web and email

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Username/password** - Optional. A POP3 account username and password
- **Port number** - The port number the POP3 server is configured to use.

Process status monitor

The **Process status** monitor can verify that a process is running on an asset.

- System type: All but Other/Unidentified
- Category: Performance

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Process name** - Name of the process to monitor.
- **Unlisted process** - Name of process to monitor if not listed. Typically a service is not listed if it is not started yet.
- **Invert function** - Check option to make the monitor fail the test if the process is running.
- **Logon account** - To override the asset default account select an account from the list.

Radius monitor

The **Radius server** monitor tests the performance of Radius servers. Radius is a network protocol that provides authentication, access and accounting for computers that want to connect to a network. Radius is often used to provide access to wireless networks. All tests are performed using SNMP get requests. Consult your Radius server documentation to find out if your Radius server responds to SNMP requests by default or if you have to configure this feature.

- The KNM host/gateway has to be setup as a Radius client with the Radius server, using a shared secret.
- For comparison options, the Radius server also has to have a working SNMP agent installed.

Note: The community name, SNMP version, and port used by **Network Monitor** to connect to an SNMP asset is set on the **Authentication** (page 40) tab of an asset node. The asset node may inherit this setting from a parent node. See the **Installation Checklist** (page 9).

- System type: All
- Category: Network services

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

These fields are required to connect to the Radius server to perform configured tests.

- **Secret** - Pre-shared secret word used to encrypt all passwords sent to Radius server for authentication.
- **Logon account** - The logon account contains the credentials to use when authenticating with the Radius server.

Performance monitoring options

Each test is performed in the scope of a time span. The time span is denoted in seconds.

- **Max invalid auth requests** - The maximum allowed number of access request packets received from an unknown address during the time span defined by the field below. The test fails if the number exceeds this value. Leave the field blank to not perform this test.
- **Max accounting requests** - The number of accounting request packets received from an unknown address during the time span defined by the field below. The test fails if the number exceeds this value. Leave the field blank to not perform this test.
- **Max total access rejects** - The maximum number of access rejected packets sent during the time span defined by the field below. Leave the field blank to not perform this test.

Comparison options

In addition to the above tests a customized SNMP get request can be made. The result of the request can be compared to a predefined value using a compare operation.

- **Radius compare OID** - An OID relative to the base Radius OID (.1.2.6.1.2.1.67 or .iso.org.dod.internet.mgmt.mib-2.radiusMIB) that can be requested for each test and compared with a predefined compare value. Leave the field blank to not perform this test.
- **Compare value** - Value to compare the query result with.
- **Value type** - Type of value that is compared with the retrieved value from the database.
- **Operation** - Operation to evaluate the returned query result and the compare value to determine if the test succeeded or failed.

Salesforce query monitor

Salesforce query server monitors a Salesforce database. The Salesforce monitor executes an SQL query and compares the result to a predefined value.

- System type: Windows, Linux/UNIX, Other/Unidentified
- Category: Database

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Basic tab

Salesforce monitor properties

- **SQL query** - SQL query to perform.

Salesforce account

- **Inherit credentials** - If checked, inherits credentials from the asset. If blank, enter monitor-specific credentials.

Note: For this monitor, uncheck this checkbox and enter monitor-specific credentials.

- **Username/password** - Credential used to authenticate access for this monitor.
- **Fail if no rows** - Check this option to make the monitor fail the test if the query returns no rows.
- **Data type** - `SQL query value` is the only option currently supported.

Threshold settings

- **Value type** - Type of value that the value queried from the Salesforce database is compared with.
- **Compare operation** - Specify how the queried value and the compare value should relate to each other for a successful test.
- **Compare value** - Value to compare the queried value with.
- **Time period** - If blank, the **Compare value** is compared with the queried value. If a **Time Period** value in seconds is entered, the **Compare value** is compared with the difference in queried values between two successive time periods.

SMTP server monitor

The **SMTP server** monitor checks that it can connect to an SMTP server and that the SMTP server returns a valid return code.

- System type: All
- Category: Web and email

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Port** - The port number the SMTP server is configured to use.

SNMP monitor

The **SNMP** monitor is a dynamic tool for querying multiple asset identifiers (OID) from an remote SNMP agent and perform calculations on the returned values.

Note: The community name, SNMP version, and port used by **Network Monitor** to connect to an SNMP asset is set on the **Authentication** (page 40) tab of an asset node. The asset node may inherit this setting from a parent node. See the **Installation Checklist** (page 9).

- System type: All
- Category: SNMP

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific settings

- **OID1, 2, 3, ...** - Specifies a list of numbered OIDs.

- Click **Add OID** and **Remove OID** to add or remove OIDs to this monitor.
- You can specify either a named OID or a OID in number format. If you specify a named OID, **Network Monitor** tries to resolve it to its number format automatically when the field loses focus. **Network Monitor** uses the currently compiled MIBs to attempt to find the number format of the OID.
- The [...] button next to the OID field display a MIB Browser dialog that can be used to select asset identifiers from the remote SNMP agent.
- When the MIB browser displays an OID number with a @string it means you can use this string as part of the OID. For example the OID .1.3.6.1.2.1.2.2.1.16@Intel(R) PRO/1000 MT Network Connection can be entered in the OID field instead of identifying the index number of the network connection.
- **Calculation** - A calculation using the values queried from the asset identifiers. The example in the image above calculates the network utilization from an interface.
- **Result translation** - Translates the result into a readable string. This option is only available when the value type in the comparison is set to string. The result translation feature can be used to translate a non-descriptive OID value into a readable string. The OID value retrieved can still be a numeric value, but is treated as a string.
 - Example 1*
Unknown(1), Alarm(2), Failed(3), Ok(4)
 - Example 2*
Unknown=1,Alarm=2,Failed=3,OK=4

The values 1, 2, 3 and 4 are translated to Unknown, Alarm, Failed and OK. Both examples above are valid notations. The final translated string is the string used in the comparison operation.
- **Valid values / min / max** - Enables the monitor to filter out all values below and above the given threshold.
- **Data type** - The unit of data sampled by the test. This makes it possible to group data with other monitors using the same type in reports.
- **Counter mode**
 - **Delta** - Calculate the difference between the last test and the current test. Recommended when the value returned grows continuously.
 - **Absolute value** - Use the absolute value returned.
- **Value type** - Type of value that is compared with the retrieved value.
- **Compare Operation** - Operation to use when comparing.
- **Compare value** - Value to compare with the resulting value from the calculation.

SNMP trap monitor

The **SNMP trap** monitor receives trap messages from SNMP monitors on remote hosts. The monitor only receives messages that originate from the asset's IP address. The first step of the filtering is done with the specified enterprise OIDs. Further inspection of the trap is done with the variable binding filter, which can include several rules. The rules are either evaluated all together (AND operation) or one by one (OR operation). The resulting trap triggers a failed test. The monitor can filter out standard generic SNMP v1 and v2c trap types.

Each OID field can be populated by selecting it from the **MIB browser** (page 93). The MIB browser is opened by pressing the button to the right of the OID field.

See the

- System type: All
- Category: SNMP

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Basic tab

- **OID include filter** - Enter one or more OIDs, separated by a comma. The monitor triggers an alarm for the specified enterprise OID.
 - You can specify either a named OID or a OID in number format. If you specify a named OID, **Network Monitor** tries to resolve it to its number format automatically when the field loses focus. **Network Monitor** uses the currently compiled MIBs to attempt to find the number format of the OID.
 - The [...] button next to the OID field display a MIB Browser dialog that can be used to select asset identifiers from the remote SNMP agent.
 - When the MIB browser displays an OID number with a @string it means you can use this string as part of the OID. For example the OID .1.3.6.1.2.1.2.2.1.16@Intel(R) PRO/1000 MT Network Connection can be entered in the OID field instead of identifying the index number of the network connection.
- **OID exclude filter** - Enter one or more OIDs, separated by a comma. This monitors ignores traps from the specified enterprise OID.
- **Community** - SNMP community to use.

Variable Binding filter tab

- **Include all variables** - If checked, include all variable bindings from the trap in the alarm message. If unchecked only *matched* variable bindings will be included.
- **Match option** - If **All**, all variable bindings must match. If **At least one**, only one variable binding must match.
- **OID/Value pairs** - Filter rule to evaluate trap data. Performs a compare operation on a dynamic number of OIDs in the trap. The filter rules can be evaluated together or one by one. The result of the operation must be evaluate to **true** to be considered a matching trap.

Trap type filter tab

- **Trap type filter** - Trap types to be included in the test.

Coldstart
 Warmstart
 Link down
 Link up
 Authentication failed
 EGP
 Enterprise

SQL Server monitor

The **SQL Server** monitor type is capable of monitoring several key aspects of a Microsoft SQL Server database. The monitor uses the native SQL Server interface and does not require an ODBC driver installed on the **Network Monitor** host machine.

- System type: Windows
- Category: Database

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Basic tab

Basic monitor settings

These fields are required to connect to the database to perform configured tests.

- **Logon account** - The logon account contains the credentials to use when authenticating with the SQL Server database.
- **Instance name** - The SQL server instance name to use.
- **Database name** - Name of database to connect to.
- **Port** - The port number the database server listens to. Defaults to port 1433.
- **Protocol type** - Default protocol, TCP/IP, Named Pipes, Shared Memory
- **Data type** - SQL query value. This is the only option currently supported.

Performance monitoring

Note: Leave these fields blank to not perform these tests.

- **Max users** - Maximum number of allowed users logged on at the same time.
- **Buffer cache hit ratio** - The buffer cache hit ratio indicates the percent of the total number of requests that have been served without accessing the disk. A higher value translates into better database performance. Set this value to the lowest acceptable value. If the ratio falls below this value the monitor fails the test.
- **Max replication latency** - A value in seconds that is the maximum difference in time between master and slave. If this time is exceeded the monitor fails the test.
- **SQL compilations** - A numeric value that is the maximum number of SQL compilations that can occur per second. If this value is exceeded the monitor fails the test. A high value of SQL compilations per second can result in high CPU usage.

Tablespace monitoring options

Note: Leave these fields blank to not perform these tests.

Table space is associated with physical files stored on disk. Each database can be associated with one or more table spaces, for the storage of tables and indexes. Monitoring tablespace usage enables you to be warned before the remaining free space in a table space passes below a threshold.

- **Database disk usage** - A threshold value that sets the maximum allowed usage of a table space in percent. This field applies to all table spaces in the database, subsequent fields can be used to configure exceptions from this rule for up to five other table spaces.
- **Tablespace usage / % max usage (1-5)** - A threshold value for the maximum allowed usage for a specific table space. These fields override the global table space threshold.

Threshold settings

An optional SQL statement can be executed and its output compared to a predefined value using a compare operation.

- **SQL query** - Optional SQL query to perform.
- **Fail if no rows** - Check this option to make the monitor fail the test if the query returns no rows.
- **Value type** - Type of value that is compared with the retrieved value from the database.
- **Compare operation** - Operation to evaluate the returned query result and the compare value, to determine if the test succeeded or failed.
- **Compare value** - Value to compare query result with.

SQL server account

- **Inherit credentials** - If checked, inherits credentials from the asset. If blank, enter monitor-specific credentials.
- **Username/password** - Credential used to authenticate access for this monitor.

SSH2 script monitor

The **SSH2 script** monitor can execute a command or script on a SSH2 host and compare the returned value with a predefined string using a compare type. If the compare operation evaluates to **false** the monitor generates an alarm.

- System type: All
- Category: Script

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Command** - A command to execute on the host. The command should return a value after execution.
- **Logon account** - To override the asset default account, select an account from the list.
- **Data type** - The unit of data returned by the script. This makes it possible to group data from this type of monitor with other monitors such as **CPU utilization** in reports.
- **Port** - Port number.
- **Compare value** - Value to compare the returned result with.
- **Value type** - Type of value returned.
- **Operation** - Compare operation to use when evaluating the result. If the returned value compared with the compare value evaluates to **false** the monitor fails the test.

SSH2 server monitor

The **SSH2 server** monitor verifies that a SSH2 server is responding to user logon attempts. This monitor does not support the older SSH1.x protocol. If credentials are omitted, the monitor performs a connection test only.

- System type: All
- Category: Network services

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Logon account** - To override the asset default account, select an account from the list.
- **Port** - Port number that server listens to. Defaults to **22**.

Swap file utilization monitor

Swap file utilization monitors swap space utilization on the asset.

- System type: All but Other/Unidentified
- Category: Performance

On Windows assets, the methods for swap file utilization is *WMI* or *Windows performance counters*.

- For WMI or Windows performance counters, a Windows user with permissions to read the registry on the monitored asset is required.
- When using Windows performance counters, the service “Remote Registry” must be enabled and started on the monitored asset.

On Unix assets, KNM connects to a monitored asset using SSH2, issuing commands specific to the selected operating system. Ensure the user used for UNIX assets can issue required commands. `free -m` is the default command. It may require software installation on your asset.

Note: If you experience issues with this monitor type on Windows machines, try unchecking the **Use WMI** checkbox on the **Advanced tab** (page 50) of the asset node.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Max swap utilization** - Specifies the percent max threshold.
- **Swap file name** - Name of the swap file to monitor. Click the **Rescan swap files** link to update the list.
- **Logon account** - To override the asset default account select an account from the list.

Windows specific properties

- **Detailed error report** - Lists all processes and their memory usage in an error report.

Syslog monitor

The **Syslog** monitor can intercept syslog message sent to **Network Monitor** from one or more syslog hosts. The monitor can be configured to receive different types of messages. More than one syslog monitor can be added to each asset to receive different combinations of messages.

- System type: All
- Category: Log

Prerequisites

- Activate syslog message collection for each gateway separately, by checking the Network Monitor > (selected gateway) > Edit > **Advanced tab** (page 39) > **Syslog server** checkbox.
- View intercepted syslog messages display on the Network Monitor Tools > **List syslog messages** (page 97) page.

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Include string(s)** - Message included if it contains one of the strings specified in this field. Separate multiple strings with a comma.
- **Exclude string(s)** - Message excluded if it contains one of the strings specified in this field. Separate multiple strings with a comma.

TCP port scan monitor

The **TCP port scan** monitor verifies that the specified ports are either open or closed. By default, triggers an alarm is if specified ports are open. If the **Inverted function** is checked, triggers an alarm if the specified ports are closed.

- System type: All
- Category: Others

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Port number range** - Triggers an alarm if specified ports are open. Port ranges use the following format:
 - **21-23** - The monitor scans ports between and including 21 to 23.
 - **80,21-23** - The monitor scans port 80 and ports between and including 21 to 23. The monitor can check up to 100 ports.
- **Invert function** - If checked, triggers an alarm if the specified ports are closed.

Telnet server monitor

The **Telnet server** monitor verifies that a telnet server is responding.

- System type: All
- Category: Network service

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Port** - The port number the telnet server is configured to use. Defaults to **23**.

Terminal service monitor

The **Terminal service** monitor responds to new logon sessions.

- System type: All but Other/Unidentified
- Category: Network services

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Port** - The port number the terminal server is configured to use. Defaults to **3389**.

TFTP server monitor

The **TFTP server** monitor tests if a TFTP server is responding to a RRQ operation. The purpose of the test is to verify that the TFTP server is running. The monitor tries to download a file named **KNM**. This file does not have to exist for the test to succeed. The monitor merely checks that the TFTP server is responding in the correct way to such a request.

- System type: All
- Category: Network services

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Port** - The port number the TFTP server is configured to use. Defaults to **69**.

Transfer speed monitor

The **Transfer speed** monitor measures the transfer speed between **Network Monitor** and an asset. The test measures the time it takes to download the specified amount of data from the `chargen.exe` server running on the asset.

A `chargen` (Character Generator) server must be installed and running on the asset. Microsoft supplies a `chargen` server for Windows as part of the **Simple TCP/IP Services** service. This service is typically installed as a feature on Windows servers. The `chargen.exe` server uses port 19 (TCP) by default.

- System type: All
- Category: Network services

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Transfer speed** - Minimum transfer speed in the selected unit.
- **Unit** - The unit to record the transfer speed test in. Shown in real time chart and reports.
- **Data size** - Size, in kilo bytes, of total amount of data to receive in the test.
- **Port number** - The port number the TFTP server is configured to use. Defaults to 19.

VMware performance monitor

The **VMware performance** monitor can query a VMware performance counter for a VMware host or a vCenter server and compare it to a value using a compare operation. If the compare operation evaluates to `false` the monitor fails the test. Supports ESX 4.1 & ESXi 5. Makes no changes to the target VMware host machine. Supports most performance counters assets, such as hosts, datastores, and virtualstores. VMware counters for guests (virtual machines) are not supported.

- System type: VMware
- Category: Performance

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

The screenshot shows the 'Object properties' dialog box. The 'System type' dropdown is set to 'VMWare' and the 'ESX' version dropdown is set to 'ESX 4.1'. A red box highlights these two dropdowns. The 'Description' field is empty, and the 'Free text' field is also empty.

Identify the asset as a VMWare system type

Edit monitor ▶ Export settings ▶ Import settings

Basic properties

Name: CPU Usage Name of this monitor

Type: VMware performance Monitor type

Object: Vmware ESX 4.1 The monitor is owned by this object

Test interval: 10 Time in seconds between tests

Advanced properties (Click to expand/hide)

Alarm filtering (Click to expand/hide)

VMware performance monitor properties

Port: 443 Use this port to connect to the machine.

Counter: cpu.usage.none Name of counter of object [Rescan services](#)

Instance: 10 Name of instance of counter

Data type: CPU utilization Select the type of data stored by the monitor.

Comparison options

Value type: Integer Specify the type of the result. This setting will affect the compare operation.

Compare operation: Pass if not equal Specify how the result should relate to the compare value.

Compare value: 50 The value to compare with the result

Statistics (Click to expand/hide)

VMware performance monitor properties page

Monitor specific properties

- **Counter/Instance** - Name of the primary performance counter to test. The instance field is intentionally left blank for some counter types. A scan automatically enumerates the values displayed. Click the [Rescan](#) link to refresh these values.
- **Data type** - The unit of data sampled by the test. This makes it possible to group data from this type of monitor with other monitors such as CPU utilization in reports.
- **Value type** - Type of value returned.
- **Compare operation** - Operation used to evaluate the returned result and the predefined compare value.
- **Compare value** - User defined compare value. Only numerical values are valid.

Web server monitor

The **Web server** monitor can test a web server and validate the content of the requested page. Verify that the content in the requested page has not changed since the previous test. Search for a string in the page and verify links.

- System type: All
- Category: Network services

Note: Only monitor specific settings are documented here. See [Standard monitor settings \(page 63\)](#).

Basic tab

URL & request settings

- **URL** - URL of the page to download, relative to the web server address. The URL specified determines the links displayed in Web server monitor page links section.
- **Use secure HTTP** - Check this option to enable the monitor to communicate using secure HTTP (SSL).
- **Port** - Port number used to connect to the web server.

Threshold settings

Monitor Reference

- **Search string** - The string the page searches for. If not found, the test fails.
- **Page fetch time** - A threshold value in milliseconds. If the page is not delivered within the threshold value, the test fails.
- **Verify checksum** - Check option to have the monitor calculate the checksum value of the page. If the checksum value changes between two tests the current test fails. *To reset the checksum, open the property page and save the monitor.*
- **Perform login** - If checked, displays the HTTP account section below. Logs on to the server with the specified credential.

HTTP account

- **Inherit credentials** - If checked, inherits credentials from the asset. If blank, enter monitor-specific credentials.
- **Username/password** - Credential used to authenticate access for this monitor.
- **Port** - The port to connect to the HTTP account.

Advanced tab

Web server monitor advanced settings.

- **User agent** - Overrides the default user agent variable sent in the request.
- **Custom cookie** - Optional cookie to send with the get request.
- **Custom host** - Optional host header field to support named base virtual hosts.
- **Ignore CN check** - If checked the monitor does not validate the common name of the server certificate. This option is only valid if the monitor is using secure http.
- **Ignore date check** - If checked the monitor does not validate the expiration date of the server certificate. This option is only valid if the monitor is using secure http.
- **Ignore CA check** - If checked the monitor does not validate the certificate authority of the server certificate. This option is only valid if the monitor is using secure http.
- **Certificate store** - Name of the system certificate store. Use only if you want the monitor to send a client certificate to the server.
- **Certificate subject** - Subject line of certificate to use in the system certificate store. Use only if you want the monitor to send a client certificate to the server.
- **Proxy server** - Optional address of proxy server.
- **Proxy port** - Optional server port of proxy server.

Windows performance monitor

The **Windows performance** monitor can query a Windows performance counter to compare with a compare value using a compare operation. If the compare operation evaluates to `false` the monitor fails the test. Optionally two performance counters can be queried and combined before being compared with the compare value.

- System type: Windows
- Category: Performance

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Object/Counter/Instance** - Name of the primary performance asset to test. These values can be enumerated by using the enumeration function. The instance field is intentionally left blank for some counter types. Click the **Rescan** link to refresh these values

- **Object/Counter/Instance** - Optional. Secondary performance asset. These values can be enumerated by using the enumeration function. The instance field is intentionally left blank for some counter types.
- **Combine operation** - Optional operation used when querying two counters. They can be combined into a final result by using the add, subtract, divide or multiply operation.
- **Divisor** - A value that the retrieved value is divided with before the comparison.
- **Data type** - The unit of data sampled by the test. This makes it possible to group data with other monitors using the same type in reports.
- **Value type** - Type of value that is compared with the retrieved value.
- **Compare Operation** - Operation to use when comparing.
- **Compare value** - Value to compare with the resulting value from the calculation.
- **Inherit credentials** - Specifies the Windows domain credential, if one is required. If checked, inherited. If blank, overrides the Windows domain credential set for the asset on the **Authentication** (page 40) tab of an asset node.

Windows service status monitor

The **Windows service status** monitor tests that a Windows service is running.

- System type: Windows
- Category: Performance

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Available services** - List of services to select from. Click the **Select** button to append the selected service to the field service name. To refresh the list click the **Rescan** services link.
- **Service name** - Name of the service to monitor. Separate multiple services with a comma. When combining this monitor with a **Windows service control action** (page 149), only one service can be selected.
- **Invert function** - If checked, the monitor triggers an alarm if any of the listed services are running.
- **Inherit credentials** - Specifies the Windows domain credential, if one is required. If checked, inherited. If blank, overrides the Windows domain credential set for the asset on the **Authentication** (page 40) tab of an asset node.

See Also

- **Windows service control** (page 157) (scheduled event)
- **Windows service control** (page 149) (action)
- **Windows service list** (page 92) (direct control)

WMI Query monitor

The **WMI query** monitor can be used to execute WQL queries and perform conditional testing of the returned value. The monitor can execute all standard WQL queries, but the returned value comparison is limited to one field of the returned data.

- System type: Windows
- Category: Performance

Note: See **Windows Management Instrumentation** (page 178).

Note: Only monitor specific settings are documented here. See **Standard monitor settings** (page 63).

Monitor specific properties

- **Namespace** - Name space to execute the query within. The default namespace is `root\cimv2`.
- **WQL** - A WQL query.
- **Value name** - The name of the value to retrieve when the query has been executed. If more than one result row is returned, the value is retrieved from the first row in the result set.
- **Data type** - The unit of data sampled by the test. This makes it possible to group data with other monitors using the same type in reports.
- **Value type** - Type of value that is compared with the retrieved value.
- **Compare Operation** - Operation to use when comparing.
- **Compare value** - Value to compare with the resulting value from the calculation.

Chapter 4

Action Reference

This chapter contains a reference for all available actions and their respective settings. Actions are used on the **Actions tab** (page 56).

In This Chapter

Clear event log action	143
Execute command via SSH2 action	143
Execute Windows command action	144
HTTP Get/Post action	144
List reset action	146
Lua scripts action	146
Send mail action	146
Send message via PageGate action	147
Send SMS action	147
Send Wake-on-LAN packet action	148
SNMP Set action	148
Ticket action	149
Windows service control action	149

Clear event log action

The **Clear event log** action clears an event log on a specified Windows host.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Connect to** - Monitor host or Specific host. If specific host, enter the **Hostname**.
- **Host name** - Host name or IP number. Leave blank to use the address of the asset.
- **Credentials** - Monitor credentials or Stored credentials.
- **Inherit credentials** - If stored credentials is selected, the **Inherit credential** option displays. If checked, inherits credentials from the asset. If blank, enter action-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this action.
- **Log name** - Name of the log to clear. For example, Application.

Execute command via SSH2 action

The SSH2 action executes a command on a SSH2 server. Optionally the action can be configured to use the telnet protocol instead.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Connect to** - Monitor host or Specific host. If specific host, enter the **Hostname**.
- **Host name** - Host name or IP number. Leave blank to use the address of the asset.

- **Connection type** - SSH or Telnet. If telnet, ensure telnet parameters are correctly configured using the Network Monitor Settings > **Other system settings** (page 104) > **Monitor defaults** tab.

Warning: Remember that telnet is not encrypted and the username/password is sent in clear text.

- **Command** - Command to execute. The following formatting variables can be included when specifying a command.
 - %[asset.name] - asset name
 - %[monitor.name] - monitor name
 - %[asset.ip] - asset address
- **Port** - Port number that SSH2 server is listening on.
- **Credentials** - Monitor credentials or Stored credentials.
- **Inherit credentials** - If stored credentials is selected, the **Inherit credential** option displays. If checked, inherits credentials from the asset. If blank, enter action-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this action.

Execute Windows command action

The **Execute Windows command** action executes a command on the **Network Monitor** host machine. The command runs as a system user process and cannot require any interaction with a user.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Command** - Command to execute. The command is an executable that is located in the KNM root directory or in the Windows or System32 directory.
- **Parameters** - A string passed to the executed command as arguments.
- **Credentials** - Monitor credentials or Stored credentials.
- **Inherit credentials** - If stored credentials is selected, the **Inherit credential** option displays. If checked, inherits credentials from the asset. If blank, enter action-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this action.

HTTP Get/Post action

The **HTTP Get/Post** action sends a HTTP Get or Post request to a web server.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Connect to** - Monitor host or Specific host. If specific host, enter the **Hostname**.
- **Host name** - Host name or IP number. Leave blank to use the address of the asset.
- **Get/Post** - Method to use when sending request to web server.
- **URL** - The URL can be an absolute URL or an relative URL to the asset.
- **SSL** - Check option to use SSL. Remember that the web server normally listens to a different port then the default port of 80 for SSL traffic. If necessary, change the port number when selecting this option. The action accepts server side certificates with an invalid Common Name, expired date or invalid certificate authority. Checking and unchecking this box changes the port number between 80 (unchecked) and 443 (checked).
- **Port** - Port number. Defaults to 80.
- **Parameters** - *Post request only*. Enter parameters using the format name=value, one parameter per row. The following **formatting variables** (page 66) can be included in a parameter.

- `[%[system.time]` - current time
- `[%[asset.name]` - asset name
- `[%[asset.address]` - asset address
- `[%[monitor.name]` - monitor name
- `[%[monitor.error]` - monitor error message
- `[%[monitor.error2]` - monitor error message, no time stamp
- `[%[asset.description]` - asset description
- `[%[group.name]` - group name
- `[%[group.contact]` - group contact
- **Character encoding** - ISO-8859-1 or UTF-8. The encoding used by the request.
- **HTTP authentication** - If checked, enter a credential to authenticate the request.
- **Credentials** - Monitor credentials or Stored credentials.
- **Inherit credentials** - If stored credentials is selected, the **Inherit credential** option displays. If checked, inherits credentials from the asset. If blank, enter action-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this action.
- **Proxy settings**
 - **Proxy server** - Address of proxy server.
 - **Proxy port** - Proxy server port number.

Example: Get and post request with absolute URL

This example demonstrates two different ways of sending requests with variables to a web server, using either the get request or post request.

Get request

- **URL** - `http://www.yourserver.com/test.php?test1=1&test2=2`

Post request

- **URL** - `http://www.yourserver.com/test.php`
- **Parameters**
 - `test1=1`
 - `test2=2`

Example: Get and post request with a relative URL

This example demonstrates two different ways of sending requests with variables to a web server, using either the get request or post request. The URL is relative to the address of the asset calling the action.

Get request

- **URL** - `test.php?test1=1&test2=2`

Post request

- **URL** - `test.php`
- **Parameters**
 - `test1=1`
 - `test2=2`

List reset action

The list reset action, when executed, causes the execution to restart from the first action. The list reset action can be used to get a *loop* behavior. The list reset action is not available as a recovery action.

Lua scripts action

The **Lua scripts** action executes a **Lua** (page 186) script, the asset of the monitor that calls the action is used by the script as the host. The Lua script action can execute both simple and advanced scripts. Scripts using the advanced script model have custom defined argument sections that are not described here.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Author** - The creator of the Lua script.
- **Version** - The version of the Lua script.
- **Description** - A one line summary of the Lua script.

Note: Additional parameters display here, as required to support the Lua script.

- **Credentials**
 - **No authentication** - No other credential settings are required.
 - **Use specific credentials in API** - Set an **Account type** to Windows domain account, SSH/Telnet account or VMware account.
 - **Perform Windows impersonation** - Use a user logon account.
- **Inherit credentials** - If **Use specific credential in API** or **Perform Windows impersonation** is selected, the **Inherit credential** option displays. If checked, inherits credentials from the asset. If blank, enter action-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this action.

Send mail action

The **Send mail** action sends an email to one or more recipients. The message is formatted using the format specified or inherited by the monitor.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Users on duty** - The message is sent to on duty users only. If no users are scheduled on duty, no message is sent.
- **Notification group** - The message is sent to all users in the user group assigned to the asset.
- **Group manager** - The message is only sent to the user that is designated as group manager of the user group assigned to the asset. If the user group does not have an designated group manager, no message is sent.
- **Specific user group** - The message is sent to the selected user group. Using this option you can escalate the alarm to include more users then only the users in the user group assigned to the asset.
- **Specific recipient** - The message is sent to one or more email addresses separated by a semi-colon.

- **Short message** - If checked, a compressed message is sent. For example if the message is sent over an SMS gateway. This option removes the following information to conserve the size of message.
 - `[%[asset.description]` - asset description
 - `[%[user.distribution_list]` - distribution list
 - `[%[monitor.dependency_status]` - dependency tree status
 - `[%[monitor.error]` - monitor error message
 - `[%[network.contact]` - network contact

Send message via PageGate action

The **Send message via PageGate** action sends a message to a Pagegate user. The message is formatted using the format specified or inherited by the monitor.

Parameters

- **Alarm number** - The **alarm count** (*page 56*) this action triggers on.
- **Users on duty** - The message is sent to on duty users only. If no users are scheduled on duty, no message is sent.
- **Notification group** - The message is sent to all users in the user group assigned to the asset.
- **Group manager** - The message is only sent to the user that is designated as group manager of the user group assigned to the asset. If the user group does not have an designated group manager, no message is sent.
- **Specific user group** - The message is sent to the selected user group. Using this option you can escalate the alarm to include more users then only the users in the user group assigned to the asset.
- **Specific recipient** - The message is sent to one or more email addresses separated by a semi-colon.
- **Short message** - If checked, a compressed message is sent. For example if the message is sent over an SMS gateway. This option removes the following information to conserve the size of message.
 - `[%[asset.description]` - asset description
 - `[%[user.distribution_list]` - distribution list
 - `[%[monitor.dependency_status]` - dependency tree status
 - `[%[monitor.error]` - monitor error message
 - `[%[network.contact]` - network contact

Send SMS action

The **Send SMS** action sends an SMS to one or more recipients. The message is formatted using the format specified or inherited by the monitor. The max message text is 160 characters. Excessive text is truncated before sending the SMS.

To use this action **SMS settings** (*page 104*) must be configured.

Parameters

- **Alarm number** - The **alarm count** (*page 56*) this action triggers on.
- **Users on duty** - The message is sent to on duty users only. If no users are scheduled on duty, no message is sent.
- **Notification group** - The message is sent to all users in the user group assigned to the asset.

- **Group manager** - The message is only sent to the user that is designated as group manager of the user group assigned to the asset. If the user group does not have an designated group manager, no message is sent.
- **Specific user group** - The message is sent to the selected user group. Using this option you can escalate the alarm to include more users then only the users in the user group assigned to the asset.
- **Specific recipient** - The message is sent to one or more email addresses separated by a semi-colon.
- **Short message** - If checked, a compressed message is sent. For example if the message is sent over an SMS gateway. This option removes the following information to conserve the size of message.
 - `%[asset.description]` - asset description
 - `%[user.distribution_list]` - distribution list
 - `%[monitor.dependency_status]` - dependency tree status
 - `%[monitor.error]` - monitor error message
 - `%[network.contact]` - network contact

Send Wake-on-LAN packet action

The **Send Wake-on-LAN packet** action (WOL) can start a host that is compliant with the WOL standard. Refer to the host's documentation to determine if the action can be used.

Note: This action is restricted to waking up hosts located on the same *broadcast domain* as the host used to send the WOL packet. Assets typically can broadcast a message to all assets sharing the same router. Routers act as boundaries between broadcast domains. A LAN may include multiple routers, each router representing another broadcast domain.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Connect to** - Monitor host or Specific host. If specific host, enter the **Mac address**.
- **MAC address** - The MAC address of the interface to send the WOL packet to. The format of the MAC address is AA-BB-CC-DD-EE-FF. Leave the field blank to use the MAC address of the asset.
- **Interval** - The time to wait, in seconds, between sending each packet. If the packet count is set to 5 and the interval to 5, 5 packets are sent during a 25 second period.
- **Packet count** - How many times the packet should be sent. Set this value to higher then 1 to be sure that the host receives it.

SNMP Set action

The **SNMP Set** action can be used to change values of asset identifiers (OIDs) in a remote SNMP agent.

Note: The community name, SNMP version, and port used by **Network Monitor** to connect to an SNMP asset is set on the **Authentication** (page 40) tab of an asset node. The asset node may inherit this setting from a parent node. See the **Installation Checklist** (page 9).

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Connect to** - Monitor host or Specific host. If specific host, enter the **Hostname**.

- **Host name** - Host name or IP number. Leave blank to use the address of the asset.
- **OID** - Enter the relevant OID.
 - You can specify either a named OID or a OID in number format. If you specify a named OID, **Network Monitor** tries to resolve it to its number format automatically when the field loses focus. **Network Monitor** uses the currently compiled MIBs to attempt to find the number format of the OID.
 - The [...] button next to the OID field display a MIB Browser dialog that can be used to select asset identifiers from the remote SNMP agent.
 - When the MIB browser displays an OID number with a @string it means you can use this string as part of the OID. For example the OID .1.3.6.1.2.1.2.2.1.16@Intel(R) PRO/1000 MT Network Connection can be entered in the OID field instead of identifying the index number of the network connection.
- **Value** - Value to set.
- **Syntax type** - Type of value. The value can be an integer or a string.
- **Credentials** - Monitor credentials or Stored credentials.
- **Inherit credentials** - If stored credentials is selected, the **Inherit credential** option displays. If checked, inherits credentials from the asset. If blank, enter action-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this action.

Ticket action

The **Ticket** action creates a ticket when triggered by an alarm count on an asset **Network Monitor** is monitoring. By default the **Ticket** action is inherited by all assets from the KNM group node. The alarm count is set to 1.

Note: A ticket is created in either the **Ticketing** module or **Service Desk**, depending on whether **Service Desk** has been **activated** (<http://help.kaseya.com/webhelp/EN/KSD/9000000/index.asp#5478.htm>) within the VSA.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **User** - Select a default VSA user for the **Ticket** action. This is the VSA user assigned to the created ticket if no other VSA user is assigned.

Windows service control action

The **Windows service control** action can start, stop, pause, continue and restart Windows services. All service actions share the same set of parameters.

Parameters

- **Alarm number** - The **alarm count** (page 56) this action triggers on.
- **Connect to** - Monitor host or Specific host. If specific host, enter the **Hostname**.
- **Host name** - Host name or IP number. Leave blank to use the address of the asset.
- **Service name** - Name of service. Leave this blank to get the service name from the monitor. This requires that the monitor executing this action be a **Windows service status monitor** (page 141) with only one service configured to check.
- **Type** - Select the type of operation to perform.

Scheduled Event Reference

Continue service
Pause service
Start service
Stop service
Restart service

- **Credentials** - Monitor credentials or Stored credentials.
- **Inherit credentials** - If stored credentials is selected, the **Inherit credential** option displays. If checked, inherits credentials from the asset. If blank, enter action-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this action.

See Also

- **Windows service control** (page 157) (schedule event)
- **Windows service list** (page 92) (direct control)
- **Windows service status** (page 141) (monitor)

Scheduled Event Reference

This chapter contains a reference for all available **scheduled events** (page 36) and their respective settings.

Clear eventlog event

The **Clear eventlog** event clears the event log on a remote Windows host.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **Hostname** - The hostname of the remote host. This can be either a DNS name or an IP address.
- **Log name** - Specify the name of the event log to clear.
- **Inherit credentials** - If checked, inherits credentials from the currently selected group or gateway node. If blank, enter event-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this event.

Execute command via SSH2/Telnet event

The **Execute command via SSH2/Telnet** event connects to a remote server using SSH2 or telnet and executes a command.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **Hostname** - The hostname of the remote host. This can be either a DNS name or an IP address.
- **Command** - Specify the command to be executed on the remote host.
- **Port** - Specify the port number where to connect. For SSH2 the default port is 22 and for telnet the default port is 23.
- **Use telnet** - If checked, **Network Monitor** connects to the remote host using the Telnet protocol. Checking this option automatically modifies the port to 23.

- **Inherit credentials** - If checked, inherits credentials from the currently selected group or gateway node. If blank, enter event-specific credentials.
- **Username/Password** - Credential used to authenticate access for this event.

Execute Windows command event

The **Execute Windows command** event executes a specified command **on the Network Monitor host machine**. This can be used to trigger scripts or batch files located on the **Network Monitor** host. The command runs as a system user process and cannot require any interaction with a user.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **Command** - Enter the command to be executed.
- **Parameters** - Add parameters to be sent with the command. Use citation characters to specify a parameter containing spaces as one parameter.
- **Inherit credentials** - If checked, inherits credentials from the currently selected group or gateway node. If blank, enter event-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this event.

Export statistics event

The **Export statistics** event exports collected statistical data for a given period. The data can be exported to CSV files (comma separated text files) for import into spreadsheet applications, or directly to another database via ODBC. Exporting to another database requires 32 bit, System DSN ODBC driver be configured on the target database machine.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event statistics

The settings for this event are divided into two sections. In the first section the type and source of the exported data is defined.

- **Data type / Selected datatypes** - Select the specific type of data to be exported. The data types are organized into categories. To add a data type to the export list, select it and click the **Select** button. Selected data types are added to the selected list. To remove a data type, select it and click the **Remove** button.
- **Period** - Specify the period to export the data.
- **Asset / Selected assets** - To select assets for data export, first select the relevant network where the asset is located, then select one or more assets from the list and click the **Select** button. Selected assets are added to the selected assets list. To remove an asset from the data export, select it and click the **Remove** button.

Export options

In this section the details for the CSV file or database export is defined.

- **Export to file** - Select this option to export statistics data to a CSV file.
 - **Filename** - This is the filename of the exported data file. Files are exported to the KNM\reports\export directory. Optionally include the following formatting variables when specifying the filename.
 - ✓ **%[system.date]** - the current date

Scheduled Event Reference

- ✓ `[%[system.time]` - the current time
- **Export to database** - Select this option to export statistics data to a database via ODBC.
 - **Datasource name** - The name of a previously defined ODBC datasource.
 - **Database name** - The name of the database to store the statistics into.
- **Clear tables before export** - Clears the database tables before exporting the data.
- **Inherit credentials** - If checked, inherits credentials from the currently selected group or gateway node. If blank, enter event-specific credentials.
- **Username/Password** - Credential used to authenticate access for this event.
- **Include marker data** - If checked and there is a problem providing real data, a placeholder value of -10000 is inserted instead. If blank, no placeholder value is inserted.

Exporting statistics to a CSV file

When exporting statistics data to a file, **Network Monitor** produces two files every time the event is executed. The files are placed in the `KNM\reports\export` folder of the KNM host machine.

One file has the name specified in the **Filename** box in the event properties. This file contains the raw exported data. The second file has the same name, but has `info_` prefixed to the name. This file contains a description of the kind of data that was exported.

The structure of the info file looks like this:

```
Network name;asset name;monitor
name;monitor-id;monitor-subid;datatype-id;unit;datatype description
```

Example

```
Default network;Backup;Disk utilization (C:);84;0;3;%;Disk utilization
```

The structure of the data file looks like this:

```
monitor-id;datatype-id;monitor-subid;timestamp;raw data;comment
```

Example

```
84;3;0;2009/08/05 09:42:57;13.669434;
```

If the record is considered invalid by **Network Monitor**, a fixed value of -10000.0 is exported.

Exporting to a database

When exporting statistics data to a database, **Network Monitor** creates two tables in the database. The first table is called `inmDataExportInformation`. It has the following structure:

```
CREATE TABLE inmDataExportInformation (networkName char(128), assetName
char(128),monitorName char(128), monitorID integer, atomID integer, dataType
integer, unitNamechar(32), exportedDataType char(128));
```

This table contains information about the data that was exported, similar to to exporting data to a file.

The second table is called `inmDataExport`. It has the following structure:

```
CREATE TABLE inmDataExport (monitorID integer, atomID integer, dataType integer,
dateTime DATETIME, dataRaw float);
```

This table contains all of the exported statistics data.

Warning: **Network Monitor** begins the export of data by dropping tables with these two names. The database user configured for **Network Monitor** will require appropriate access to DROP, CREATE and INSERT operations on the database in question. Refer to your database manual for information about how to configure a database user.

Generate report event

The **Generate report** event is used to schedule the generation of a report and send or publish the report to specific recipients.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event configuration tab

Generate report

Select the type of report to generate.

- **Generate a customized report** - If selected, all configuration settings and all asset and monitor selections have already been made using Network Monitor Reports > **Customize reports** (page 77). You only need to select the name of the customized report using the **Customized report** drop-down list.
- **Generate a report template** - If selected, you must select the report template to use, the time period, and the assets and monitors to include the report.
 - **Report template** - Select a report template to schedule. See the section below on selecting assets for a report template.
 - **Period** - Select the report period for the report template.
 - **Run as** - Select the user running the report.
 - **Separate reports** - Select this option to send separate reports for each asset.

Selection

This section only displays if **Generate a report template** was selected. Specify what assets to include in the report.

- **Select asset / Selected assets** - Enter text to display the names of assets in the **Select asset** list that match the text entered. Select one or more assets in the list, then click the **Add** button to add the assets to the **Selected assets** list. You can also click the **Select** button to browse for target assets. To remove an asset, select it and click the **Remove** button.
- **Select monitor / Selected monitors** - Enter text to display the names of monitors in the **Select monitor** list that match the text entered. Select one or more monitors in the list, then click the **Add** button to add the monitors to the **Selected monitors** list. You can also click the **Select** button to browse for target monitors. To remove a monitor, select it and click the **Remove** button.

Report recipients tab

Use this section to select the recipients of the generated report.

- **User group** - Select a user group from the list and click the **Select** button. You can include more than one group. The selected user group are added to the selected group list. To remove a user group, select it and click the **Remove** button.
- **User** - Select the user from the list and click the **Select** button. You can include more than one user. The selected user will be added to the selected user list. To remove a user, select it and click the **Remove** button.
- **Email** - Specify individual email addresses as recipients. Separate multiple entries with a comma.
- **Subject** - Specify a subject line for the emailed report. If left blank the default subject line format specified by the Network Monitor Settings > SMS > **Default messages** (page 107) tab is used.
- **Directory** - The generated report can be published on a network folder as an HTML document. Specify the path to this folder. Optionally include the following formatting variables when specifying a path.
 - `%[system.date]` - current full date

Scheduled Event Reference

- `%[system.date_year]` - current year
- `%[system.date_month]` - current month
- `%[system.date_day_of_month]` - current day in the month
- `%[system.time]` - current full time
- `%[system.time_hour]` - current hour
- `%[system.time_minute]` - current minute
- `%[system.time_second]` - current second

FTP upload options

The generated report can be published on a FTP server as a HTML document.

- **FTP host & port** - Specify the host name and port number. Defaults to `21`.
- **Inherit credentials** - If checked, inherits credentials from the currently selected group or gateway node. If blank, enter event-specific credentials.
- **Username/Password** - Credential used to authenticate access for this event.

HTTP GET/POST request event

The **HTTP GET/POST request** event performs an HTTP request to a remote host. Both GET and POST request methods are supported.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **URL** - Specify the target URL of the request.
- **SSL** - If checked, the request uses Secure Socket Layer (SSL). Checking this option automatically updates the port number.
- **Port** - Specify the port number to use. The default port for HTTP is 80.
- **Parameters** - *Post request only*. Enter parameters using the format `name=value`, one parameter per row. The following **formatting variables** (page 66) can be included in a parameter.
 - `%[system.time]` - current time
 - `%[asset.name]` - asset name
 - `%[asset.address]` - asset address
 - `%[monitor.name]` - monitor name
 - `%[monitor.error]` - monitor error message
 - `%[monitor.error2]` - monitor error message, no time stamp
 - `%[asset.description]` - asset description
 - `%[group.name]` - group name
 - `%[group.contact]` - group contact
- **Character encoding** - `ISO-8859-1` or `UTF-8`. The encoding used by the request.
- **HTTP authentication** - If checked, enter a credential to authenticate the request.
- **Inherit credentials** - If checked, inherits credentials from the currently selected group or gateway node. If blank, enter event-specific credentials.
- **Username/Password** - Credential used to authenticate access for this event.
- **Proxy settings**
 - **Proxy server** - Address of proxy server.
 - **Proxy port** - Proxy server port number.

Lua scripts event

The **Lua scripts** event executes a Lua script. Lua is the scripting language natively supported by **Network Monitor**. See **Lua** (page 186) for more information.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **Script** - Select the script to be executed. Lua scripts used with **Network Monitor** should be placed in the `KNM\scripts` folder of the KNM host machine. Once a script has been selected, individual fields for the script parameters display.
- **Credentials**
 - **No authentication** - No credentials are required.
 - **Use specific credentials in API** - Set an **Account type** to Windows domain account, SSH/Telnet account or VMware account. If this option is selected, **Network Monitor** does not perform Windows authentication before executing the script. Instead, the specified logon account information is passed to the script as a parameter. This is useful for scripts that want to perform custom logons, for example, with SSH2.
 - **Perform Windows impersonation** - A Windows authentication is performed with the specified host before executing the script. This is useful for scripts that require authentication before executing.
- **Inherit credentials** - If **Use specific credential in API** or **Perform Windows impersonation** is selected, the **Inherit credential** option displays. If checked, inherits credentials from the group or gateway node. If blank, enter event-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this event.

Send email event

The **Send email** event sends an email with specified content to one or more users or user groups. For information on how to configure email settings, see the Email and SMS settings topic.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **User group** - Select a user group to be the recipient of the message.
- **User / Selected users** - Add specific users to be recipients of the message by selecting them from the list and clicking the **Select** button. To remove a user, select it from the list and click the **Remove** button.
- **Specific recipient** - Enter specific email addresses. Separate multiple entries with a comma.
- **Subject** - Specify the subject line of the message.
- **Message** - Specify the message body text.

Send message via PageGate event

The **Send message via PageGate** event sends a paging message through a PageGate paging server to one or more users or user groups. For information on how to configure PageGate, see the **Miscellaneous settings** (page 104) section.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **User group** - Select a user group to be the recipient of the message.
- **User / Selected users** - Add specific users to be recipients of the message by selecting them from the list and clicking the **Select** button. To remove a user, select it from the list and click the **Remove** button.
- **Specific recipient** - Enter specific PageGate users. Separate multiple entries with a comma.
- **Subject** - Specify the subject line of the message.
- **Message** - Specify the message body text.

Send SMS event

The **Send SMS** event sends a SMS message specified content to one or more users or user groups. For information on how to configure an SMS capable asset, see the Email and SMS settings topic.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **User group** - Select a user group to be the recipient of the message.
- **User / Selected users** - Add specific users to be recipients of the message by selecting them from the list and clicking the **Select** button. To remove a user, select it from the list and click the **Remove** button.
- **Specific recipient** - Enter specific phone numbers. Separate multiple entries with a comma.
- **Subject** - Specify the subject line of the message.
- **Message** - Specify the message body text.

Send Wake-On-LAN packet event

The **Send Wake-On-LAN packet** event can power up a remote host by using the Wake-On-LAN protocol. To be able to use this event, the remote host must support the Wake-On-LAN feature.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **Mac address** - Specify the Mac address of the network card on the remote host that should receive the Wake-On-LAN request. The format of the MAC address is AA-BB-CC-DD-EE-FF.
- **Interval** - The time to wait, in seconds, between sending each packet. If the packet count is set to 5 and the interval to 5, 5 packets are sent during a 25 second period.
- **Packet count** - How many times the packet should be sent. Set this value to higher than 1 to be sure that the host receives it.

SNMP Set event

The **SNMP Set** event sends an SNMP set request to a remote SNMP agent.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Note: The community name, SNMP version, and port used by **Network Monitor** to connect to an SNMP asset is set on the **Authentication** (page 40) tab of an asset node. The asset node may inherit this setting from a parent node. See the **Installation Checklist** (page 9).

Event settings

- **Hostname** - The hostname of the remote SNMP agent. This can be either a DNS name or an IP address.
- **OID** - Enter the relevant OID.
 - You can specify either a named OID or a OID in number format. If you specify a named OID, **Network Monitor** tries to resolve it to its number format automatically when the field loses focus. **Network Monitor** uses the currently compiled MIBs to attempt to find the number format of the OID.
 - The [...] button next to the OID field display a MIB Browser dialog that can be used to select asset identifiers from the remote SNMP agent.
 - When the MIB browser displays an OID number with a @string it means you can use this string as part of the OID. For example the OID .1.3.6.1.2.1.2.2.1.16@Intel(R) PRO/1000 MT Network Connection can be entered in the OID field instead of identifying the index number of the network connection.
- **Value** - Value to set.
- **Syntax** - Type of value. The value can be an integer or a string.
- **Inherit credentials** - If checked, inherits credentials from the group. If blank, enter event-specific credentials.
- **SNMP version / Read community / Write community** - Credential used to authenticate access and run the **SNMP Set** event.

Trigger monitor event

The **Trigger monitor** event can be used to execute a monitor test at a given time. This can be useful for monitors that should only be tested on a very specific time during a period, for example. *Once a monitor is scheduled for a test, it is no longer tested periodically as normal.*

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **Monitor** - Select the monitor to be triggered.

Windows service control event

The **Windows service control** event can modify the status of a Windows service on a remote host.

Note: See the **Schedules tab** (page 36) topic for an introduction to scheduling events.

Event settings

- **Hostname** - The hostname of the remote host. This can be either a DNS name or an IP address.
- **Service name** - Specify the name of the service. This should be the service name and not the display name.
- **Type** - Select the type of operation to perform.
 - Continue service

Scheduled Event Reference

Pause service
Start service
Stop service
Restart service

- **Inherit credentials** - If checked, inherits credentials from the currently selected group or gateway node. If blank, enter event-specific credentials.
- **Domain or Computer/Username/Password** - Credential used to authenticate access for this event.

See Also

- **Windows service control** (*page 149*) (action)
- **Windows service list** (*page 92*) (direct control)
- **Windows service status** (*page 141*) (monitor)

Chapter 5

Advanced Topics

In This Chapter

Init.cfg parameters	159
Backup of Network Monitor	160
Data extraction reference	160
UNIX system support files	167
Enabling the ODBC Driver	169

Init.cfg parameters

The `init.cfg` file is used by **Network Monitor** for settings that are needed before the database with the configuration is loaded. It controls which port **Network Monitor** starts the web server on and in which mode **Network Monitor** starts in (Standard, Distributed server or Distributed gateway). The `init.cfg` file is located in the KNM root directory.

Log

- `LOG_LEVEL = 0` - Log level, if set to other than zero **Network Monitor** writes debug information into the text log. Valid log level is 0, 1 and 2. If log level is set to 2 (default 1) **Network Monitor** starts logging detailed information to the `<Kaseya_Installation_Directory>\Logs\Services\KaseyaNetworkMonitor.log` file. Can be useful when debugging mail and SMS sending behavior for example. Can be changed while **Network Monitor** is running.

SSH2

- `SSH2_TIMEOUT=25000` - SSH2 client timeout time in milliseconds. Defaults to 25000 (25 seconds). Can be changed while **Network Monitor** is running.
- `SSH2_TRACELEVEL=0` - Tracelevel can be used to debug the ssh2 connection. Defaults to 0. A valid range is 0 to 4 (max output). Can be changed while **Network Monitor** is running.

Testing thread pool configuration

- `TP_INIT_SIZE` - The initial size of the thread. Defaults to 20.
- `TP_MAX_AGE` - The max age in seconds a thread can be unused before being deleted from the pool. Defaults to 3600 (one hour). The purpose of this parameter is to have the thread pool balance the size to a optimal size for your configuration.
- `TP_MAX_SIZE` - Max size that the thread pool can grow to. Defaults to 125.

Other

- `OBJECT_IP_CACHE=1` - **Network Monitor** resolves all asset host names into IP addresses. This feature can be turned off if there is problems with the local DNS. Defaults to 1 (enabled). Optionally 0 (disabled). Can be changed while **Network Monitor** is running.
- `DELAY_TEST_START=0` - This parameter can be used to delay the start of monitor tests when **Network Monitor** is starting up. Defaults to 0 seconds. Useful for reducing machine boot time stress by delaying the start of **Network Monitor** monitor tests. Can not be changed while **Network Monitor** is running.

- `OPERATOR_SESSION_TIMEOUT=20` - Sets the user session timeout value, in minutes. If no timeout is wanted, set value to -1. Can be changed while **Network Monitor** is running.
- `SNMP_TIMEOUT=10000` - To set the timeout used by all SNMP functions (monitors, actions etc), in milliseconds. Defaults to 10 seconds. Can be changed while **Network Monitor** is running.
- `ENABLE_CRASHFILE=true` - If enabled and **Network Monitor** hangs in a deadlocked state, **Network Monitor** produces a crash dump file called `crash.now` in the KNM root directory. This file is used by **Network Monitor** developers to analyze why the deadlock occurred. Can be changed while **Network Monitor** is running.
- `DISTTEST_UPDATE_INTERVAL=60` - Time between events that cause the gateway and server to exchange information. Can be set in both gateway and server `init.cfg` files to separate values. The default 60 seconds is recommended.
- `DISABLE_RTS` - If this variable is present and set to 1 in the `init.cfg` file at startup, no real-time statistics are loaded for monitors. This can greatly speed up the startup time of **Network Monitor**.
- `NO_TESTING` - If this variable is present and set to 1 in the `init.cfg` file at startup, no testing is performed until a user enables the testing again.
- `HOSTNAME_OVERRIDE=myhost.domain.local` - When sending notifications to users a link to the monitor/asset is included in the notification e-mail. The link starts with the host name of the **Network Monitor** host machine. This parameter can be used to override that name. Can be changed while **Network Monitor** is running.
- `DISTTEST_MODE=server` - This parameter tells **Network Monitor** to start the distributed subsystem in either “server” or “gateway” mode. This parameter is dependent on the `DISTTEST_ENABLE` parameter. Can be changed while **Network Monitor** is running.
- `DISTTEST_ENABLE=1` - This parameter tells **Network Monitor** to start the distributed subsystem. This parameter is dependent on the `DISTTEST_MODE` parameter. The parameter can be set to 1 to enable or 0 to disable. Can be changed while **Network Monitor** is running.

Backup of Network Monitor

The following database, files and directories should be included in a backup of **Network Monitor**:

- `ksubscribers` - The SQL server database for your VSA.

These files and directories are located in the `<Kaseya_Installation_Directory>\KNM` directory:

- `\server.nxd`
- `\rmstorage`
- `\mibs` - If new mibs have been added.
- `\script` - If new scripts have been added or any scripts changed.

Data extraction reference

The data extraction interface can extract data from **Network Monitor** with HTTP Get commands.

Prerequisite

Each get request sent to **Network Monitor** must include a user username. If the user is also flagged as a system administrator, the user has system wide access. Otherwise the information is restricted to the data controlled by the user groups the user is member of. If the user is not allowed to access the information **Network Monitor** returns an HTTP 404 error code.

URL Syntax

The format of the URL sent to **Network Monitor** contains some required parameters.

Example URL for extracting a chart from a monitor

```
http://localhost/knm/extract.xsi?cmd=monitor_graph&user=Admin&id=8&param1=2
```

cmd	Command to execute
user	Network Monitor user username
id	Id of monitor or user
param1	Custom parameter

dir

The `dir` command returns a list of available monitors and users with their name and id. This command can be useful when designing extraction URLs for all other commands.

Syntax

```
http://localhost/knm/extract.xsi?cmd=dir&user=Admin
```

cmd	dir
user	Network Monitor user username

Returned data

A list of monitors and users with their IDs.

monitor_graph

The `monitor_graph` command returns a PNG image file with the selected real time chart. This is the same chart that is shown in the [Monitor information](#) page. Before a chart can be extracted, the chart must be enabled using the [Monitor information](#) page.

Syntax

```
http://localhost/knm/extract.xsi?cmd=monitor_graph&user=Admin&id=8&param1=2&deviceid=2
```

cmd	monitor_graph
user	KNM user username
id	ID number of monitor
param1	Zero based index of chart to retrieve. The index is based on enabled graphs.
deviceid	ID of asset

Returned data

A PNG image file with the default size of 747x120 pixels and a color depth of 3 bytes per pixel.

monitor_status_list

The `monitor_status_list` command returns the monitor status string. The status string is the same status shown in the [Monitor information](#) page.

Syntax

```
http://localhost/knm/extract.xsi?cmd=monitor_status_list&user=Admin&deviceid=2
```

cmd	monitor_status_list
user	KNM user username
deviceid	ID of asset

Returned data

A string containing the name of the asset and monitor, the status string and the status of the monitor separated by a pipe sign (|). Each line is separated by a CRLF.

Example

```
MyAsset | CPU load Monitor | Current CPU usage 11.00 % | OK
MyAsset | Memory size Monitor | Free memory 256 MB | FAILED
```

monitor_statusstring

The `monitor_statusstring` command returns the monitor status string. The status string is the same shown in the [Monitor information](#) page.

Syntax

```
http://localhost/knm/extract.xsi?cmd=monitor_statusstring&user=Admin&id=8&deviceid=2
```

cmd	monitor_statusstring
user	KNM user username
id	ID number of monitor
deviceid	ID of asset

Returned data

A string containing the name of the monitor, the status string and the status of the monitor separated by a pipe sign (|).

Example

```
CPU load Monitor | Current CPU usage 11.00 % | OK
```

monitor_uptimestring

The `monitor_uptimestring` command returns the monitor uptime string. The uptime string describes the uptime of the monitor in hours, minutes and second. If the monitor is currently in alarm state an asterisk (*) is added to the front of the string to note that the string indicates the downtime of the monitor.

Syntax

```
http://localhost/knm/extract.xsi?cmd=monitor_uptimestring&user=Admin&id=8&deviceid=2
```

cmd	monitor_uptimestring
user	KNM user username
id	ID number of monitor
deviceid	ID of asset

Returned data

A string containing the name of the monitor and the uptime/downtime string separated by a pipe sign (|).

Example

```
CPU load Monitor | 0h 59m 35s
```

device_xml

The `device_xml` command returns an xml document containing information about an asset. To access the asset the user must be a member of the user group assigned to the asset.

Syntax

```
http://localhost/knm/extract.xsi?cmd=device_xml&user=Admin&id=2
```

cmd	device_xml
user	KNM user username
id	ID number of the asset

Returned data

An xml document.

XML fields

DEVICE	Root of tree
NAME	Real name
DESC	Description of the asset
IP_ADDRESS	IP address or host name of asset
MAC_ADDRESS	MAC address of asset (if available)
ACTIVE	YES if asset is enabled, NO if disabled
MAINTENANCE	"Available" if user is scheduled and on duty, "n/a" if not on duty or not scheduled
MONITOR	Child to ASSET
NAME	Monitor name
TEST_INTERVAL	Interval between tests, in seconds
ALARM_DELAY	Interval between tests when monitor is in alarm state, in seconds
ALARM_GENERATION	How many consecutive tests that have to fail before an monitor is considered to be in alarm state
LAST_TEST	Time of the most recent test
LAST_OK_TEST	Time of the most recent ok test
LAST_FAILED_TEST	Time of the most recent failed test
TEST_DONE	Number of tests done since last reboot
ACTIVE	YES if monitor is enabled, or NO if disabled
TYPE	Type of monitor
STATUS	State of monitor, can be OK, FAILED or ALARM

Advanced Topics

STATUS_STRING	The most recent status string
UPTIME	Time that the monitor have been in OK state or ALARM state, when in ALARM state the string is prefixed with a '*' sign
INM_ALARM_MESSAGE	Child to MONITOR, shows the last 5 status strings
MESSAGE	Status text
TIME	Time of the entry
STATUS	OK, FAILED or ALARM
INM_GRAPH_LINK	Child to MONITOR, contains information about the realtime charts displayed in the monitor information page
LINK	A data extraction link to the chart
DESC	Description of the chart
UNIT	Unit of the Y axis of the chart
PERIOD	Time period of the chart
STATUS_EX	Extended status for SNMP, SSH2 Script, ODBC and WinPerf monitors
STATUS	State of monitor can be OK, FAILED or ALARM
UNIT	User defined unit
COMPARE_VALUE	User defined value that value returned from test is compared with, to evaluate the result of the test.
COMPARE_OPERATION	Operation to compare returned value from test and the user defined compare value. Can be: <ul style="list-style-type: none">• EQUAL• NOT EQUAL• GREATER• LESS• EQUAL OR GREATER• EQUAL OR LESS
LAST_VALUE	Last value returned from test.

Example

```
<DEVICE>
  <NAME>DOMAINSERVER</NAME>
  <DESC></DESC>
  <IP_ADDRESS>192.168.1.1</IP_ADDRESS>
  <MAC_ADDRESS>00-00-5A-A8-07-D8</MAC_ADDRESS>
  <ACTIVE>YES</ACTIVE>
  <MAINTENANCE>NO</MAINTENANCE>
  <MONITOR>
    <NAME>Bandwidth test</NAME>
    <TEST_INTERVAL>10</TEST_INTERVAL>
    <ALARM_DELAY>600</ALARM_DELAY>
    <ALARM_GENERATION>5</ALARM_GENERATION>
    <LAST_TEST>2004-06-10 13:38:55</LAST_TEST>
    <LAST_OK_TEST>2004-06-10 13:38:40</LAST_OK_TEST>
    <TEST_DONE>0</TEST_DONE>
    <ACTIVE>NO</ACTIVE>
```

```

        <TYPE>Bandwidth test</TYPE>
        <STATUS>OK</STATUS>
        <STATUS_STRING></STATUS_STRING>
        <UPTIME>23t 4m 45s</UPTIME>
    </MONITOR>
</DEVICE>

```

devicelist_xml

The `devicelist_xml` command returns an xml document containing a list on all assets and monitors that the user can access.

Syntax

```
http://localhost/KNM/extract.xsi?cmd=devicelist_xml&user=Admin
```

cmd	devicelist_xml
user	KNM user username

Returned data

An xml document.

XML fields

DEVICELIST	Root of tree
DEVICE	Root of asset
NAME	Name of the asset
DESC	Description of the asset
ID	ID Number of asset

MONITOR	Root of asset
ID	ID Number of Monitor
NAME	Name of the monitor

Example

```

<DEVICELIST>
  <DEVICE>
    <NAME>Fileserver</NAME>
    <DESC>Office fileserver</DESC>
    <ID>955</ID>
    <MONITOR>
      <ID>8</ID>
      <NAME>Bandwidth test</NAME>
    </MONITOR>
  </DEVICE>
</DEVICELIST>

```

user_status

The `user_status` command returns user status and information.

Syntax

```
http://localhost/knm/extract.xsi?cmd=user_status&user=Admin&id=2
```

cmd	user_status
user	KNM user username

Advanced Topics

id	ID number of user
----	-------------------

Returned data

A string containing user status and information, the fields are separated by a pipe sign (|).

Format of returned data.

UserName | Name | Phone | Cell phone | Address 1 | Address 2 | Scheduled status | Online status

Username	KNM user username
Name	Real name
Phone	Phone number
Cell phone	Cell phone number
Address 1	Address field
Address 2	Address field
Scheduled status	"Available" if user is scheduled and on duty, "n/a" if not on duty or not scheduled
Online status	"Online" if user is logged on to KNM

Example

Admin | Robert | 0611-22334 | | Box 277 | 871 31 Härnösand Sweden | n/a | Online

test_status

The `test_status` command returns the overall status of all the monitors.

Syntax

```
http://localhost/knm/extract.xsi?cmd=test_status&user=Admin
```

cmd	test_status
user	KNM user username

Returned data

A string containing the current test status. The status indicates if there is at least one or more monitors in failed or alarm state.

Example

ALARM

version

The `version` command returns the current **Network Monitor** version number.

Syntax

```
http://localhost/knm/extract.xsi?cmd=version&user=Admin
```

cmd	Version
user	KNM user username

Returned data

A string containing the version number of **Network Monitor**.

Example

7.0

UNIX system support files

The system type determines which types of monitors are available to the asset and how they perform the test.

Network Monitor supports all built-in Windows system types. New *system types* can be created using a set of configuration files located in the `KNM\system` folder of the KNM host machine.

Note: This topic focuses mainly on UNIX, but its instructions can be used with any system type that has shell access through SSH or telnet.

System specification

To support monitoring of a disk, CPU, swap and so on, **Network Monitor** log in using either SSH or telnet, runs a command on the UNIX host and parses the result. What command and how the result is parsed is described in configuration files in the `KNM\system` folder.

All system specifications inherit the one labeled `Generic UNIX`. So it is only necessary to write parsing information for those commands that are different from the ones specified in the `Generic UNIX` system type.

Generic UNIX system definition file

```
<system name="Generic UNIX" release="" author="Kaseya" type="unix" internalID="5" fileRevision="1">
  <parsing>
    <!-- disk -->
    <disk>
      <!-- enumeration of disk volumes -->
      <enumeration>
        <query>
          <command>df</command>
          <enumList startLine="2">
            <value id="diskVolume" field="1" />
          </enumList>
        </query>
        <result id="volumeID">diskVolume</result>
      </enumeration>
      <!-- monitoring disk volumes-->
      <monitoring>
        <!-- free and used disk space -->
        <diskSpace>
          <query>
            <command>df -k $volume</command>
            <value id="freeSpace" line="-1" field="-3"/>
            <value id="usedSpace" line="-1" field="-4"/>
          </query>
          <result id="freeSpace" unit="MB">freeSpace / 1024</result>
          <result id="usedSpace" unit="MB">usedSpace / 1024</result>
        </diskSpace>
      </monitoring>
    </disk>
    <!-- cpu -->
    <cpu>
      <!-- enumeration of CPU's -->
      <enumeration>
        <query>
```

Advanced Topics

```
<command>mpstat -P ALL</command>
<enumList startLine="5">
  <value id="cpuNumber" field="3" />
</enumList>
</query>
<result id="cpuID">cpuNumber</result>
</enumeration>
<monitoring>
  <!-- utilization of given CPU-->
  <cpuUtilization>
    <query>
      <command>mpstat -P $cpu 2 2</command>
      <value id="userLoad" line="-1" field="-9"/>
      <value id="systemLoad" line="-1" field="-7"/>
    </query>
    <result id="cpuAverageLoad" unit="%">userLoad + systemLoad</result>
  </cpuUtilization>
  <!-- overall system CPU load, used if a CPU is not specified -->
  <cpuAverageLoad>
    <query>
      <command>vmstat 2 2</command>
      <value id="userLoad" line="-1" field="-5"/>
      <value id="systemLoad" line="-1" field="-4"/>
    </query>
    <result id="cpuAverageLoad" unit="%">userLoad + systemLoad</result>
  </cpuAverageLoad>
</monitoring>
</cpu>
<!-- processes -->
<process>
  <!-- process enumeration -->
  <enumeration>
    <query>
      <command>ps -awxu</command>
      <enumList startLine="2">
        <value id="processName" field="11" />
      </enumList>
    </query>
    <result id="processName">processName</result>
  </enumeration>
  <monitoring>
    <!-- checks if a given process is running -->
    <processRunning>
      <query>
        <command>ps -awxu</command>
        <value id="processName">
          <match type="line">$process</match>
        </value>
      </query>
      <result id="processName">processName</result>
    </processRunning>
  </monitoring>
</process>
<!-- swap -->
<swap>
  <monitoring>
    <swapUtilization>
      <query>
        <command>free -m</command>
        <value id="swapUsed" line="-1" field="-3"/>
        <value id="swapFree" line="-1" field="-2"/>
      </query>
      <result id="swapFree" unit="MB">swapFree</result>
      <result id="swapUsed" unit="MB">swapUsed</result>
    </swapUtilization>
  </monitoring>
</swap>
<!-- memory usage -->
<memory>
```

```

<monitoring>
  <!-- free and used memory -->
  <freeMemory>
    <query>
      <command>free -m</command>
      <value id="freeMem" line="3" field="-1"/>
      <value id="usedMem" line="3" field="-2"/>
    </query>
    <result id="freeMemory" unit="MB">freeMem</result>
    <result id="usedMemory" unit="MB">usedMem</result>
  </freeMemory>
</monitoring>
</memory>
<!-- file change -->
<file>
  <monitoring>
    <fileChange>
      <query>
        <command>ls -l --full-time $filename</command>
        <value id="fileSize" line="1" field="5"/>
        <value id="fileDate" line="1" field="6"/>
        <value id="fileTime" line="1" field="7"/>
      </query>
      <result id="fileSize" unit="B">fileSize</result>
      <result id="fileDate">fileDate</result>
      <result id="fileTime">fileTime</result>
    </fileChange>
  </monitoring>
</file>
</parsing>
</system>

```

Enabling the ODBC Driver

Enabling the ODBC driver in the standalone edition of **Network Monitor** allows you to run SQL queries against the **Network Monitor** data.

Prerequisites

- Make sure "Microsoft Visual C++ 2010 Redistributable Package (x86)" and/or "Microsoft Visual C++ 2010 Redistributable Package (x64)" is installed on the KNM host machine.

Installation

On the VSA / Network Monitor Server Machine

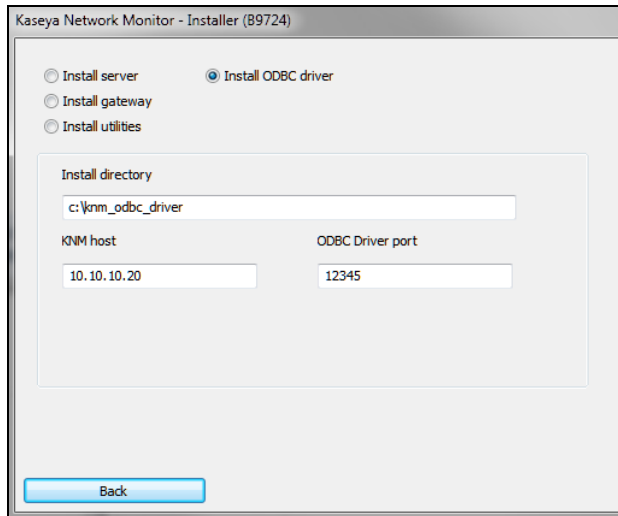
1. Open `cmd.exe` in administrators mode.
2. Change directory to the `knm` root directory.
3. Change directory to the `dsii_driver` directory under the `knm` root directory.
4. Install the KNM ODBC driver with the following command:
`dsii_driver.exe -Install`
5. Open the service control manager and make sure the "`KNM5DSIIService`" is started and set to "automatic" startup.
6. Create or identify the **API Key** associated with any **Network Monitor** user. This field is located on the Network Monitor > Users > My settings > **Basic properties tab** (page 100).

Note: Enter the API Key as the username used to authenticate with, when making an ODBC connection to the **Network Monitor** server. The authentication password can be any string.

On the Local Machine

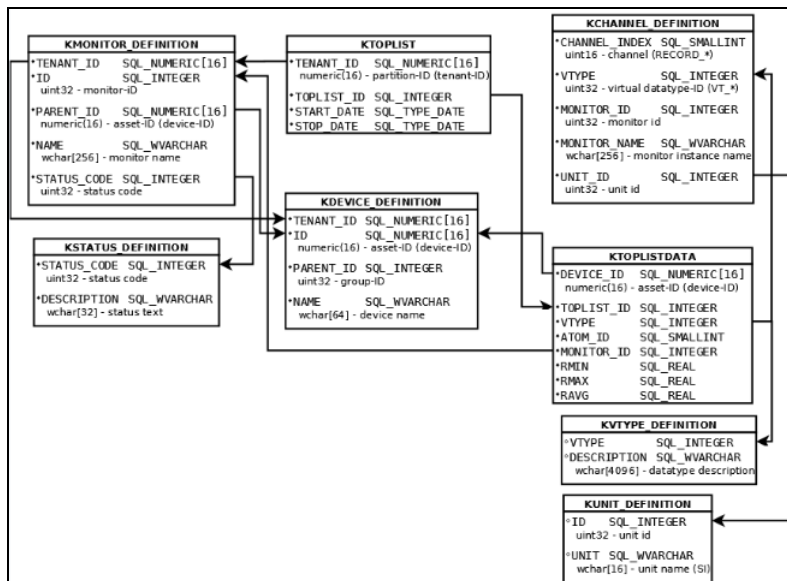
Advanced Topics

- Copy the knmsetup.exe installer file from <Kaseya_Installation_Directory>\KNM\Install directory to your local machine.
- Run knmsetup.exe on your local machine a select the **Install ODBC driver** option.
- When installing, enter the KNM host machine IP number in the KNM host field and keep the port number to the default port 12345.



- When the installation is done you should be able to do queries of the following tables.

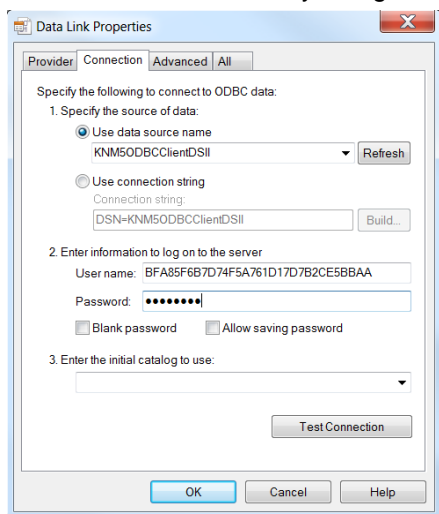
CHANNEL_DEFINITION
 ASSET_DEFINITION
 GROUP_DEFINITION
 MONITOR_DEFINITION
 STATUS_DEFINITION
 UNIT_DEFINITION
 VTYPE_DEFINITION
 TOPLIST
 TOPLISTDATA



Example: Querying Network Monitor Using Excel 2010

- Display a blank worksheet in *Excel 2010*.

2. Select the **Data > From Other Sources > From Data Connection Wizard** option.
3. Select the **ODBC DSN** option.
4. Select the **ODBC Data Source** for **Network Monitor**. By default this name is **KNM50DBCCClientDSII**.
5. Select the following data source properties.
 - **Use data source name** - **KNM50DBCCClientDSII**
 - **User name** – Enter the **API key** for any user in your Network Monitor server. An **API key** is created or identified using the > Users and user groups > Create a new user > **Basic properties tab** (page 100).
 - **Password** – Enter any string.



6. Select the **Network Monitor** table you want to create a data connection with.
7. Save the data connection file. This enables you to reuse the data connection later.
8. Select how you want to view the data in your workbook, and the starting cell.
9. Review the **Network Monitor** now displayed in the spreadsheet.
10. From now on, you can click **Refresh** (Alt+F5) to update the **Network Monitor** data displayed in the spreadsheet.

Chapter 6

Windows Troubleshooting and Performance Monitoring

In This Chapter

Troubleshooting Windows monitoring and authentication	173
Windows performance registry	176
Windows Management Instrumentation (WMI)	178

Troubleshooting Windows monitoring and authentication

Network Monitor is capable of *agent-less* monitoring of remote Windows workstations and services. The prerequisite for monitoring a remote asset is a successful authentication with a Windows account that has access to a number of different resources on the monitored asset.

There are a number of different problems that can arise. This section addresses the most common issues.

Warning: This section is provided as a troubleshooting reference and Kaseya can not guarantee that these problems can be solved. All modifications done to the system, including modifying the registry is done at your own risk.

Network Monitor Service account and rights assignment

If the Kaseya Network Monitor service is running under a user account other than LocalSystem, ensure the following local security policies are enabled for the service account.

- Log on as a service
- Act as part of the operating system (Windows 2000)
- Bypass traverse checking
- Read, write and execute rights on the KNM folder of the KNM host machine.

To make full use of the built-in account manager, all assets should be assigned an account other than the base service account.

Monitoring accounts

With **Network Monitor** you have the ability to assign a default account to each asset. This account is used to authenticate access to the monitored asset.

In the following documentation we refer to this account as the *monitoring account*. In the **Edit asset** (page 47) page its called the **Default account**. In the Edit monitor page the account selection option should be set to **Use asset default account**.

The monitoring account should be a member of the Administrators group on the asset being monitored. In most cases this is the Domain Admin group.

Account username format

Depending on the location of the monitoring account **Network Monitor** requires you to format the username according to the following rules. These rules also apply to Windows in general.

- `.\username` - Account is found by **Network Monitor** on the local machine.
- `username` - Account is found by **Network Monitor** on the local machine.
- `domain\username` - Account is found by **Network Monitor** using the domain name.
- `username@domain.com` - Same as above but valid for XP, 2003 and Vista.

Monitors using Windows authentication

The following monitors all require Windows authentication:

- CPU utilization
- Disk utilization
- Memory utilization
- Swap file utilization
- Process
- Windows performance
- WMI

These monitors use the remote registry service to query the monitored asset. Ensure that the remote registry service is running on both the monitored asset and the **Network Monitor** host.

By default, only administrators can access the remote registry. This is controlled by the registry key.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg`

You can edit the permissions of this registry key to limit or grant access to the remote registry. If the key does not exist, access is granted to everyone.

A special case exists for the `Disk utilization` monitor in compatibility mode. In this case, you need to specify the default share representing the monitored disk. For example, instead of specifying `C:` you should specify `C$` and ensure that this default share exists and is accessible by the monitoring account.

Event log monitor

By default, everyone can read the eventlog, except the `Security` eventlog. To read the `Security` eventlog the user must be a member of the administrator group. Access to different event logs are controlled by this registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog`

You can edit the permissions of this registry key to limit or grant access to the remote eventlog.

Service monitor

This monitor uses the Remote Procedure Call (RPC) service to query the status of a service running on the monitored machine. Ensure the Remote Procedure Call (RPC) service is running on the monitored asset and the **Network Monitor** host. The monitor account must be an administrator on the monitored host to gain access to the service manager.

External resources

Warning: These links are only provided as a reference. All modifications to the system, including modifying the registry is done at your own risk.

- **How to restrict access to the registry from a remote computer**
(<http://support.microsoft.com/kb/153183/en-us>)

- **Removing the Everyone Group from Group Policies in the Remote Registry Services Permanently Removes All Access** (<http://support.microsoft.com/kb/281641/en-us>)
- **A custom program that uses the RegConnectRegistry function can no longer access the registry of a remote computer in Windows Server 2003 with Service Pack 1 or in an x64-based version of Windows Server 2003** (<http://support.microsoft.com/kb/906570>)
- **Controlling remote Performance Monitor access to Windows NT servers** (<http://support.microsoft.com/kb/164018/en-us>)
- **Troubleshooting Performance Monitor Counter Problems** (<http://support.microsoft.com/kb/152513/en-us>)
- **"Unable to complete the operation on <event log>. Access is denied." error message when you try to access a log on a Windows Server 2003-based computer** (<http://support.microsoft.com/kb/888189/en-us>)
- **Error message when you try to make a remote connection to the registry of a Windows-based computer from a Windows Server 2003 SP1-based computer: "Access denied"** (<http://support.microsoft.com/kb/913327/en-us>)

Troubleshooting

This section describes how to troubleshoot some common problems related to Windows authentication.

Access denied

Occurs as either a spontaneous error or as a permanent error when monitoring an asset.

Access denied.

Cause

Access to the monitored asset is denied. This can be caused by an authentication failure or the monitored asset is too busy serving new requests.

Resolution/workarounds

- Ensure that the monitoring account has access rights to the monitored asset. In most cases this error is caused by the **Network Monitor** monitoring account not being an administrator on the monitored asset.
- Increase the test interval of the monitor.
- Use the **Alarm filtering** features in the monitor to filter out non-threshold errors.
- Firewall restrictions prevents **Network Monitor** from accessing the monitored asset. This error can be resolved by unblocking port 445 to the monitored asset.

Network path can not be found

Occurs as either a spontaneous error or as a permanent error when monitoring an asset.

The network path was not found.

Cause

The network path could not be found or accessed because of firewall restrictions, a name resolution error or a network error.

Resolution/workarounds

- DNS server is overloaded and can not translate the asset address. Try entering the IP number as the asset address.
- Firewall restrictions prevent **Network Monitor** from accessing the monitored asset. This error can be resolved by unblocking port 445 to the monitored asset.

- If the monitor is a `Disk utilization` monitor and you are running in Win32 compatible mode, ensure that the share is available. If you want to directly monitor a disk rather than a share, use the default share name of the disk (e.g. `C$`) instead of the volume name (e.g. `C:`).

Performance related issues with monitored asset

Spontaneous errors occur during specific times of the day or other patterns occur, such as when backup starts or large queries run in a database on the monitored asset.

Cause

The monitored asset may be unable to complete requests from **Network Monitor** since it's busy performing other tasks. The problem can also be network bandwidth related. For example monitoring assets over an VPN connection can severely degrade network performance and latency. The error messages can vary but most commonly they are all related to RPC failures.

Resolution/workarounds

- Lower the test frequency to 300 seconds
- Set the **Alarm generation** value to at least 5 to filter out false positives
- Use the **Alarm filtering** features in the monitor to filter out non-threshold errors.
- If low network bandwidth or high network latency is a factor, a gateway can be placed closer to the monitored asset. A gateway uses only a fraction of the network bandwidth that a normal test does.

The RPC server is unavailable

Errors occur either randomly or all the time with the following error text.

The RPC server is unavailable

Cause

The most common cause for this problem is that the remote registry of the monitored machine is either stopped or has experienced problems accepting new connections.

Resolution/workarounds

- Restart the remote registry service of the monitored asset.
- Review the assets overall performance. The asset might be too busy to serve more connections.
- Use the Alarm filtering features in the monitor to filter out non-threshold errors.
- Check the DNS entry for the monitored asset, confirm that both a forward and reverse zone entry exists.

Windows performance registry

The Windows performance register is a virtual registry hive that contains performance metrics from a number of installed providers. All the communication with the performance registry is done via the remote registry service.

The following monitors can use the Windows performance registry

- Windows performance monitor
- CPU monitor
- Memory monitor
- Swap size monitor
- Bandwidth monitor
- Disk monitor

All monitors, except the Windows performance monitor, can be forced to use WMI, by checking **Use**

WMI checkbox in the **Asset property** page.

Advanced properties (Click to expand/hide)

Simple maintenance: -

Day of week: ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Time zone:

Root monitor:

SNMP port:

Favourite: ☐

No SSH2 con. sharing: ☐

No inspection: ☐

Use WMI: ☒

Wake-On-LAN:

Specify maintenance period for this object here in HH:MM format. This period can wrap to the next day if needed. Select which day(s) of the week the maintenance schedule will be active.

Time zone where object is located. Selecting a timezone will cause realtime charts in this object to be displayed in the object's local time. Root monitor in a local dependency tree. Select the monitor which all other monitors in this object will be dependent on. If this is a template, the dependency tree will be inherited. Connection port for SNMP communication.

Tag as a favourite.

Disable the use of persistent SSH2 connections for this object.

Disable automatic object inspection on this object.

Use WMI for performance monitoring on this object.

If you want to specify actions to send Wake-On-LAN packets to this machine, specify the MAC-address of the interface you wish to send those packets to here. Format is AA-BB-CC-DD-EE-FF.

Subtopics

- **How to verify that KNM have access to remote registry service** (page 177)
- **Memory leaks in remote registry service on monitored machine** (page 177)
- **Caching of counters** (page 178)

How to verify that KNM have access to remote registry service

1. Logon to the KNM host machine using the Windows account used to monitoring
2. Start the 32 bit version of the `perfmon.exe` application. This file is located in the `SysWOW64` directory on a 64 bit host machine.
3. Connect to the monitored machine and add a counter.

If this test fails, **Network Monitor** will not succeed in enumerating and sampling counters on the monitored machine.

1. Check that firewall is opened for Remote Administration in the correct profile.
2. Make sure the Remote registry service is running on the monitored machine
3. Verify that the account is allowed to access the performance counter hive. See <http://support.microsoft.com/kb/300702/en-us> (<http://support.microsoft.com/kb/300702/en-us>).
4. If its a standalone Vista/7 machine (not in a domain) you have to disable UAC to prevent it from filtering out the credentials. See <http://support.microsoft.com/kb/951016> (<http://support.microsoft.com/kb/951016>).
5. If counters are missing, and you have verified that the same counters are missing in the `performon.exe` tool, the performance counter library might need to be rebuilt. See <http://support.microsoft.com/kb/300956> (<http://support.microsoft.com/kb/300956>).
6. If counters still are missing the counters may be published by a 64 bit dll, **Network Monitor** is a 32 bit application and cannot yet read 64 bit counter values. User have either to install a 32 bit version of the dll or use WMI to query the counter.

Memory leaks in remote registry service on monitored machine

Since the performance registry hive is loading external executable code to publish performance data to consumers—for example, **Network Monitor**—there might be problems with the loadable modules, such as memory leaks and lock ups.

This can result in low memory conditions for the monitored machine.

As its impossible for us to fix the problematic dlls, other than search for newer version of the program, the only thing we can recommend to the user is to create a Scheduled event that restarts the remote registry service on the monitored machine every 24 hours.

Caching of counters

When the monitor of an asset performs its first test after restarting, it caches all the counter and [Winperf] asset names to improve the bandwidth usage for all subsequent tests performed against the asset.

This can be a problem if the user installs a new piece of software on the monitored machine that publishes additional performance counters, after **Network Monitor** has tested a Windows performance monitor against it. The problem manifests itself as "missing counters" when **Network Monitor** enumerates the counters, but the counters are visible in the `perfmon.exe` tool.

To reset the cache the user needs to open up the **Network Monitor System admin** console from the **Tools** menu. The user needs to be system admin to see the menu entry. Issue the following command:

```
clear-counter-cache <asset>
```

OBJECT_NAME is the exact name of the asset that is having its cache reset.

Windows Management Instrumentation (WMI)

WMI is used by default by all Windows performance monitors when creating a new asset. The WMI protocol has an advantage over older Windows performance registry calls, being more bandwidth effective. However, on some platforms like Windows Vista and Windows 2008 (without any service packs), WMI has a high performance impact and therefore Winperf may be preferred when monitoring these two platforms.

For inexperienced system administrators, WMI has a history of being hard to configure for remote monitoring.

WMI Troubleshooting

This article describes common problems with Windows performance monitoring and how to resolve it.

Background

The following error message is displayed

```
Access denied. User may lack remote launch and remote activation permission.
```

The following monitor types use WMI when the asset flag **Use WMI** is checked.

- WMI Query monitor (*)
- Active directory monitor(*)
- Bandwidth monitor
- CPU monitor
- Disk monitor
- Memory monitor
- Swap monitor

* Always use WMI

This error message is displayed when:

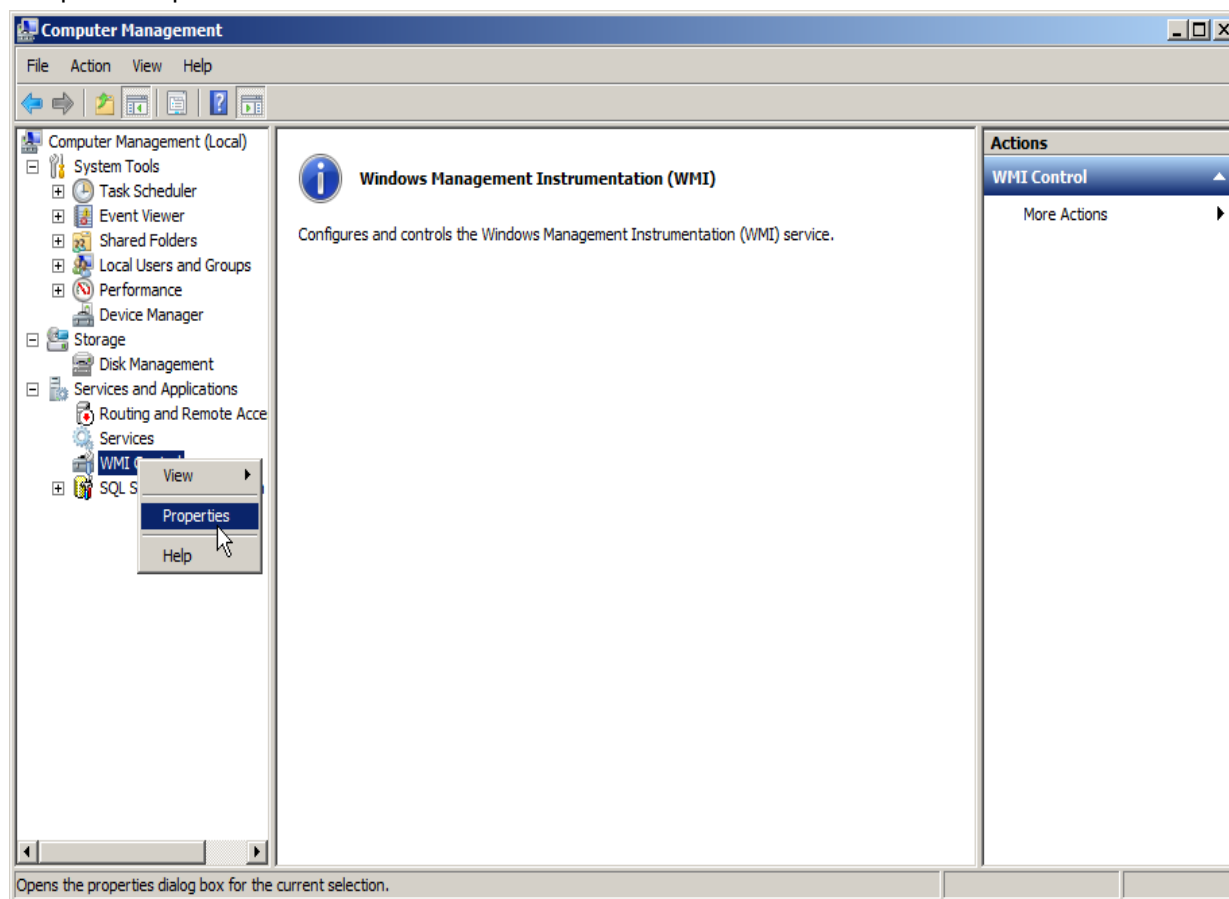
- The user account used is not enabled to use WMI in the domain or on the monitored machine.
- The firewall is closed.
- The user is not an administrator on the monitored machine.

Subtopics

- **Verifying that WMI is enabled for the account** (page 179)
- **Adjusting the firewall settings** (page 181)
- **Additional for non-administrator users** (page 181)
- **Verifying that WMI works** (page 181)
- Problem with data returned from performance counters read by WMI
- **Full index of Microsoft WMI troubleshooting articles** (page 183)

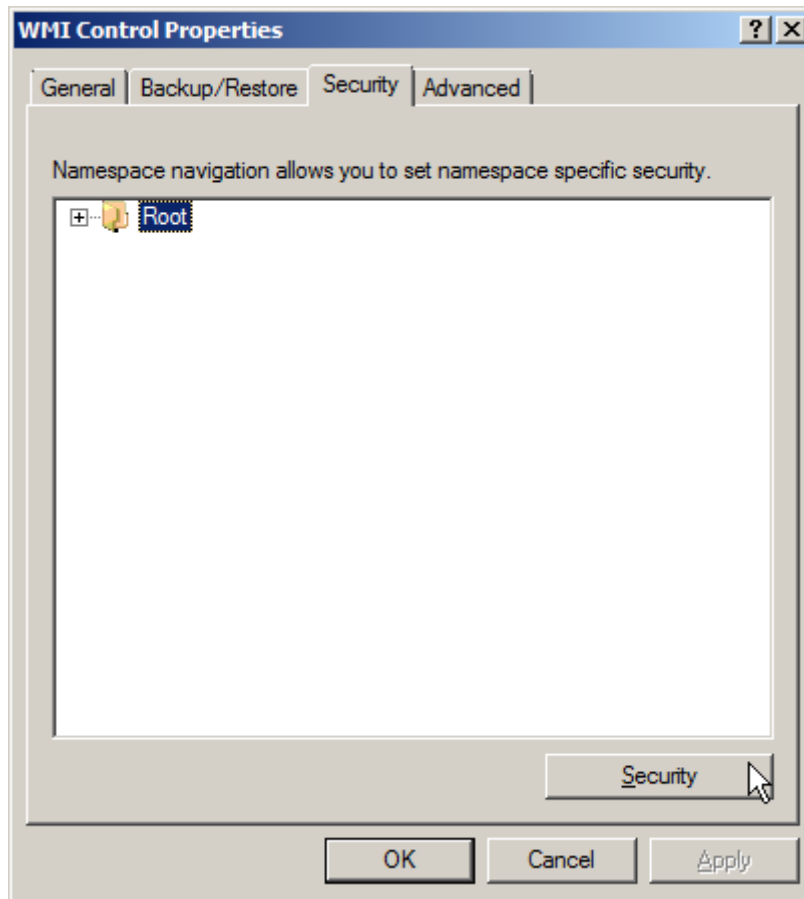
Verifying that WMI is enabled for the account

Open Administrative tools > Computer management, right click "WMI Control" to select the "Properties" option.

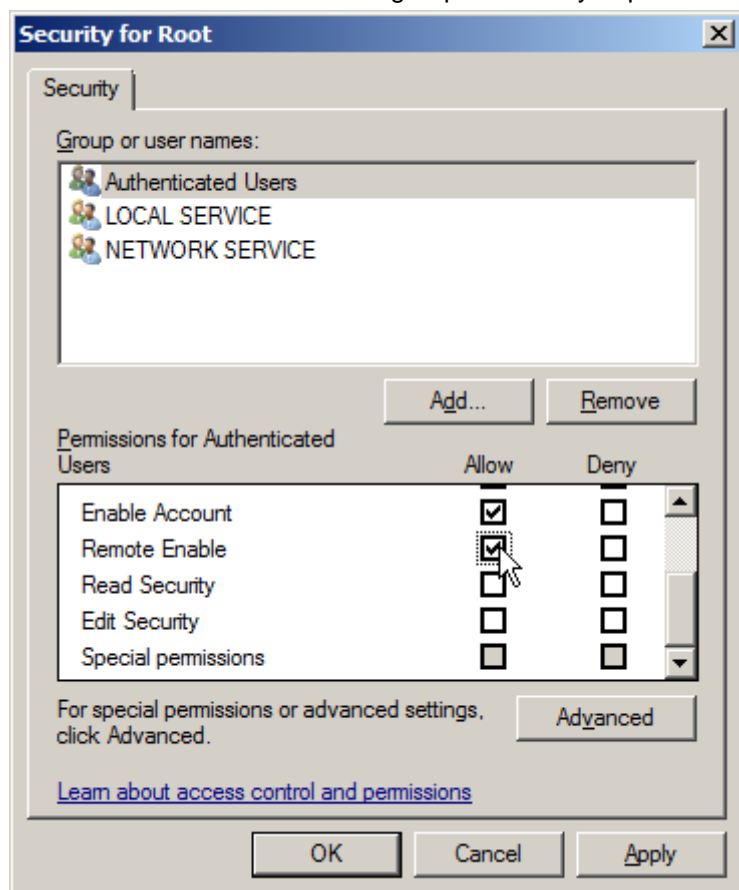


Windows Troubleshooting and Performance Monitoring

Select the security tab and click "Security".



Enable "Remote enable" for the group/user that you plan to use.



Click "Apply" and close the dialog.

Adjusting the firewall settings

Open the command prompt, as administrator, and execute the following command to enable the inbound rule for WMI.

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)"
new enable=yes
```

Additional for non-administrator users

Enable the non-administrator to interact with DCOM by following the simple steps listed in the following MSDN article.

- <http://msdn2.microsoft.com/en-us/library/Aa393266.aspx>
(<http://msdn.microsoft.com/en-us/library/aa393266.aspx>)

In the article, follow the steps to:

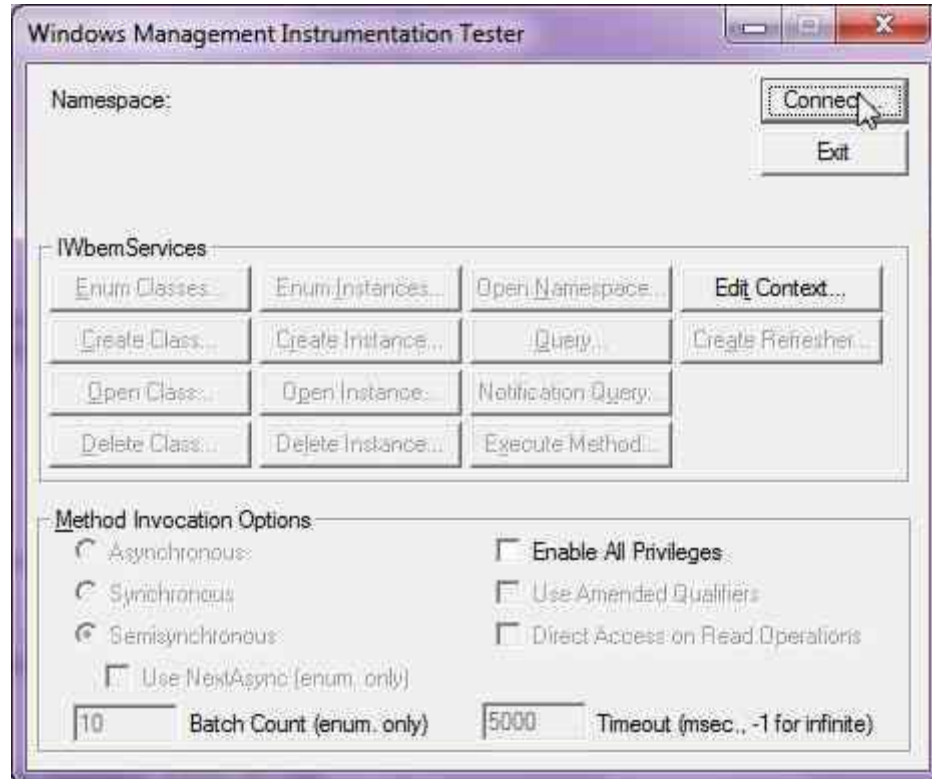
- Grant DCOM remote launch and activation permissions for a user or group.
- Grant DCOM remote access permissions.

Verifying that WMI works

The `wbemtest.exe` utility can be used to verify that its possible to make a WMI call to the monitored machine from the KNM host machine. To start the utility, logon to the KNM host machine desktop and open the start menu, in the "Run" field, type the following and press enter:

wbemtest.exe

When the utility has started, click the "Connect" button.

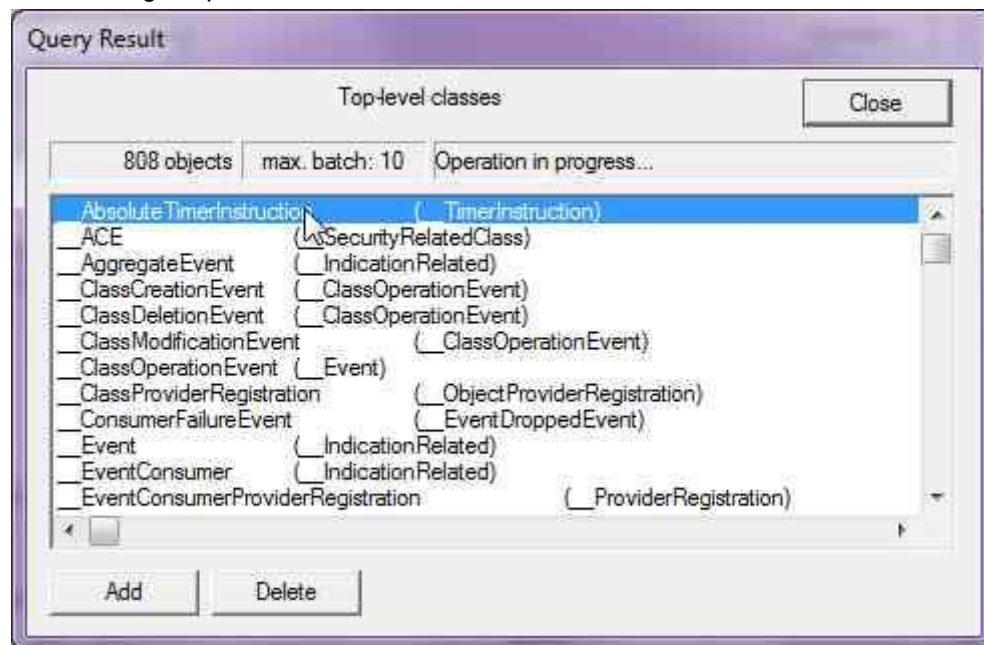


Enter the following address and replace "my_ip" with the IP number of the monitored machine:

\\my_ip\root\cimv2

Enter the username and password that you use in KNM. In the Authority field, enter the domain name of the user. Click "Connect" and then "Enum classes".

In the dialog "Superclass info", click the recursive radio button and click ok.



The utility now populates the Query result window with information from the monitored machine. If this

does not happen, consult the following troubleshooting information on Microsoft support web site.

Problem with data returned from performance counters read by WMI

Sometimes the performance register and WMI can become out of sync or the process that collects performance data for WMI can hang on a locked resource.

As a last resort after rebooting the monitored machine, resync the performance counters to WMI using the steps outlined in this article.

- <http://support.microsoft.com/kb/266416> (<http://support.microsoft.com/kb/266416>)

Full index of Microsoft WMI troubleshooting articles

- <http://msdn.microsoft.com/en-us/library/msaspx>
(<http://msdn.microsoft.com/en-us/library/ms735120.aspx>)
- <http://msdn.microsoft.com/en-us/library/aa394603.aspx>
(<http://msdn.microsoft.com/en-us/library/aa394603.aspx>)
- <http://msdn.microsoft.com/en-us/library/Aa393266.aspx>
(<http://msdn.microsoft.com/en-us/library/aa393266.aspx>)
- <http://support.microsoft.com/kb/266416> (<http://support.microsoft.com/kb/266416>)
- <http://support.microsoft.com/kb/300956> (<http://support.microsoft.com/kb/300956>)
- <http://support.microsoft.com/kb/300702/en-us> (<http://support.microsoft.com/kb/300702/en-us>)
- <https://social.technet.microsoft.com/Forums/windows/en-US/8ed26d46-9994-4052-a307-5b071805aea8/wmi-corrupt-how-to-reinstallrepair>
(<https://social.technet.microsoft.com/Forums/windows/en-US/8ed26d46-9994-4052-a307-5b071805aea8/wmi-corrupt-how-to-reinstallrepair>)
- <http://support.microsoft.com/kb/951016> (<http://support.microsoft.com/kb/951016>)

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."

Chapter 7

Utilities Reference

In This Chapter

Utilities Overview	185
Compiling Custom MIB Files	185
Lua	186
Gizmo	188
Dashboard Map Editor	189

Utilities Overview

Four additional utilities are installed when you install **Network Monitor**. These utilities are not required to use **Network Monitor**. These are located on the Network Monitor > Tools > [Utility downloads](#) page.

- **DME** - The **Dashboard Map Editor** (page 189).
- **Gizmo** - The **Gizmo** (page 188) system tray application.
- **MIB compiler** - The **MIB Compiler** (page 94) utility.
- **Lua IDE** - The **Lua** (page 186) Development Environment

Compiling Custom MIB Files

By using the MIB compiler you can compile text MIB files into a binary format that **Network Monitor** can read. Compiling MIB files requires understanding about how MIB files work as well as a general understanding of SNMP and **MIB objects** (page 93). A number of different RFC documents outline the fundamental base that all other MIB files are based on.

Note: The community name, SNMP version, and port used by **Network Monitor** to connect to an SNMP asset is set on the **Authentication** (page 40) tab of an asset node. The asset node may inherit this setting from a parent node. See the **Installation Checklist** (page 9).

As an example, this is the compile order of a CISCO ® product MIB.

1. `SNMPv2-SMI.mib`
2. `SNMPv2-TC.mib`
3. `SNMPv2-MIB.mib`
4. `RFC1213-MIB.mib`
5. `IF-MIB.mib`
6. `CISCO-SMI.mib`
7. `CISCO-PRODUCTS-MIB.mib`
8. `CISCO-TC.mib`

The first 5 files in this example are common for most product MIB files, and are included in the default `knm.mib` binary MIB file.

Warning: All of these files must be compiled at the same time, otherwise the MIB compiler fails due to unresolved symbols.

Contents of the default KNM MIB file

The default `knm.mib` file included in the installation contains the following base OIDs (object identifiers).

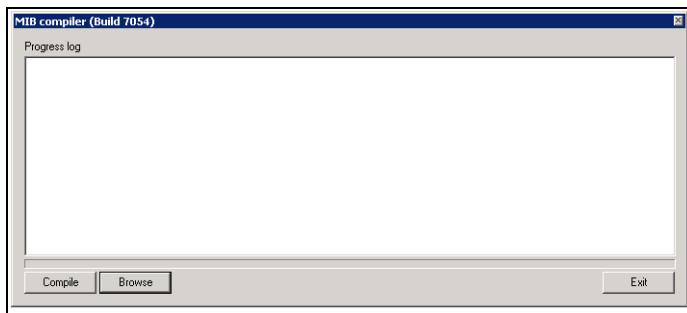
- `iso.org.dod.internet.directory`
- `iso.org.dod.internet.mgmt`
- `iso.org.dod.internet.experimental`
- `iso.org.dod.internet.private`
- `iso.org.dod.internet.security`

The file is located in the `\<Kaseya_Installation_Directory>\KNM\mibs` directory.

Download and Run the MIB Compiler

1. Navigate to the Network Monitor > Tools > [Utility downloads](#) page.
2. Click the [MIB compiler](#) link to download the utility to your local machine.
3. Run the utility.

Compiling a MIB file



1. Start the `<Kaseya_Installation_Directory>\knm\mibcompiler.exe`.
2. Click the [Browse](#) button to select one or more `*.mib` files.
 - Locate the default `knm.mib` file in the `KNM\mibs` folder of the **Network Monitor** host machine and double click it to select it.
 - Select any additional `*.mib` files you want to include for compiling.
3. Click the [Compile](#) button.
4. Specify where where you want to save the compiled `*.dat` file.
5. Click the [Browse](#) button to select the `*.dat` file that was just compiled. An interactive MIB tree displays in the main window. You can use it to navigate through the different OIDs.
6. Move or copy the compiled `*.dat` file to the `KNM\mibs` folder.

Lua

Lua is a powerful light-weight programming language designed for extending applications. Lua is also frequently used as a general-purpose, stand-alone language. Lua is free software. Lua combines simple procedural syntax with powerful data description constructs based on associative arrays and extensible semantics. Lua is dynamically typed, interpreted from byte codes, and has automatic memory management with garbage collection, making it ideal for configuration, scripting, and rapid

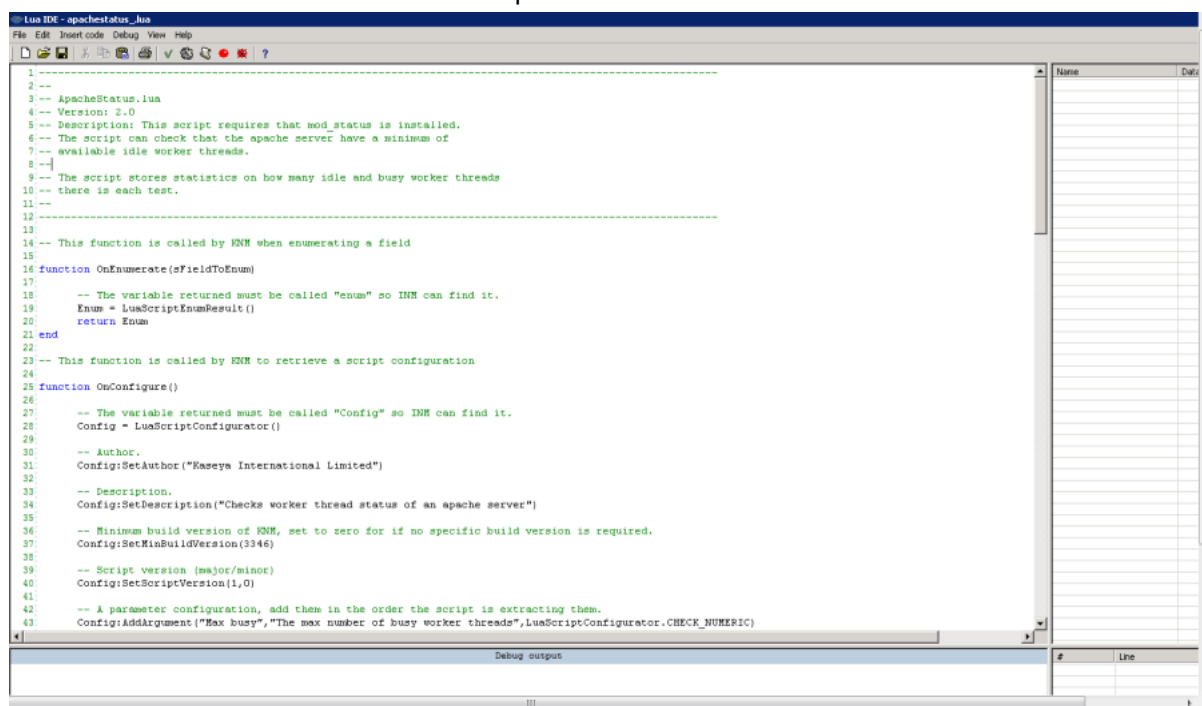
prototyping.

Network Monitor and Lua

Network Monitor includes support for the Lua scripting language (www.lua.org).

- Customers can create custom made monitors to test systems and equipment not supported by any current monitoring solution.
- New monitors, actions and events can be created and tested in the development environment provided by Kaseya, before they are exported and used in **Network Monitor**.
- A comprehensive library of pre-made classes, such as FTP clients, HTTP clients and file management, are available to developers. See the **KNM API documentation** (<http://help.kaseya.com/webhelp/EN/knm/9000000/api/index.asp#home.htm>) for more information about the different pre-made classes.

The development environment includes debugger, keyword highlighting, integrated help and other features available in state-of-the-art development tools.



Download and Run the Lua IDE

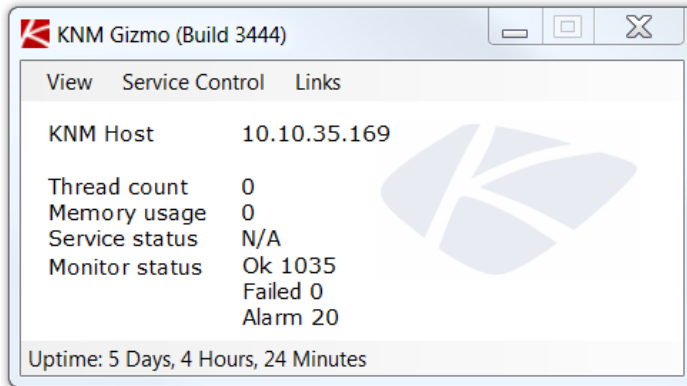
1. Navigate to the Network Monitor > Tools > **Utility downloads** page.
2. Click the **Lua IDE** link to download the utility to your local machine.
3. Run the utility.

Lua modules included in KNM

- Base
- Math
- String
- Table

Gizmo

Gizmo is a small system tray application that can be installed on your workstation.



Features

- Alarm notification
- Network Monitor log viewer
- Start/stop Network Monitor
- Statistics, including Network Monitor memory usage, cpu usage and uptime

Requirements

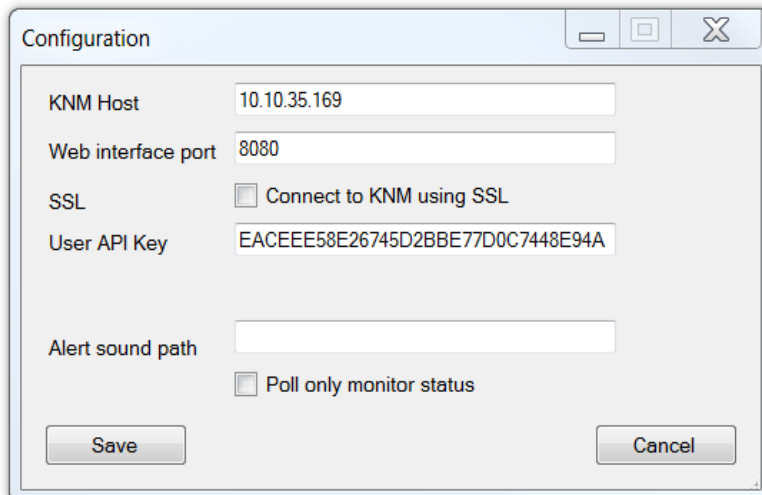
- Net 2.0 Runtime installed

Download and Run Gizmo

1. Navigate to the Network Monitor > Tools > [Utility downloads](#) page.
2. Click the [Gizmo](#) link to download the utility to your local machine.
3. Run the utility.

Gizmo configuration

Before you can start using Gizmo you need to configure the application. Select [View > Configure](#) and enter the following parameters.



- [KNM Host](#) - The DNS name or IP number of the computer hosting **Network Monitor**.

- **Web interface port** - The port number where the **Network Monitor** management interface is accessed. Defaults to 8080.
- **SSL** - Option to connect to **Network Monitor** using SSL. Check this option if your **Network Monitor** installation uses SSL for the management interface.
- **User API key** - Copy and paste your user API key from the Network Monitor User > My settings > Basic properties tab > **API key** field. If no API key value exists yet, click **New** and save the **Edit my settings** page.
- **Alert sound path** - Path to a **.wav** file that contains a sound played when an alarm or error occurs.
- **Poll only monitor status** - Enable this option if the user running Gizmo does not have Windows account administration rights to access the service data base and remote registry of the **Network Monitor** host machine.

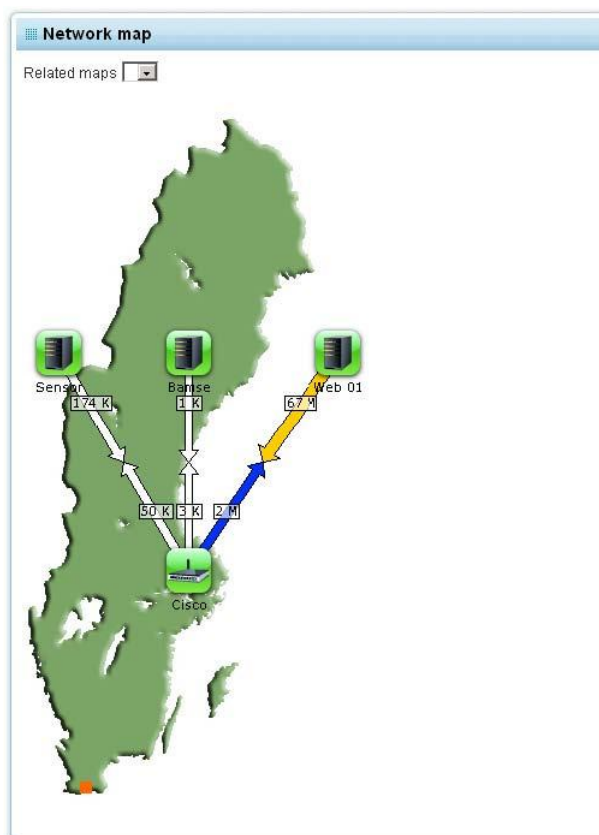
Click the **Save** button to store your settings.

Note: Your Windows account used to run Gizmo requires permission to access the service control manager of the **Network Monitor** host computer. Use the **Poll only monitor status** to work around this requirement.

Dashboard Map Editor

Network Monitor is capable of displaying the status of groups and assets, as well as bandwidth utilization data, in **dashboard** (page 88) *network map* widgets. Network maps are defined and edited in a separate **Dashboard Map Editor** (DME) application.

Note: The Dashboard Map Editor utility requires Microsoft .Net Framework 4.0 or later.



Starting the Map Editor

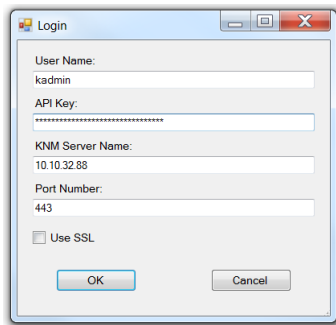
Download and Run the Dashboard Map Editor

1. Navigate to the Network Monitor > Tools > [Utility downloads](#) page.
2. Click the [DME](#) link to download the utility to your local machine.
3. Run the utility.

Logon to the Dashboard Map Editor

Logon to the [Dashboard Map Editor](#) by entering the following:

- **User Name** - Your VSA user name.
- **API Key** - Your API key. This key is set using the Network Monitor > User > My settings > [Basic properties tab](#) (page 100) tab.
- **KNM Server Name** - The address to your **Network Monitor** server.
- **Port** - The port number to use. Defaults to 443.



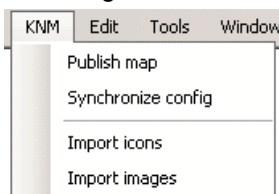
Importing Map Images

Importing Map Graphics

For most network maps you will want to use a background image, such as an image of a geographical location or a drawing of a server hall. First import the image using the editor.

Note: The editor only supports images in the .png (Portable Network Graphics) format. If you have an image that you want to use that is in another format, first convert it using another application.

To import your image, select [Import images](#) from the **KNM** menu. Then select your image file and click **Ok**. The image is sent to the **Network Monitor** server and is available for use in the editor.



Importing Custom Icons

Network Monitor comes with a set of stock icons for use with your network maps, ready for use. It's also possible to import your own custom icons to use as backgrounds for the various entities on network maps.

Note: The editor only supports icons in the .png (Portable Network Graphics) format. If you have an icon that you want to use that is in another format, first convert it using another application.

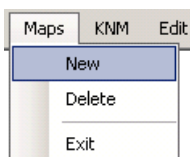
To import a custom icon, select the **Import icons** command from the **KNM** menu. Then select your image file and click **Ok**. The image is sent to the **Network Monitor** server and is available for use in the editor. If your icons are very large, the default method of displaying their status in the background may or may not work well. In such cases, it's recommended that you use the status overlay method described in the **Configuring Maps** (page 191) topic.

Note: For image transparency, it's recommended that your icons use the 32-bit RGBA format with a proper alpha channel.

Configuring Maps

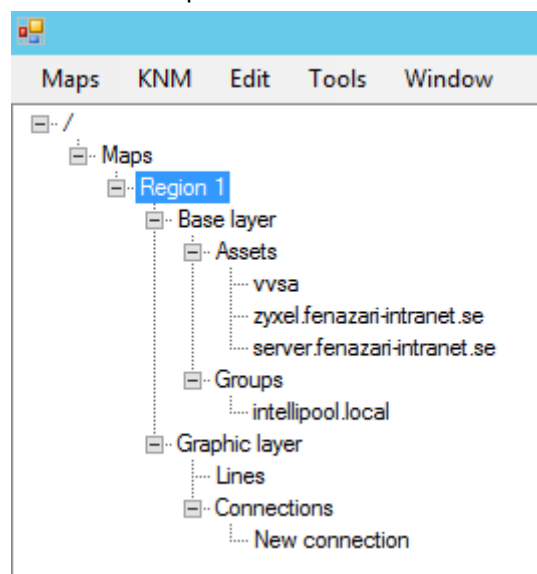
Adding Network Maps

To create a new network map, select the **New** command from the **Maps** menu.



Editing Network Maps

All network maps are listed as child nodes under the **Maps** node in a *map tree*.



Setting Network Map Properties

Click any network map node to set its basic properties. After making changes to map properties, click the **OK** button to see the map updated.

- **Map name** - The name of the network map as displayed in the map tree. For example: **Region 1**.
- **Map image** - The background image to be used in the map. See the **Importing map graphics** (page 190) topic for information on how to import images.
- **Background** - Manually set the **Width**, **Height** in pixels and the **Background** color of the network map.

- **Status rendering** - Defines how **Network Monitor** displays the status of assets and groups on the network map.
 - **Status in background** - Displays the status as a background, with the icon for the entity drawn above it.
 - **Status as overlay** - Displays the icon for the entity with a small status symbol attached to the upper right corner. This method is recommended when using large custom icons.

Deleting Network Maps

To permanently remove a network map from **Network Monitor**, select the **Delete** command from the **Maps** menu.

Editing Map Nodes

Selecting Map Nodes

To select content on the network map, either click directly on the desired entity, or draw a selection rectangle around the content you want to select. The selected content displays with a rectangle around it to indicate that it is currently selected. To select all content on the map, select the **Select all** command from the **Edit** menu, or use the keyboard-shortcut Ctrl+A.

- To add or remove content to your selection hold down the Ctrl key on the keyboard while selecting.
- To clear your selection, click in an open space somewhere in the map.

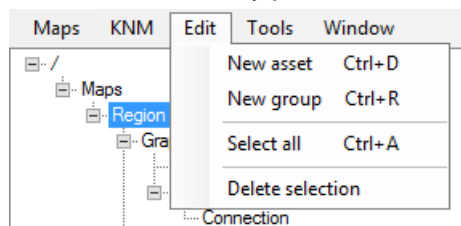
Editing Map Nodes

To change the properties of content on the map, first select it to display the properties window. Make the appropriate changes, depending on what you selected, and click the **OK** button to confirm your changes.

To move content in the map, first select it, then drag it on the map while holding the left mouse button down.

Deleting Map Nodes

To delete content from the map, first select it, then select the **Delete selection** command from the **Edit** menu, or alternatively press the **Delete** key on the keyboard.



Multi-edit of Nodes

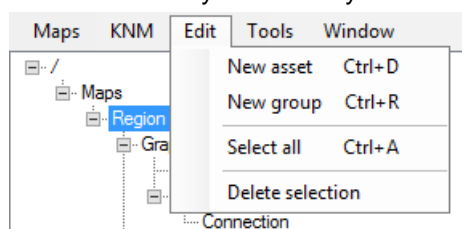
To change the icon used for several entities at once, first select the relevant entities. Then select the desired icon from the properties section. Then click the **OK** button.

Adding Map Nodes

To add a **Network Monitor** group or asset to the network map, select **New group** or **New asset** from the **Edit** menu.

- Alternatively use the keyboard-shortcut Ctrl+N for a new group.

- Alternatively use the keyboard-shortcut Ctrl+O for a new asset.



The editor places a **Network Monitor** group or asset on the map at a default position. *Hint: when using the keyboard-shortcut the new group is placed at the current mouse cursor position.* The properties of the group or asset are visible in the **Properties** section.

The following properties can be modified for a selected group or asset.

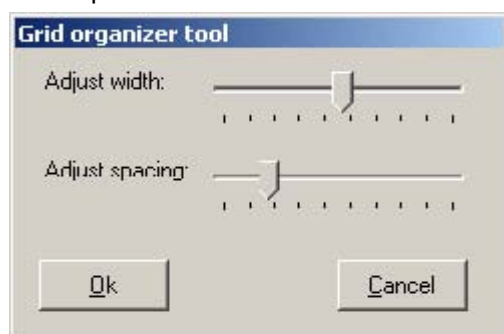
- **Group or Asset** - Select the **Network Monitor** group or asset to be displayed on the map.
- **Icon** - The icon to be displayed for the group or asset. You can select from stock icons or custom icons. See [Importing custom icons](#) for more information.
- **Position** - Manually set the position of the group or asset by specifying an X and Y coordinate.
- **Link properties** - Specify what happens when a user clicks on the group or asset from the **Network Monitor** dashboard.
 - **No link** - Nothing happens when the group or asset is clicked.
 - **Link to group** - Displays the View tabs of the specified group or asset in **Network Monitor**.
 - **Link to map** - Displays the specified map, enabling the creation of "drill-down" maps.

Using the Organizer Tools

Selected content in the map can be organized by using two tools, the **Grid organizer tool** and the **Circular organizer tool**. To access the tools, right-click in the map window after selecting the desired content and select either tool from the **Organize selection** popup menu.

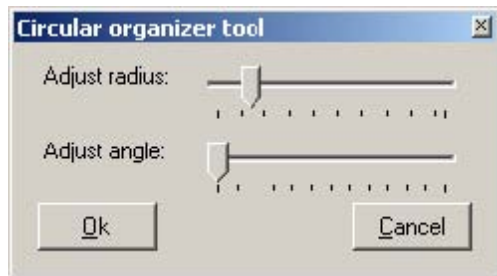
The Grid Organizer Tool

This tool is used to arrange the selected nodes neatly in a grid. Use the two slider controls to modify the width of the grid as well as individual spacing between entities. Changes are reflected immediately in the map.



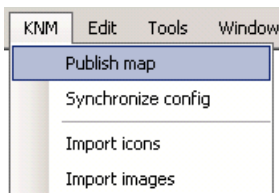
The Circular Organizer Tool

This tool is used to arrange the selected entities in a circular fashion. Use the two slider controls to modify the radius as well as angle of the entities.



Publishing Maps

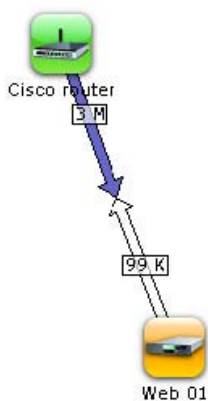
To publish changes to a network map to **Network Monitor**, select the **Publish map** command from the **KNM** menu. The current map is sent to the **Network Monitor** server, and updates immediately.



Bandwidth usage visualization

Network Monitor can display the bandwidth utilization of specified network interfaces directly on the network maps, in real time. This feature is also available for monitors on gateways. A connection has to be specified between two nodes on a network map, then linked to a **Bandwidth** monitor.

The visual feedback consists of two arrows representing the inbound and outbound traffic on the connection. The inbound traffic arrow pointing towards the asset and the outbound traffic arrow pointing away from the asset.



Bandwidth utilization visual feedback

The thickness, and color, of the arrows indicates the utilization level. The thicker the arrow is, the greater the bandwidth utilization.

The color of the arrows also give an indication to the utilization level. The arrow color is on a scale going from white (lowest utilization), blue, green, orange, up to red (highest utilization).

The amount of traffic going in each direction is also visible directly on the connection itself, expressed

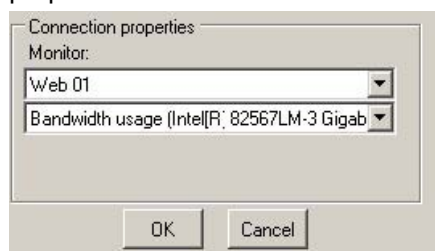
in Kbps/Mbps/Gbps as appropriate.

Creating a bandwidth connection

Displaying bandwidth utilization on a network map starts by creating a connection between two entities on the map. At least one of the entities must be a **Network Monitor** asset. The other can be another **Network Monitor** asset or group. A connection is then linked to a specific **Bandwidth utilization** monitor in **Network Monitor**. There are two different methods of creating a connection.

Creating a single connection

Select two nodes on a network map. One must be a **Network Monitor** asset. Then right-click in the map window and select **Create connection** from the **Modify selection** popup window. The connection is created and displayed as a line between the two entities. The properties window displays the properties of the connection.



To link the connection to a monitor in **Network Monitor**, first select the asset, then select the bandwidth usage monitor to associate with the connection. The bandwidth usage monitor must already be defined for the selected asset to see it displayed in the monitor drop-down list. Click the **OK** button to confirm your selection.

Optionally create a connection without linking the connection to a **Bandwidth utilization** monitor in **Network Monitor**. In this case, the connection is shown as a line between the entities on the map when viewed on the dashboard, without any visual information about the current bandwidth utilization.

Creating multiple connections

Optionally create several connections at once. First select the desired nodes on the map, then right-click and choose the **Create multiple connections** from the **Modify selection** popup window.



Select the node to create multiple connections to. A new connection for all the selected entities is created, with the selected node as the common endpoint for each of the multiple connections.

Editing a connection

To edit an existing connection, click directly on the line representing the connection in the map view. The properties of the selected connection are displayed in the properties window. To select the bandwidth usage monitor to be used for the connection, first choose the relevant asset, then the bandwidth usage monitor. The bandwidth usage monitor must already be defined for the selected asset to see it displayed in the monitor drop-down list. Click the **OK** button in the properties window to confirm your selection.

Deleting a connection

To delete a connection from the map, first select it by clicking the line representing the connection in

Utilities Reference

the map view. The selected connection is displayed in the tree control and the properties are shown in the properties view. To delete the connection, press the **Delete** key on the keyboard.

Index

A

Access denied • 175
 Acknowledging Alarms • 68
 Action Reference • 143
 Actions tab • 56
 Active Directory monitor • 110
 Adding / Editing Groups • 44
 Adding Map Nodes • 192
 Adding Monitors • 59
 Adding Preconfigured Monitors • 60
 Additional for non-administrator users • 181
 Adjusting the firewall settings • 181
 Advanced edit tab - assets • 50
 Advanced edit tab - gateways • 39
 Advanced edit tab - groups • 45
 Advanced edit tab - monitors • 63
 Advanced Topics • 159
 Alarm filtering edit tab - monitors • 64
 Alarm Messages • 65
 Asset Commands and Views • 47
 Asset maintenance • 89
 Asset templates • 101
 Asset Templates • 52
 Assets • 47
 Assets tab • 33
 Audit tab • 38
 Authentication edit tab • 40

B

Backup of Network Monitor • 160
 Bandwidth usage visualization • 194
 Bandwidth utilization monitor • 111
 Basic edit tab - monitors • 63
 Basic properties edit tab - assets • 49
 Basic properties edit tab - gateways • 39
 Basic properties edit tab - groups • 44
 Basic properties tab • 100

C

Caching of counters • 178
 CIM monitor • 112
 Citrix server monitor • 113
 Clear event log action • 143
 Clear eventlog event • 150
 Comments • 84
 Compiling Custom MIB Files • 94, 185
 Configuration Summary • 14
 Configuring Maps • 191
 CPU utilization monitor • 114
 Create a new user group • 100
 Creating a bandwidth connection • 195
 Crumblin • 18
 Customized data types • 101
 Customized reports • 77

D

Dashboard • 88
 Dashboard Map Editor • 189
 Data extraction reference • 160
 Data tables • 82
 Data Views • 21
 Database server monitor • 114
 Datastore utilization • 115
 Default messages • 107
 Dependency Testing • 51
 device_xml • 163
 devicelist_xml • 165
 DHCP query monitor • 115
 dir • 161
 Directory property monitor • 116
 Disk utilization monitor • 117
 DNS lookup monitor • 117
 Downtime report • 83

E

Edit asset maintenance • 89
 Edit Menus • 22
 Edit monitor maintenance • 90
 Edit user work schedule • 91
 Editing asset templates • 102
 Editing Assets • 49
 Editing Gateways • 38
 Editing Map Nodes • 192
 Editing Monitors • 61
 Emailing and publishing reports • 72
 Enabling the ODBC Driver • 169
 Environment monitor • 118
 Event log monitor • 118, 174
 Exchange server monitor • 119
 Execute command via SSH2 action • 143
 Execute command via SSH2/Telnet event • 150
 Execute Windows command action • 144
 Execute Windows command event • 151
 Export statistics event • 151
 External resources • 174

F

File change monitor • 120
 Format Variables • 66
 FTP server monitor • 120
 Full index of Microsoft WMI troubleshooting articles • 183

G

Gateway Commands and Views • 32
 Gateway Nodes and Network Discovery • 27
 Gateways • 30
 Generate report event • 153
 Getting Started • 16
 Gizmo • 188
 Graphs • 81
 Group Commands and Views • 43
 Groups • 42

Index

H

How to verify that KNM have access to remote registry service • 177
HTTP Get/Post action • 144
HTTP GET/POST request event • 154

I

Images • 84
IMAP4 server monitor • 121
Importing Map Images • 190
Inheritance • 17
Init.cfg parameters • 159
Installation • 9
Installing a New Instance of Network Monitor R9 • 10
Installing/Uninstalling Gateways • 27
Integration with Discovery • 25
Interface options tab • 100

J

JVM performance monitor • 121

K

Knowledge Base Articles • 86
Knowledge Base Categories • 87
Knowledge tab • 38

L

LDAP query monitor • 122
List reset action • 146
List View Controls • 19
List View Filtering • 19
Lists Views • 18
Log file monitor • 123
Log settings • 102
Lua • 186
Lua script monitor • 124
Lua scripts action • 146
Lua scripts event • 155

M

Mail server QOS monitor • 124
Management Interface • 15
Map tab • 34
Memory leaks in remote registry service on monitored machine • 177
Memory utilization monitor • 125
MIB Browser • 93
MIB Objects • 93
Migration of KNM standalone to KNM integrated • 11
Monitor Commands and Views • 55
Monitor maintenance • 90
Monitor Reference • 109
Monitor tab • 48
Monitor tree • 17
monitor_graph • 161
monitor_status_list • 161
monitor_statusstring • 162
monitor_uptimestring • 162
Monitors • 53

Monitors tab • 33
Monitors using Windows authentication • 174
Moving Nodes • 23
My settings • 99
MySQL monitor • 125

N

Navigation Panel Overview • 24, 75
Navigation Panel Reference • 75
Network Monitor Licensing in the VSA • 30
Network Monitor Module Requirements • 9
Network Monitor Overview • 7
Network Monitor Service account and rights assignment • 173
Network path can not be found • 175
NNTP server monitor • 127
NOC edit tab • 41
NOC settings • 103
Node and User Search • 19

O

Oracle monitor • 127
Organizations and Machine Groups • 28
Other system settings • 104

P

Performance related issues with monitored asset • 176
Ping monitor • 128
POP3 server monitor • 129
Pre-Installation Checklist • 9
Process status monitor • 129
Properties and Commands • 22
Publishing Maps • 194

R

Radius monitor • 129
Record manager log • 96
Renaming Gateways and Assets • 29
Report data types • 80
Report info • 79
Report properties • 78
Report styles • 79
Report templates • 78
Reports • 69

S

Salesforce query monitor • 130
Schedule blocks • 92
Scheduled Event Reference • 150
Schedules tab • 36
Scheduling reports • 73
Send email event • 155
Send mail action • 146
Send message via PageGate action • 147
Send message via PageGate event • 155
Send SMS action • 147
Send SMS event • 156
Send Wake-on-LAN packet action • 148
Send Wake-On-LAN packet event • 156
Server Sizing • 9

- Service monitor • 174
- Simulate alarm tab • 59
- SMS settings • 104
- SMTP server monitor • 131
- SNMP monitor • 131
- SNMP Set action • 148
- SNMP Set event • 156
- SNMP trap monitor • 132
- SQL Server monitor • 133
- SSH2 script monitor • 135
- SSH2 server monitor • 135
- Starting the Map Editor • 190
- State change log tab • 48
- Statistics edit tab - monitors • 64
- Summary tab • 56
- Swap file utilization monitor • 135
- Syslog message • 97
- Syslog monitor • 136
- System administrator console • 97
- System log • 99

T

- Tags edit tab • 45
- TCP port scan monitor • 136
- Telnet server monitor • 137
- Terminal service monitor • 137
- test_status • 166
- TFTP server monitor • 137
- The Monitoring View • 16
- The RPC server is unavailable • 176
- Ticket action • 29, 149
- Toplist tab • 34
- Toplists • 84
- Transfer speed monitor • 138
- Trap messages • 99
- Trigger monitor event • 157
- Troubleshooting • 175
- Troubleshooting Windows monitoring and authentication • 173

U

- UNIX system support files • 167
- User Integration • 30
- User notification groups • 100
- User notification schedules • 91
- user_status • 165
- Using the Organizer Tools • 193
- Utilities Overview • 185
- Utilities Reference • 185

V

- Verifying that WMI is enabled for the account • 179
- Verifying that WMI works • 181
- version • 166
- Viewing Customized Reports • 72
- Viewing Quick Reports • 70
- Viewing Report Templates • 69
- VMware performance monitor • 138
- VSA Integration • 24

W

- Web server monitor • 139
- Windows Management Instrumentation (WMI) • 178
- Windows performance monitor • 140
- Windows performance registry • 176
- Windows service control action • 149
- Windows service control event • 157
- Windows service list • 92
- Windows service status monitor • 141
- Windows Troubleshooting and Performance Monitoring • 173
- WMI Query monitor • 141