Network Monitor

Quick Start Guide

Version R91

English

July 7, 2016

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 1
Pre-Installation Checklist 2
Network Monitor Module Requirements 2
Server Sizing 3
Installing a New Instance of Network Monitor R91 3
Migration of KNM standalone to KNM integrated 4
Configuration Summary 7
Getting Started 8
- The Monitoring View 8
- Monitor tree 9
- Inheritance 10
- Crumbline 10
- Lists Views 10
- Node and User Search 11
- List View Controls 12
- List View Filtering 12
- Data Views 13
- Properties and Commands 15
- Edit Menus 15
- Moving Nodes 16

VSA Integration 17
- Navigation Panel Overview 17
- Integration with Discovery 19
- Gateway Nodes and Network Discovery 20
- Installing/Uninstalling Gateways 21
- Organizations and Machine Groups 21
- Renaming Gateways and Assets 22
- Ticket action 23
- User Integration 23
- Network Monitor Licensing in the VSA 24

Gateways 24
- Gateway Commands and Views 25
  - Assets tab 26
  - Monitors tab 27
  - Map tab 27
  - Toplist tab 29
  - Schedules tab 30
  - Knowledge tab 32
  - Audit tab 32

Editing Gateways 32
Basic properties edit tab - gateways 33
Advanced edit tab - gateways 33
Authentication edit tab 34
NOC edit tab 35
Groups 36
Group Commands and Views 37
Adding / Editing Groups 37
Basic properties edit tab - groups 38
Advanced edit tab - groups 38
Tags edit tab 39
Assets 40
Asset Commands and Views 40
Monitor tab 41
State change log tab 41
Editing Assets 42
Basic properties edit tab - assets 42
Advanced edit tab - assets 43
Dependency Testing 44
Asset Templates 45
Monitors 46
Monitor Commands and Views 48
Summary tab 49
Actions tab 49
Simulate alarm tab 52
Adding Monitors 52
Adding Preconfigured Monitors 53
Editing Monitors 54
Basic edit tab - monitors 56
Advanced edit tab - monitors 56
Alarm filtering edit tab - monitors 57
Statistics edit tab - monitors 57
Alarm Messages 58
Format Variables 59
Acknowledging Alarms 61
Reports 62
Viewing Report Templates 62
Viewing Quick Reports 63
Viewing Customized Reports 65
Emailing and publishing reports 65
Scheduling reports 66
Index 67

Network Monitor Overview

Network Monitor is a web-based monitoring solution for monitoring the performance and availability of a wide array of network devices. **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.
- **Subgroup** - A subgroup is a "container node" for other nodes in the **Network Monitor** monitor tree. Typically subgroups represent a logical business unit.
- **Actions** - One or more actions can 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.

- 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.

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 3)*. 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 2)*.
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 R91 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.

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 R91

Network Monitor R91 only runs as an integrated addon module with the VSA.

To add the Network Monitor R91 addon module to an existing VSA R91 on premise environment:

1. **Submit a support request** *(https://helpdesk.kaseya.com/home)* to have your VSA license updated to permit installing Network Monitor R91 as an addon module.
2. Run **Kaseya Server Setup** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/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/9010000/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 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 `nmservicelg.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/9010000/install/index.asp#18015.htm)*.
- All configuration data will be migrated to the SQL Server using by the VSA.

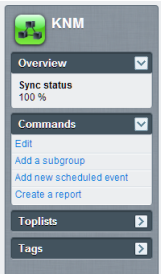
Before installing VSA R91

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.

After installing VSA R91

- 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.

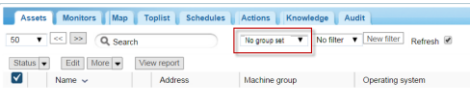
FAQ

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.

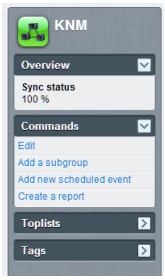
- You can use the **Add asset** function. You should select a number of devices from the unmapped group and choose this command. This command works in bulk. You will then have to select a machine group that the assets will be created in. Once you click OK the assets will be created and they should be 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.

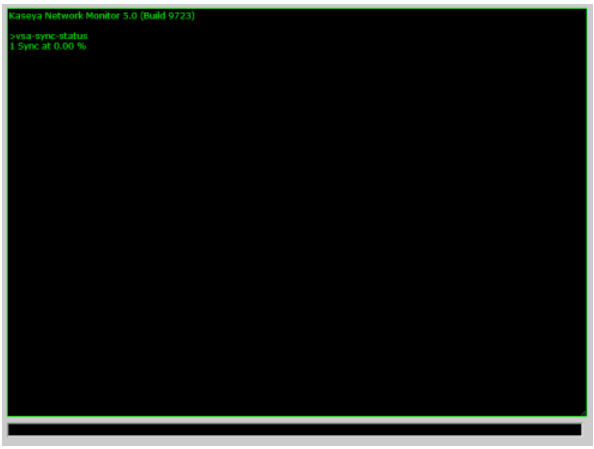
Is the sync percentage shown anywhere in the interface?

- 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** R91, 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 2)*, **Server Sizing** *(page 3)* and **Network Monitor module requirements** *(page 2)* topics.
2. Perform the steps described in **Installing a New Instance of Network Monitor R91** *(page 3)*.
3. **Logon to the VSA** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#264.htm)*.
4. Review the **Getting Started** *(page 8)* section of this documentation to familiarize yourself with the module's user interface.
5. Run **Network Discovery** *(page 19)*.
6. **Install a gateway** *(page 21)* on a discovered network.
7. **Add preconfigured monitors** *(page 53)* 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 46)*.
9. Define **actions** *(page 49)* that are executed when a monitor fails a test a consecutive number of times.
10. Test the monitor by creating a **Simulate Alarm** *(page 52)* report to confirm the alarm is configured as you expect.

Getting Started

In This Section

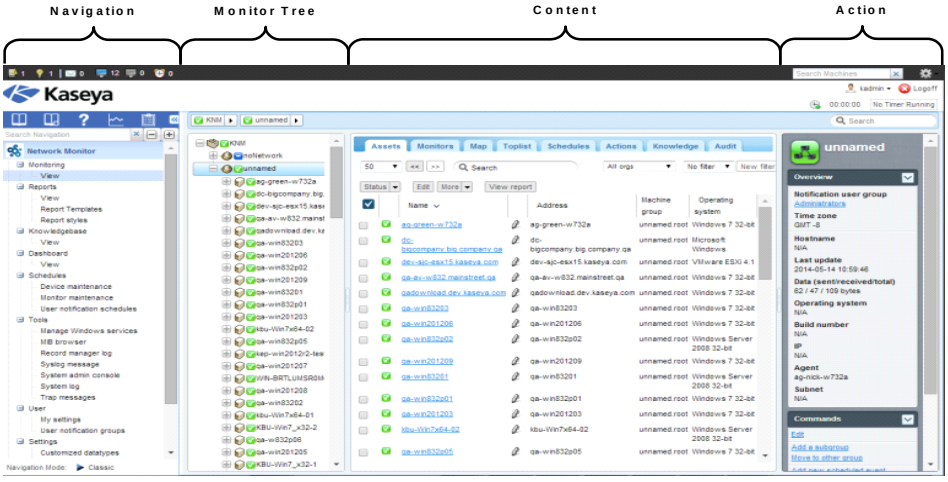
The Monitoring View	8
Monitor tree	9
Inheritance	10
Crumbline	10
Lists Views	10
Node and User Search	11
List View Controls	12
List View Filtering	12
Data Views	13
Properties and Commands	15
Edit Menus	15
Moving Nodes	16

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.

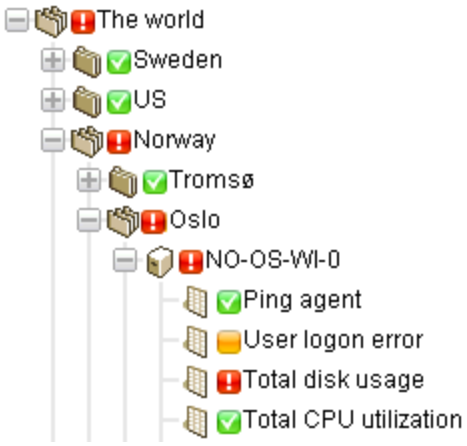
- **Navigation** - Displays the three other panels when you select the VSA > Network Monitor > Monitoring > **View** item in the navigation panel. Other items in the navigation panel provide access to **module-level settings and other views** *(page 17)*.
- **Monitor Tree** - Selects the group, gateway, 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

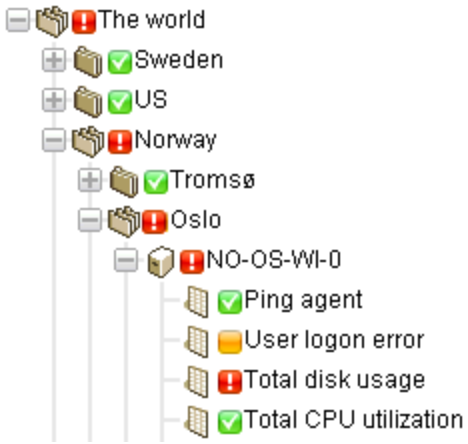
The monitor tree organizes all groups, gateways, assets and monitors managed by **Network Monitor**. Using the tree you can quickly browse to any asset and monitor.

- **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 suggroup 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.

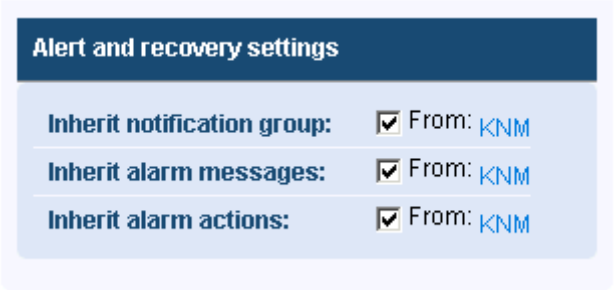


Inheritance

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.

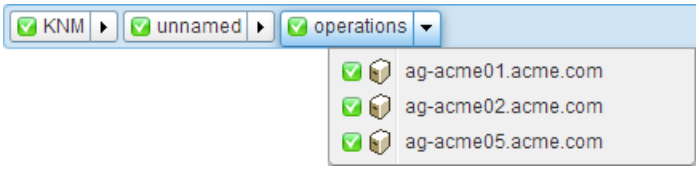


For any one node you can elect to use either an inherited setting or override it. For example, the image below shows a setting that is inherited from a higher level node. You'll spot this same convention used throughout the **Network Monitor** user interface for many different types of properties. *Note 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.



Crumbline

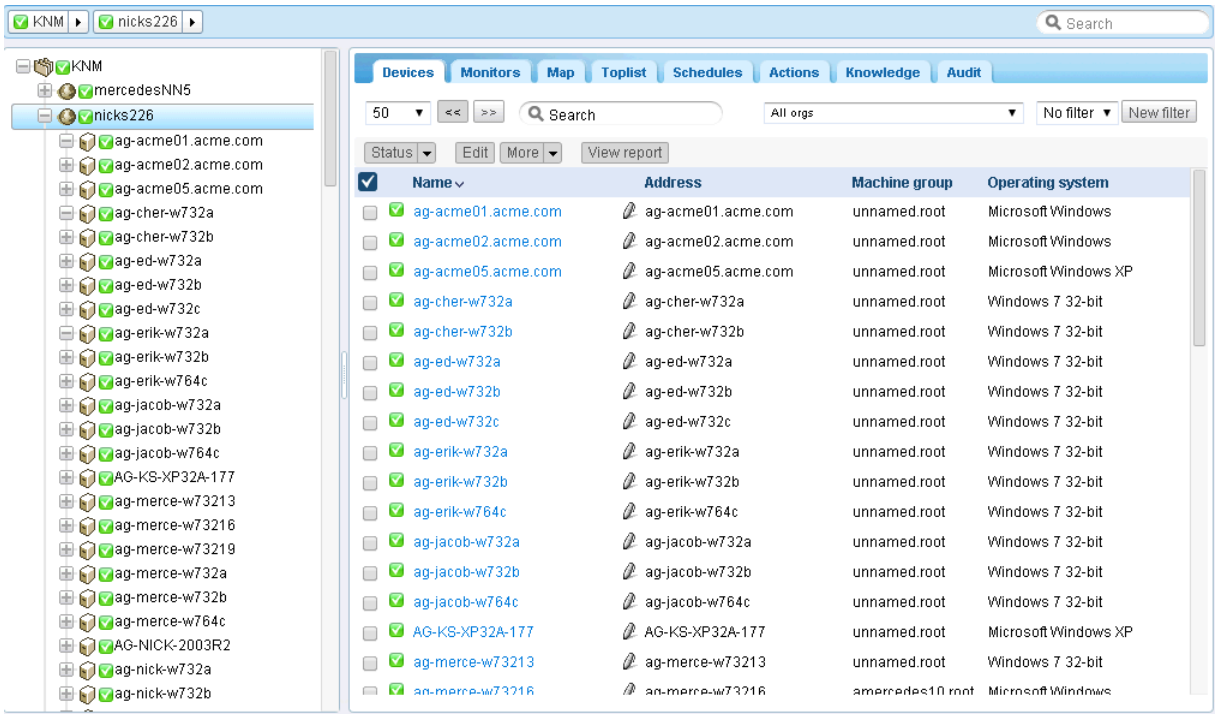
A crumbline at the top of the monitor tree shows you the currently selected node in the tree. You can click anywhere in the crumbline to jump to that node in the monitor tree. Or you can select one of the child nodes of the currently selected node.



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.



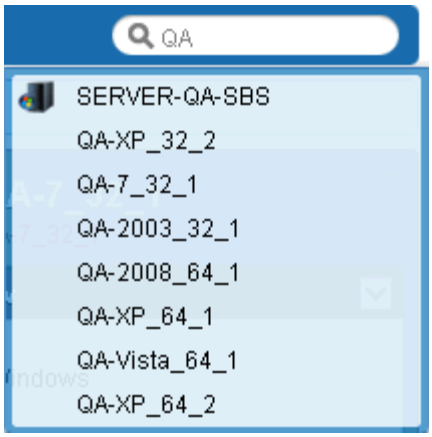
You can see all the assets and monitors that are members of that group or gateway. For example:

- 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

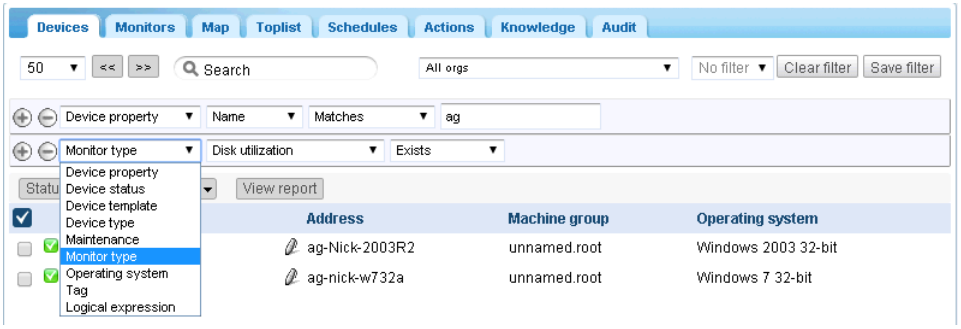
A **Search** edit box displays in the upper right hand corner. Enter a string to search the monitor tree for all *group*, *gateway* and *asset* nodes that match the string entered. **Do not press the Enter key.** Just wait for the list of nodes to be displayed below the edit box, then select one to display 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 can also page forward, page back, and **filter a list view** *(page 12)*. 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.

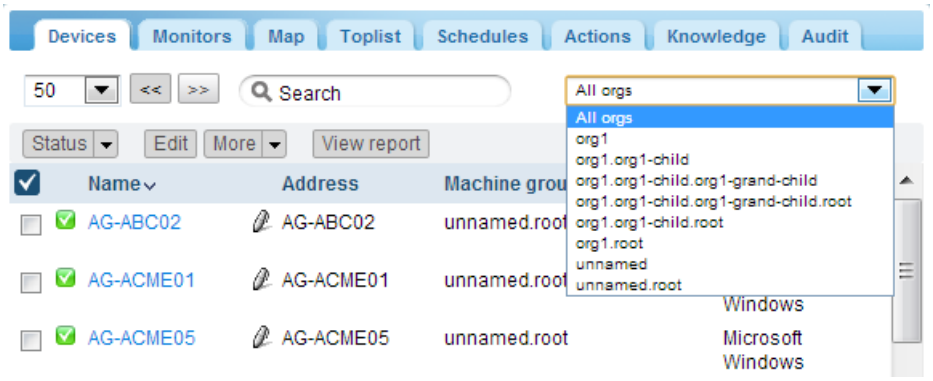
When a Group is Selected	Assets tab	name, description, address and machine group name
	Monitors tab	name, asset name, machine group name
	Schedules tab	event/schedule description
	Knowledge tab	article ID, article title
	Audit tab	message text
When an Asset is Selected	Monitors tab	monitor name, type (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 are limited by your selected VSA **scope** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#4578.htm)*.
- Filtering does not affect the display of assets in the **monitor tree** *(page 20)*.

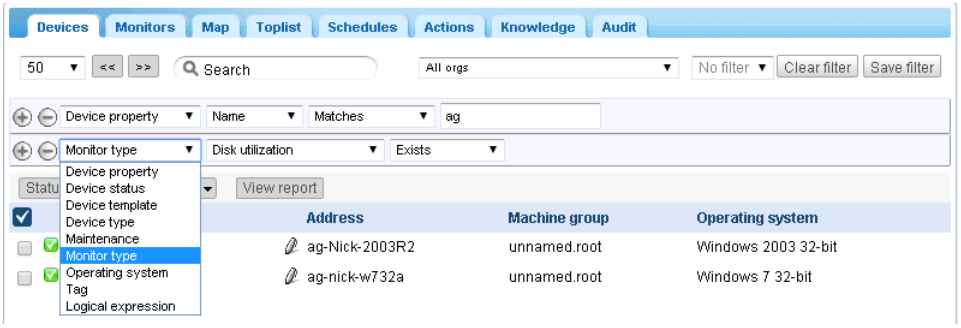
Filtering List Views by Multiple Conditions

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 of available with conditional filters:

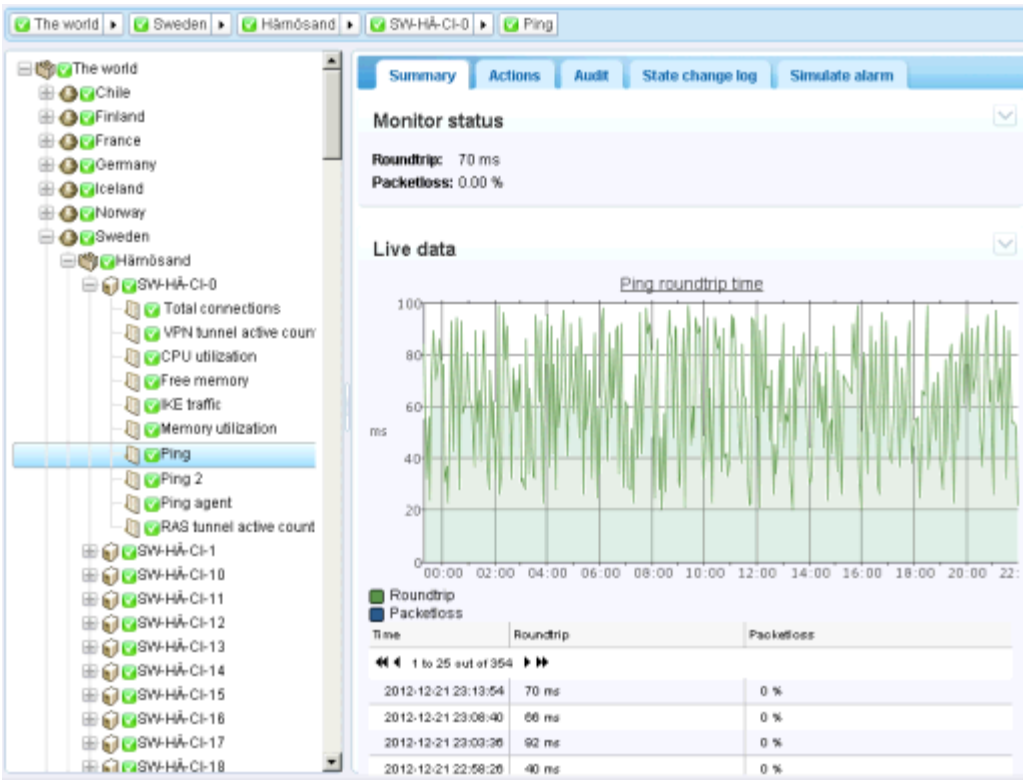
- **New filter** - Adds a new conditional filter.
- **Clear filter** - Clears a conditional filter from the list view.
- **Edit filter** - Displays a saved conditional filter so you can edit it.
- **Save filter** - Saves changes to a conditional filter.
- **Cancel edit** - Cancels edit changes to a conditional 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.



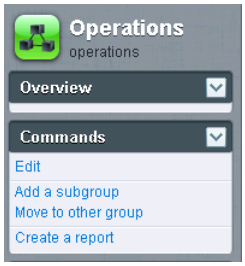
Properties and Commands

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:

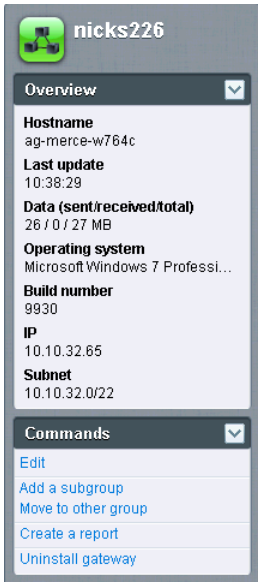
- Edit
- Add a group



Gateway Commands

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

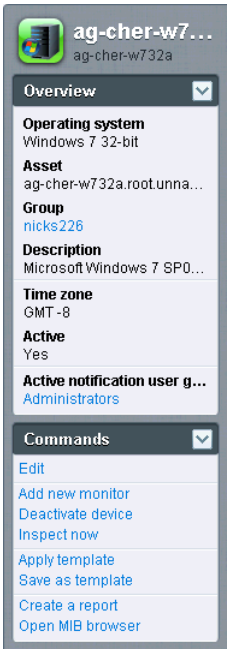
- Edit
- Add a group



Asset Commands

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

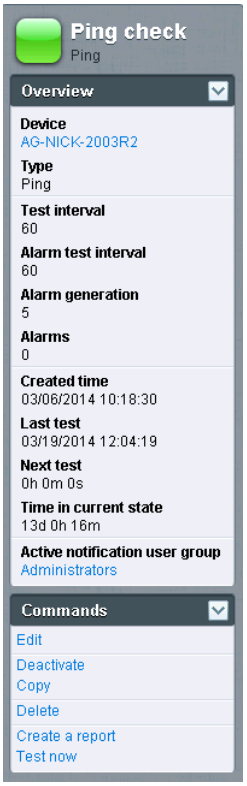
- Edit
- Add new monitor



Monitor Commands

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

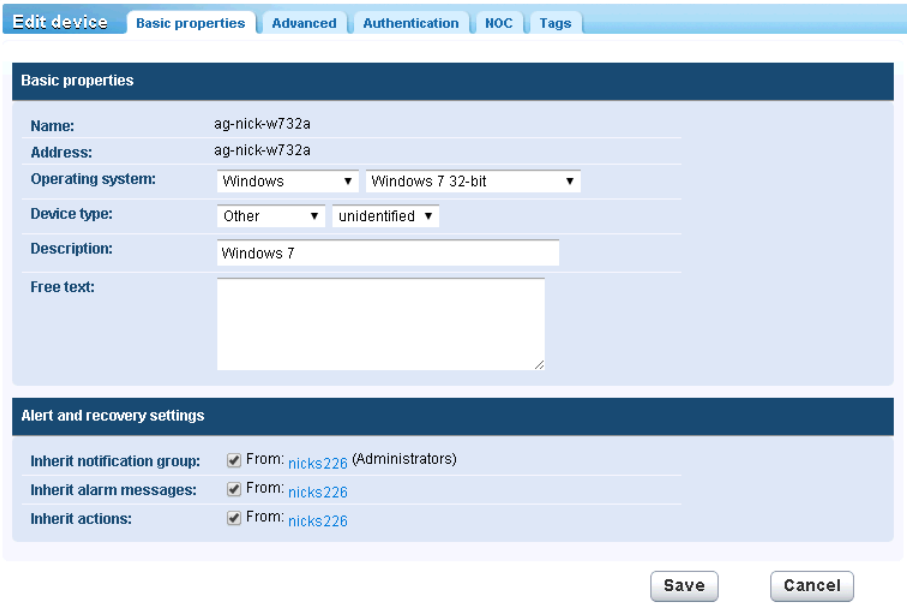
- Edit
- Test Now



Edit Menus

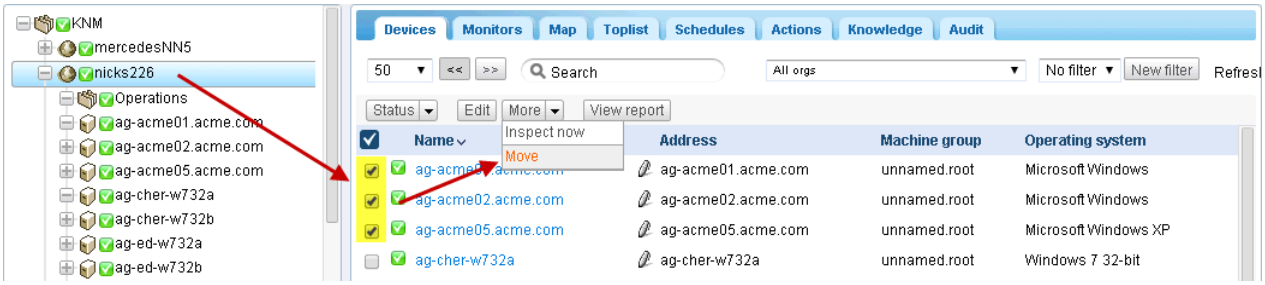
When you click the **Edit** command for a selected node you typically see a tabbed set of properties sheets. Hovering the cursor over most fields displays a tooltip balloon on the right side, providing an explanation of the field.

Click the **Save** or **Cancel** button to close the edit menu and return to the **List View** *(page 10)* or **Data View** *(page 13)* of the selected node.



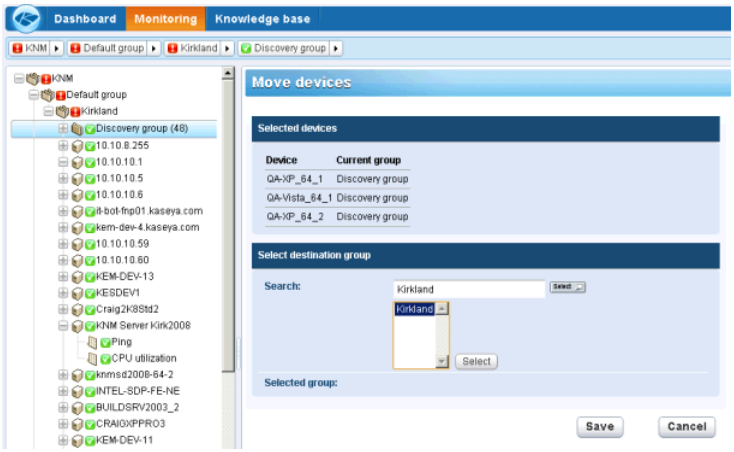
Moving Nodes

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*.



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.



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.

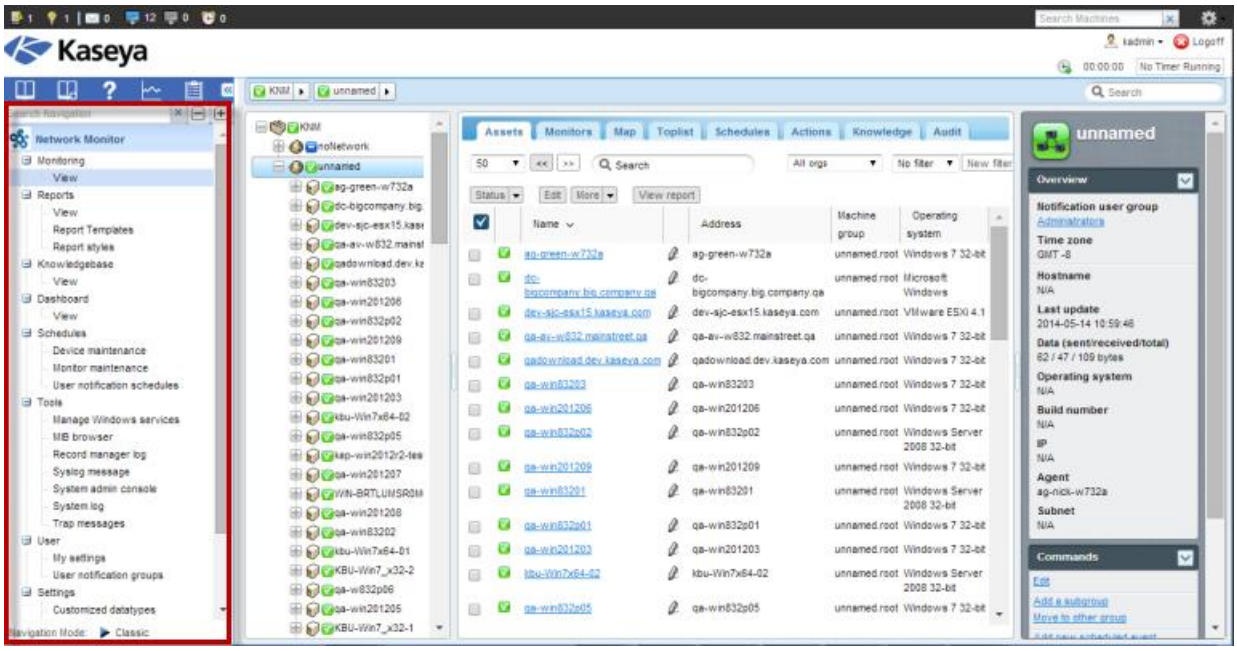
Note: You can also click the **Select** button to browse for a target node.

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 included with this documentation. The following is a summary description of each option in the navigation panel.

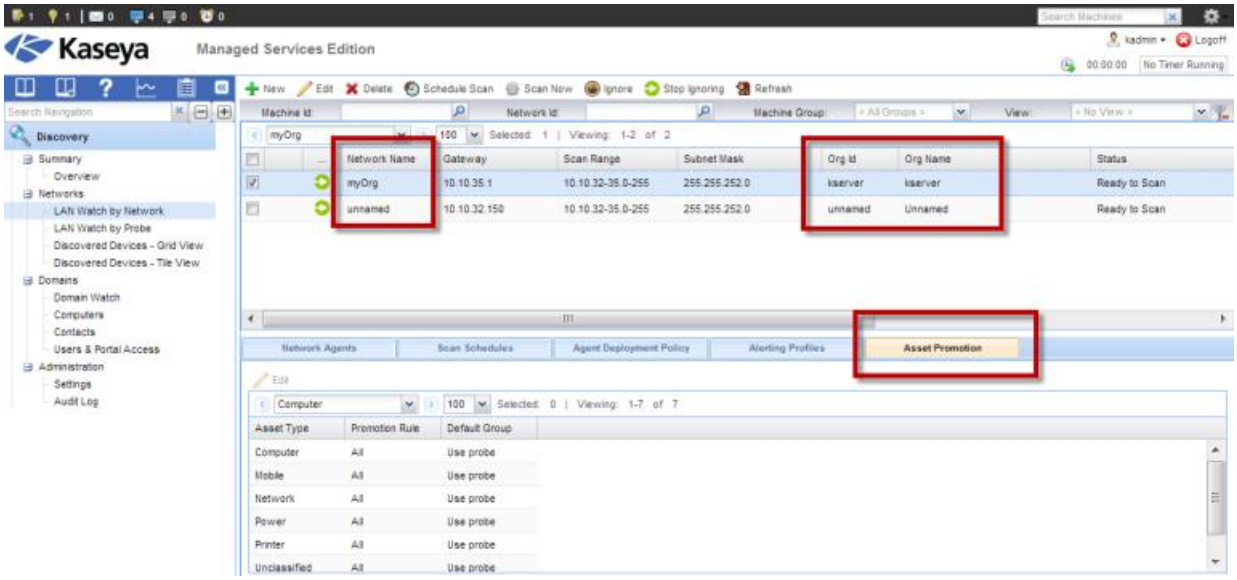
Functions	Description
Monitoring > **View** *(page 8)*	Selects the **monitoring view** *(page 8)*.
Reports > View	Configures customized reports that are bound to selected sets of nodes.
Report Templates	Configures report templates that can be applied to any set of nodes.
Report styles	Configures the overall look of reports, report templates and customized reports.
Knowledgebase > View	Selects the Knowledge base view.
Dashboard > View	Selects the Dashboard view.
Asset maintenance	Configures asset maintenance schedules.
Monitor maintenance	Configures monitor maintenance schedules.
User notification schedules	Configures Network Monitor user work schedules.
Management Windows services	Selects the Management Windows services view.
MIB browser	Selects the MIB browser view.
Record manager log	Selects the Record manager log.
Syslog message	Selects the Syslog messages view.
System admin console	Selects the System admin console view.
System log	Displays log entries created by the `Kaseya Network Monitor` service.
Trap messages	Selects the SNMP Trap messages view.
My settings	Selects the Edit my settings view.
User notification groups	Maintains user groups. Asset notifications are sent to all members of the notification user group assigned to that asset.

Customized datatypes	Creates customized data types for use with monitors capable of storing generic data.
Asset templates	Configures sets of monitors that can be applied to an asset in one step.
Log settings	Sets log policies for Network Monitor.
NOC configuration	Creates customized NOC (Network Operations Center) views.
Other system settings	Specifies additional settings for alerts and other events.
SMS	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/9010000/index.asp#10627.htm)* page, as shown below.

- See the **Agent Deployment** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/EN_agentdeployment_R91.pdf#zoom=70&navpanes=0)* quick start guide if you're new to working with agents.
- **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/9010000/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/9010000/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 20)*.

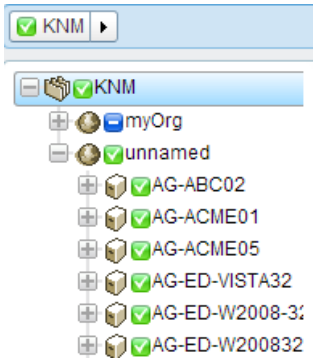
Gateway Nodes and Network Discovery

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 19)*.



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 19)*. 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.
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 52)* or **add preconfigured monitors** *(page 53)* 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

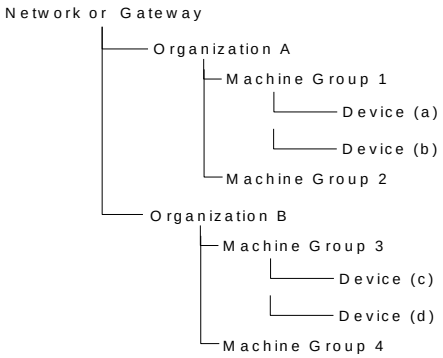
Organizations and machine groups are logical "containers" in the VSA used to organize all "assets" managed by the VSA. An asset is any machine or asset you choose to manage. Within the VSA you can assign any asset to any combination of organization and machine group.

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 12)* in **Network Monitor**.

Renaming Gateways and Assets

You cannot rename gateways or discovered assets **promoted to an asset** *(page 19)* 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/9010000/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/9010000/index.asp#10619.htm)* > **Rename Asset**
- Discovery > **Discovered Devices - Tile View** *(http://help.kaseya.com/webhelp/EN/KDIS/9010000/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/9010000/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/9010000/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/9010000/index.asp#5478.htm)* within the VSA.

Parameters

- **Alarm number** - The **alarm count** *(page 49)* 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/9010000/index.asp#4576.htm)*.

- Access to nodes within **Network Monitor** are managed using System > **Scopes** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/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/9010000/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/9010000/index.asp#503.htm)*.

> **Note:** See the **User Administration** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/EN_useradmin_R91.pdf#zoom=70&navpanes=0)* quick start guide for more information.

User Notification Groups

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

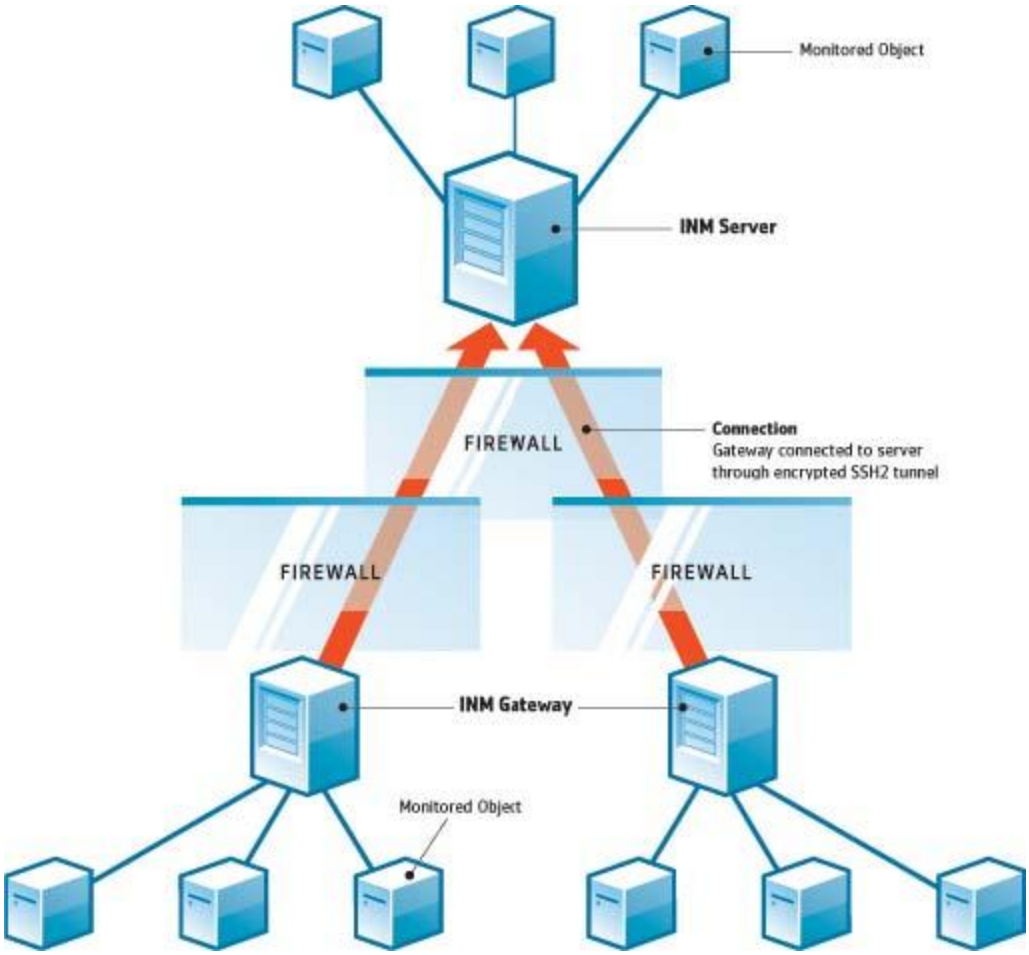
Network Monitor asset notifications are sent to all members of the user group assigned to that asset using the **Notification user group** setting on the **Basic properties tab** *(page 42)* of the asset.

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/9010000/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 37)*. Gateway nodes have additional, specialized **properties and commands** *(page 25)* for managing a gateway installed on a network.

In This Section

Gateway Commands and Views	25
Editing Gateways	32

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 37)* of a gateway.
- **Add a subgroup** - Creates a **new subgroup** *(page 37)* 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 30)*.
- **Create a report** - Creates a **report** *(page 62)*.
- **Deploy gateway** - **Installs a gateway** *(page 21)* 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 26)* - This tab displays with gateways and groups.
- **Monitors tab** *(page 27)* - This tab displays with groups, gateways, and assets.
- **Map tab** *(page 27)* - This tab displays with gateways and groups.
- **Toplist tab** *(page 29)* - This tab displays with gateways, groups, and assets.
- **Schedules tab** *(page 30)* - This tab displays with gateways and groups.
- **Actions tab** *(page 49)* - This tab displays with groups, gateways, assets and monitors.
- **Knowledge tab** *(page 32)* - This tab displays with gateways, groups, and assets.
- **Audit tab** *(page 32)* - 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 53)* 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 62)* 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 61)* 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 62)* 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.
- **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

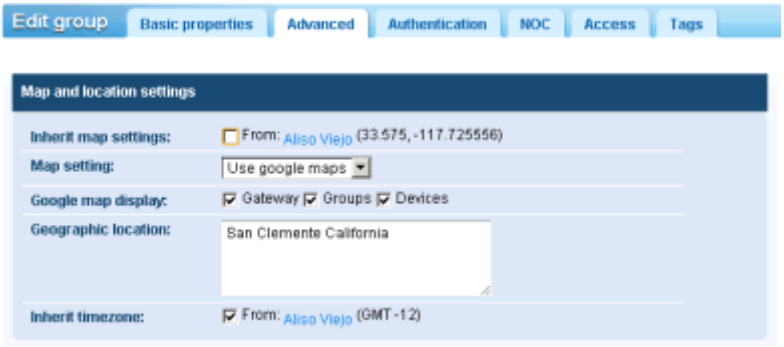
A smaller map, in the lower right hand corner of the page, shows the location of the *currently selected node*.

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.



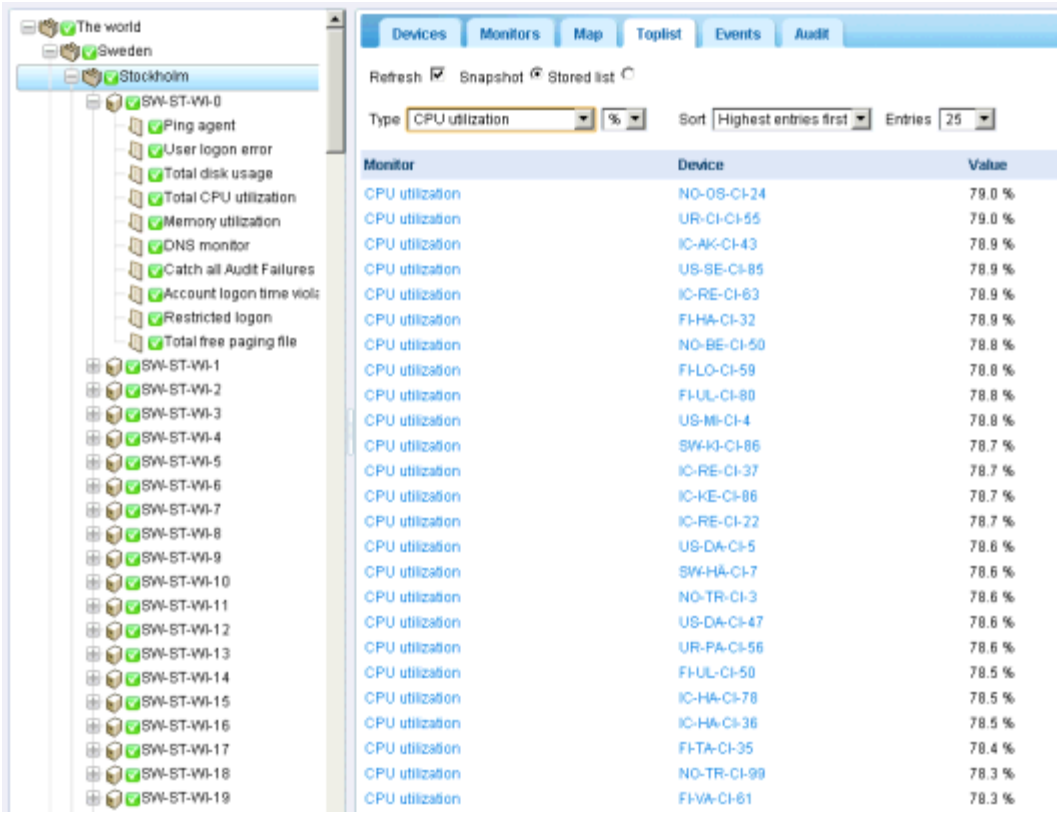
Map and location settings

- **Inherit map settings** - If checked, **map settings** *(page 27)* 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.



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* toplists 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 toplists.
  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 toplists.

  The following **Sort** options can only be used when comparing two toplists.
  - `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
    - Bandwith utilization
    - 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.

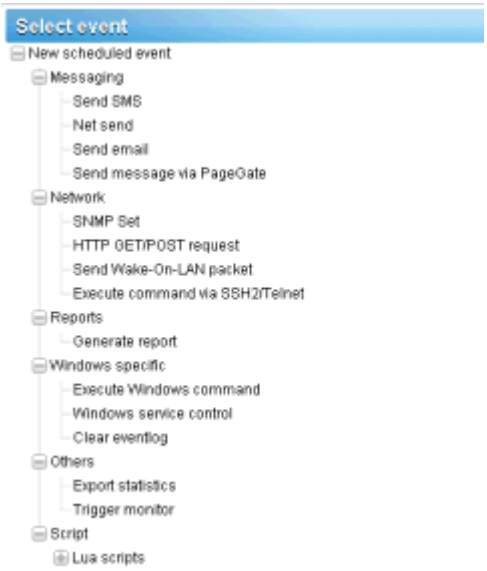
Schedules tab

This tab displays with gateways and groups.

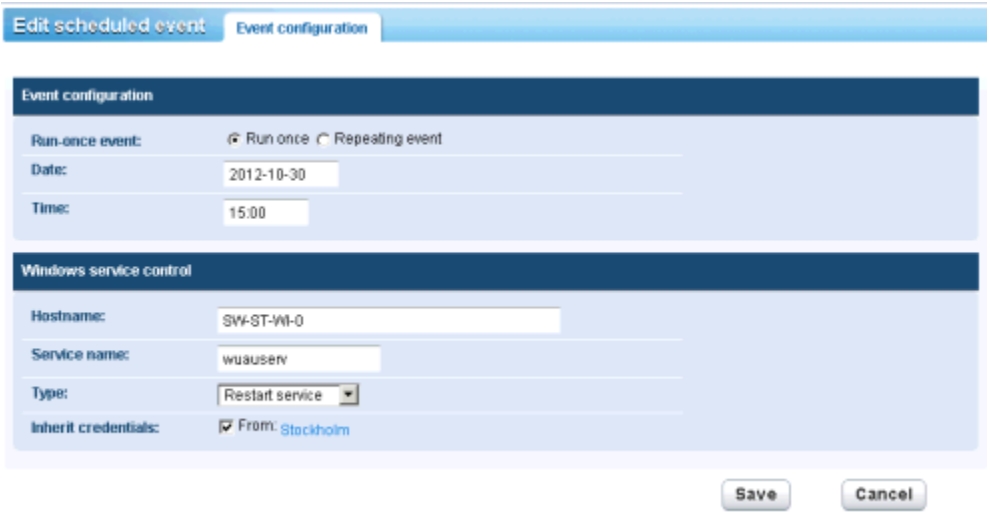
The **Schedules** tab schedules actions for a specific date and time—instead of waiting for a monitor to trigger the action. Events can be scheduled to run once or repeatedly.

> **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. 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.



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

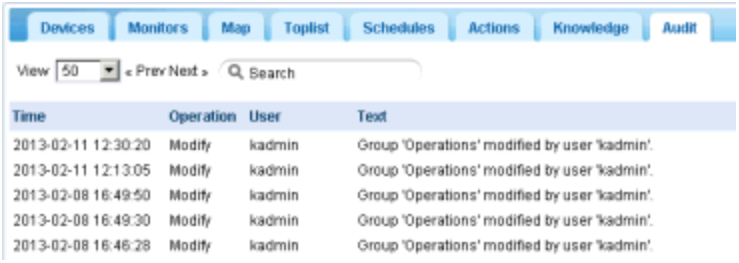
- Knowledge Base Articles
- Knowledge Base Categories

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.



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 37)*. Gateway nodes have additional, specialized properties and **commands** *(page 25)* for managing a gateway installed on a network.

- **Basic properties tab** *(page 33)* - Gateways, groups, and assets display a **Basic properties** edit tab.
- **Advanced tab** *(page 33)* - Gateways, groups, assets, and monitors display an **Advanced** edit tab.
- **Authentication tab** *(page 34)* - This edit tab displays with gateways, groups, and assets.
- **NOC tab** *(page 35)* - 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 58)* format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** *(page 49)* 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 27)* 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.
- **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 monitor requires this checkbox be enabled. Once checked, received trap messages display on the Network Monitor **Tools >** Trap messages 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.

- **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.

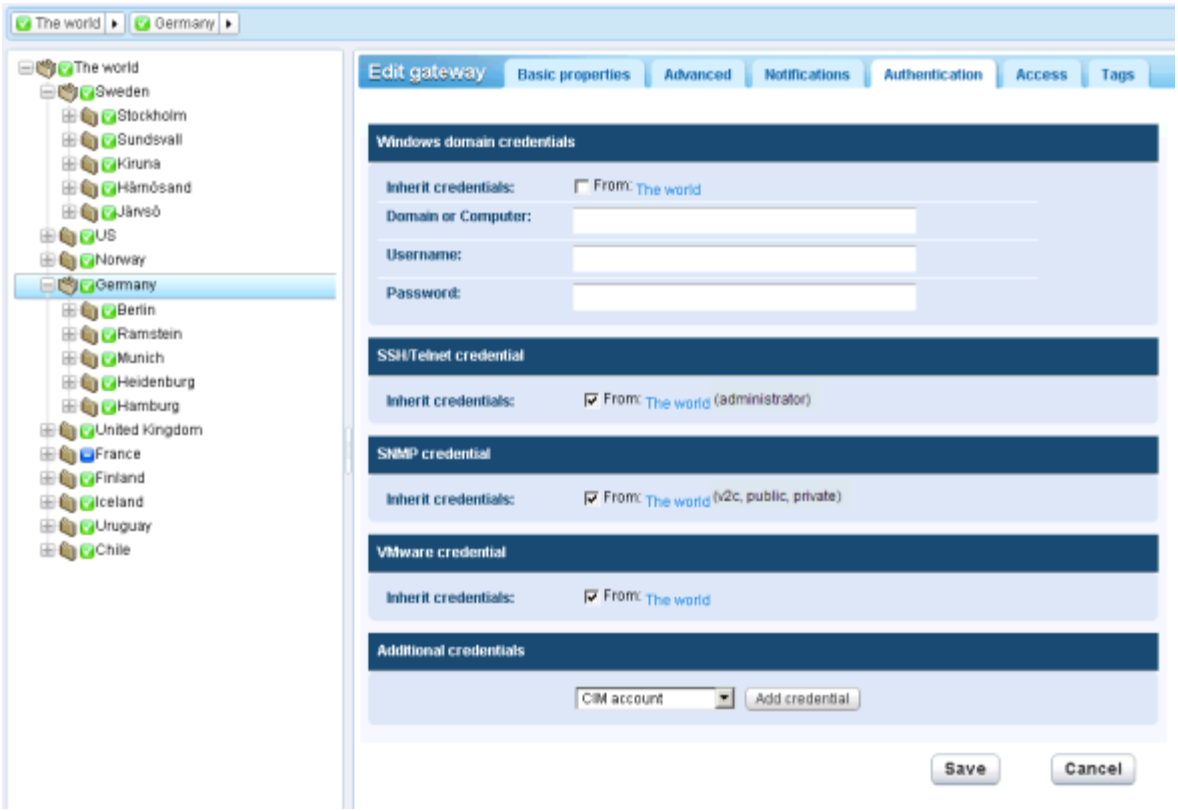
Misc settings

- **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.



For any one type of authentication, if **Inherit credentials** is checked, the credentials are inherited from a higher level node. If the checkbox is uncheck, 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.

- **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.

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.

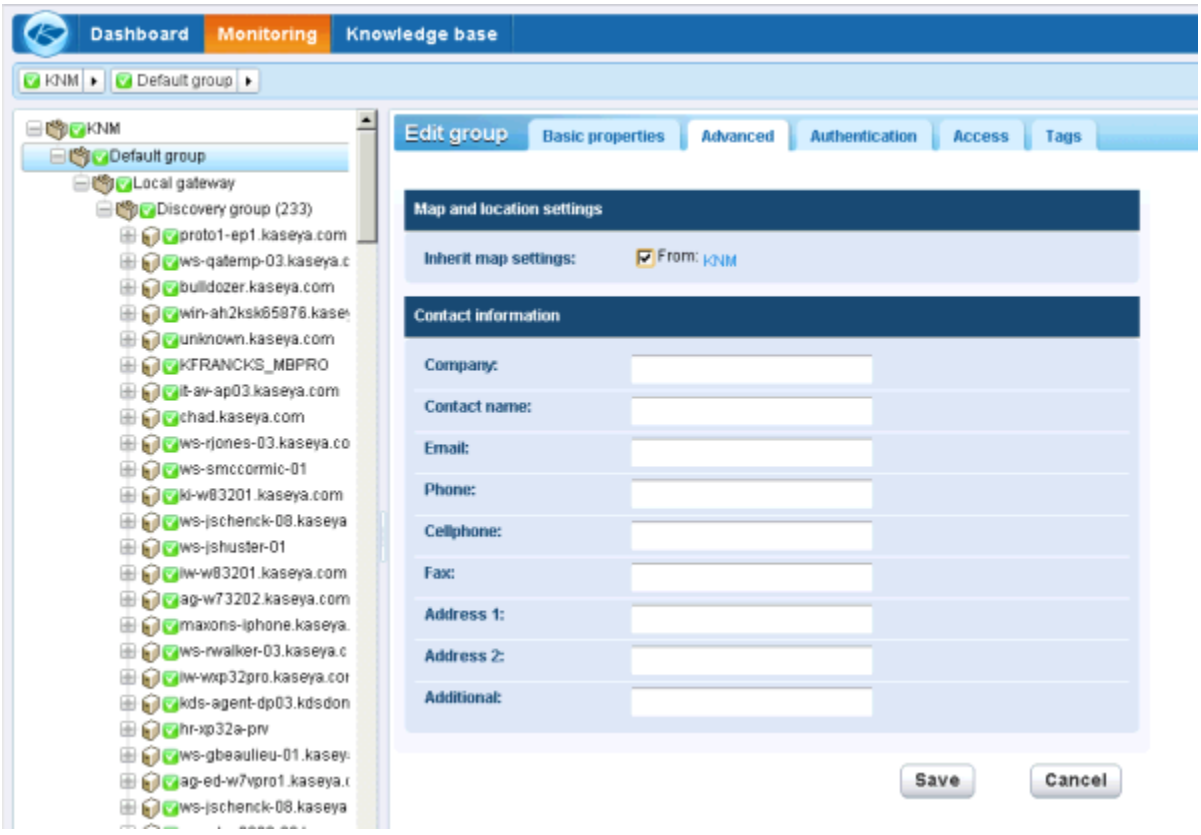
Configuring a NOC view and widget

1. Define one or more NOC views using the Network Monitor Settings > NOC configuration page.
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 assets'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 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 note 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 37
Adding / Editing Groups 37

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 37)* of a group.
- **Add a subgroup** - Creates a **new subgroup** *(page 37)* 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 30)*.
- **Create a report** - Creates a **report** *(page 62)*.

Views

Gateways and groups share the same set of views.

- **Assets tab** *(page 26)* - This tab displays with groups and gateways.
- **Monitors tab** *(page 27)* - This tab displays with gateways, groups, and assets.
- **Map tab** *(page 27)* - This tab displays with groups and gateways.
- **Toplist tab** *(page 29)* - This tab displays with gateways, groups, and assets.
- **Schedules tab** *(page 30)* - This tab displays with groups and gateways.
- **Actions tab** *(page 49)* - This tab displays with gateways, groups, assets and monitors.
- **Knowledge tab** *(page 32)* - This tab displays with gateways, groups, and assets.
- **Audit tab** *(page 32)* - 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 38)* - Gateways, groups, and assets display a **Basic properties** edit tab.

- **Advanced tab** *(page 38)* - Groups, gateways, assets, and monitors display an **Advanced** edit tab.
- **Authentication tab** *(page 34)* - This edit tab displays with groups, gateways, or assets.
- **NOC tab** *(page 35)* - This edit tab displays with groups, gateways, or assets.
- **Tag tab** *(page 39)* - 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 58)* format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** *(page 49)* 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 27)* 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.

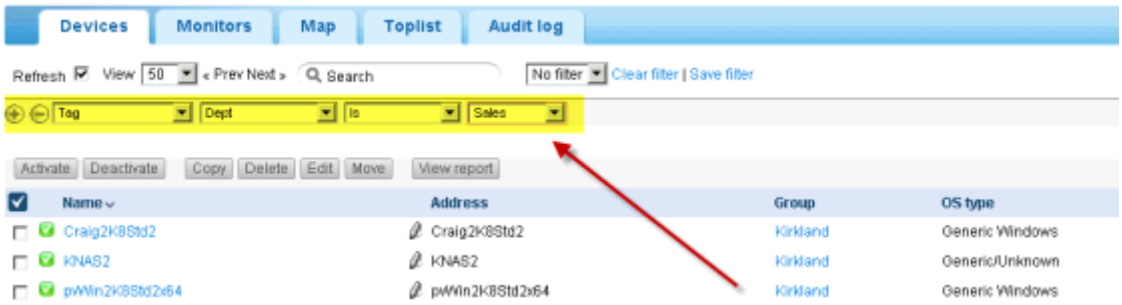
- **Company**
- **Contact name**
- **Email**
- **Phone**
- **Cellphone**
- **Fax**
- **Address 1**
- **Address 2**
- **Additional**

Tags edit tab

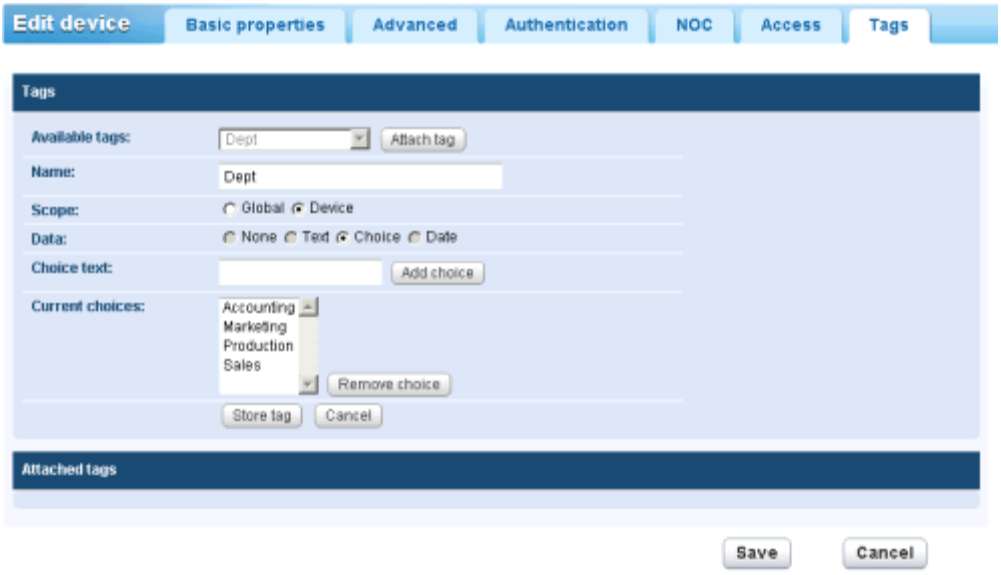
This edit tab displays with groups and assets.

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 **Edit**, then the **Tags** tab.



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`.

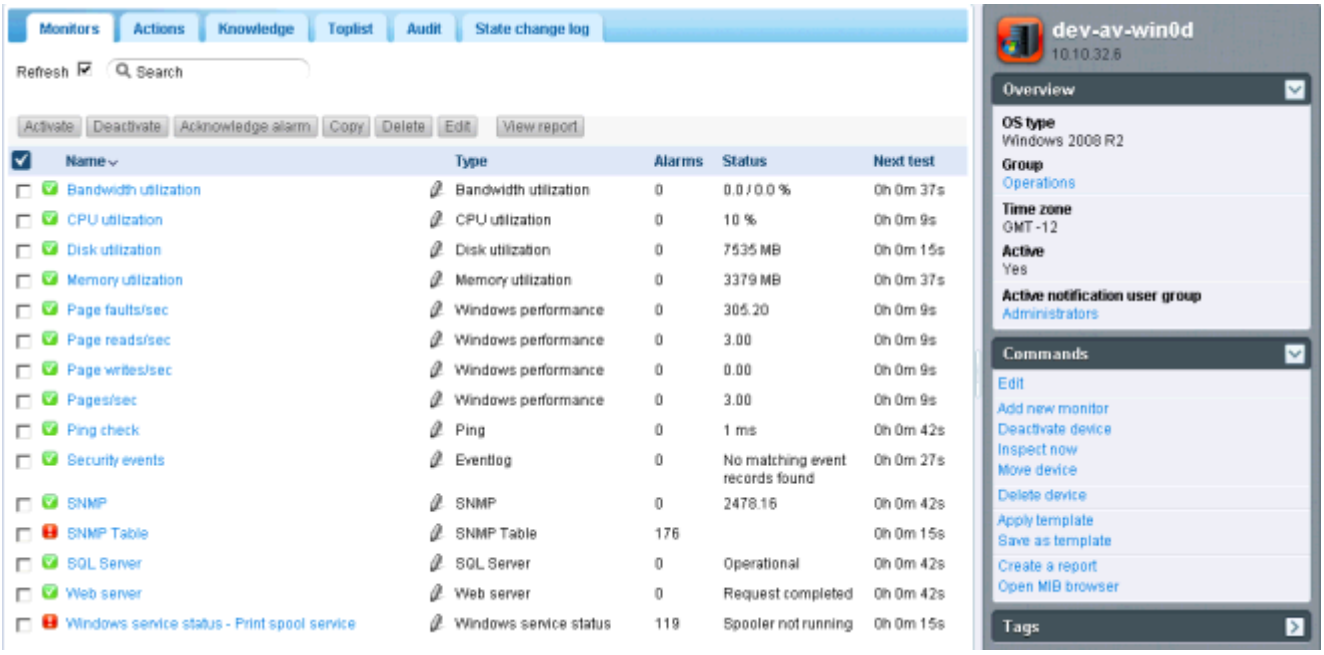
- **Date** - The user selects a date. For example, a tag called `RepairDueDate` could represent the expected date of repair for an asset.

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.



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 42)* 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 19)* **for you to work with it in Network Monitor.**

- **Add new monitor** - **Adds a new monitor** *(page 52)* to the asset.
- **Deactivate asset** - Deactivates the asset.

- **Inspect now** - Inspects an asset to determine the appropriate **pre-configured monitors** *(page 53)* 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 45)*.
- **Save as template** - Saves the set of monitors as an **asset template** *(page 45)*.
- **Create a report** - Views, emails or publishes a **report** *(page 62)*.
- **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 41)* - This tab displays with gateways, groups, and assets.
- **Actions tab** *(page 49)* - This tab displays with gateways, groups, assets and monitors.
- **Knowledge tab** *(page 32)* - This tab displays with gateways, groups, and assets.
- **Toplist tab** *(page 29)* - This tab displays with gateways, groups, and assets.
- **Audit tab** *(page 32)* - This tab displays with gateways, groups, assets and monitors.
- **State change log tab** *(page 41)* - 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 61)* 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 54)*. If multiple monitors are selected, edits shared **standard monitor properties** *(page 56)* of these monitors.
- **View report** - Generates a report for selected assets.

Table Columns

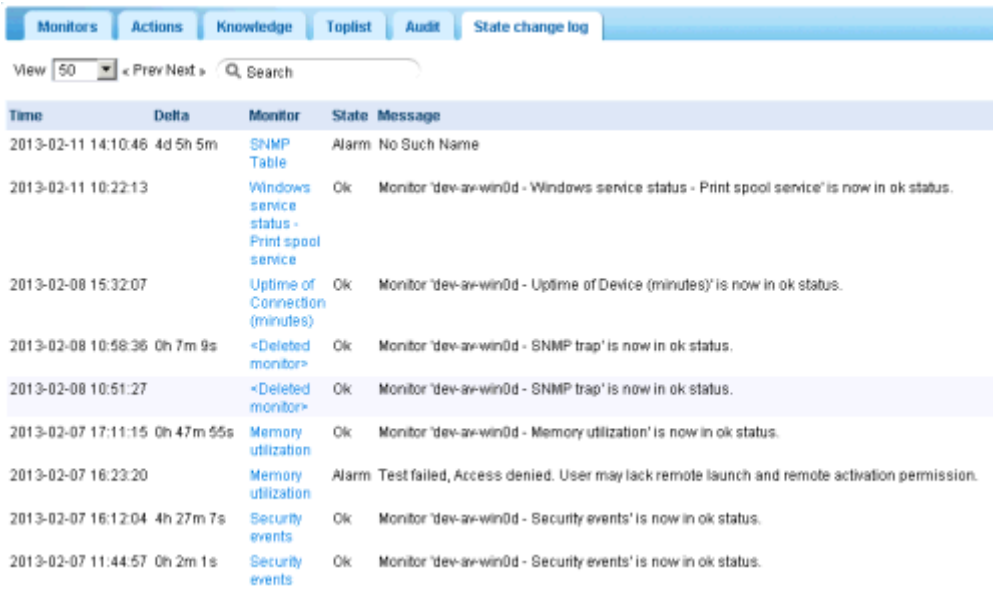
- **Name** - The name of the monitor.
- **Type** - The type of monitor.
- **Alarms** - The **alarm count** *(page 46)*. This column is only displayed on asset nodes.
- **Status** - The latest result returned from the monitor.
- **Next test** - The next time the test is scheduled to be run.

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.



Editing Assets

`<selected asset> > Edit`

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

- **Basic properties tab** *(page 42)* - Gateways, groups, and assets display a **Basic properties** edit tab.
- **Advanced tab** *(page 43)* - Gateways, groups, assets, and monitors display an **Advanced** edit tab.
- **Authentication tab** *(page 34)* - This edit tab displays with groups, gateways, and assets.
- **NOC tab** *(page 35)* - This edit tab displays with gateways, groups, and assets.
- **Tag tab** *(page 39)* - 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 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 58)* format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** *(page 49)* 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 - Always uses WMI.
  - Active directory monitor - Always uses WMI.
  - Bandwidth utilization monitor
  - CPU utilization monitor
  - Disk utilization monitor
  - Event log monitor
  - Memory utilization monitor
  - Swap file utilization monitor

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

Map and location settings

- **Inherit map settings** - If checked, **map settings** *(page 27)* 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 44)* 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 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

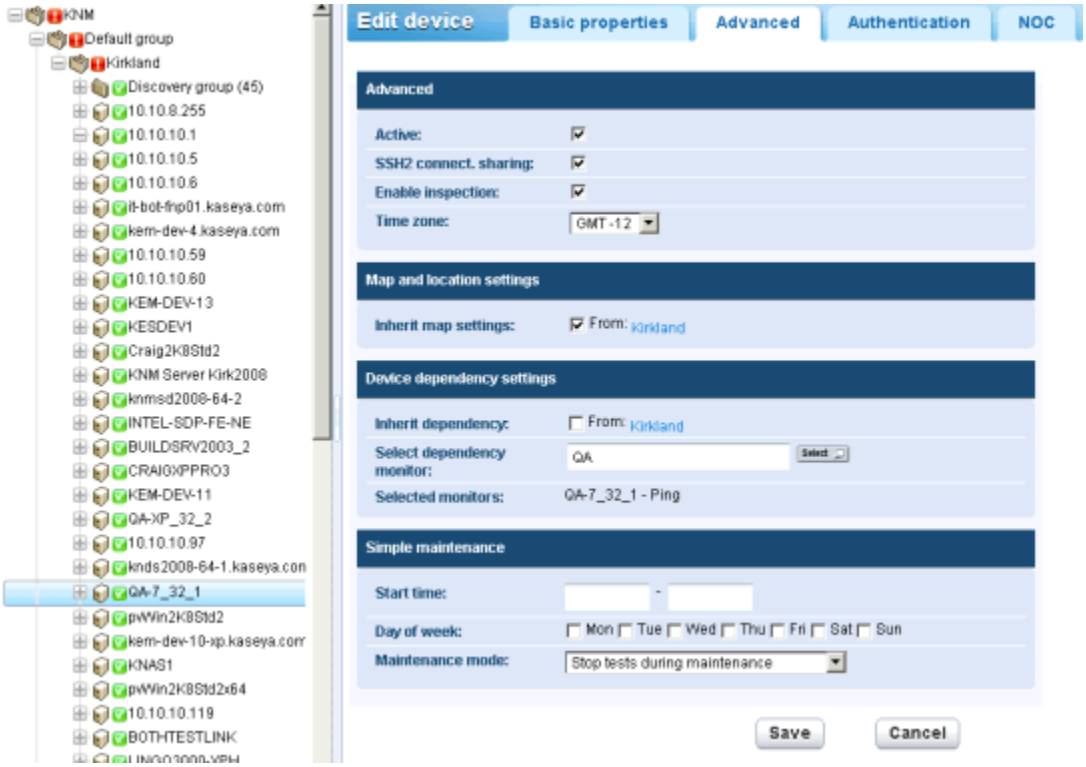
Dependencies are configured using the Advanced *(page 43)* edit tab of an assets node.

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.

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

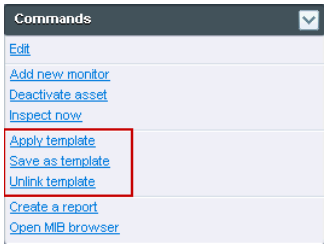
Configuring one monitor at a time for thousands of assets isn't practical. Instead configure a *set of monitors* using an asset template, then apply the asset template to the appropriate asset. You should have an asset template for each type of asset you manage.

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.

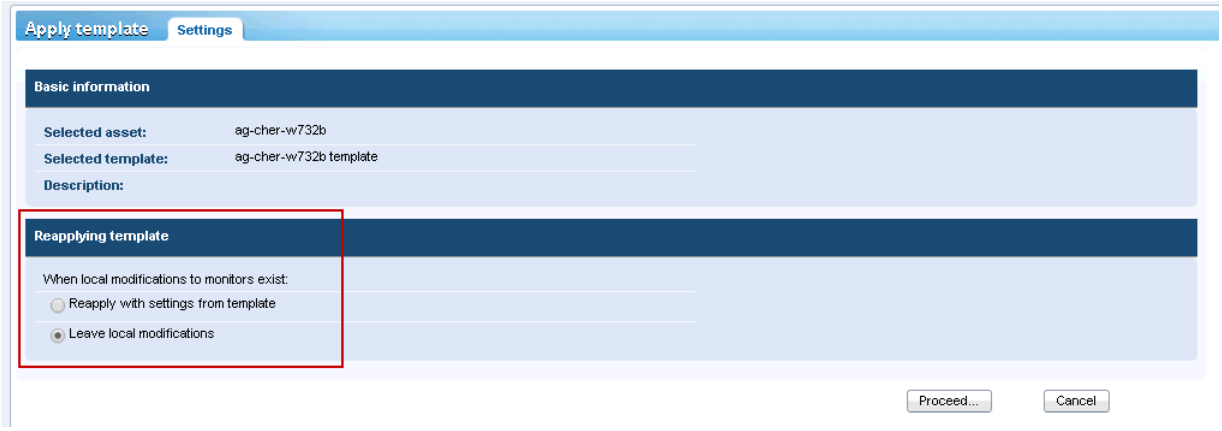
Applying Asset Templates to Assets

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 49)*.

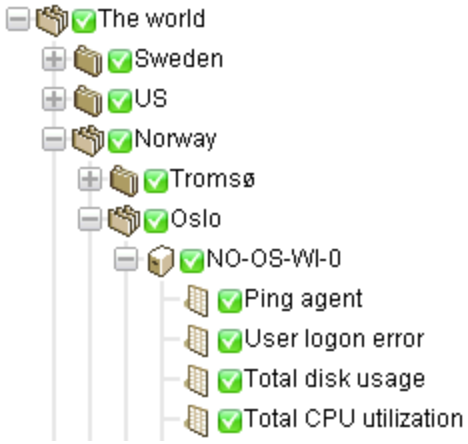
The alert status of each monitor—along with all other active monitors—is reported all the way up the monitor tree. If you are managing hundreds or thousands of monitors, this feature can quickly help you identify the individual monitor that is failing.

Alarm Status Progression

OK Status

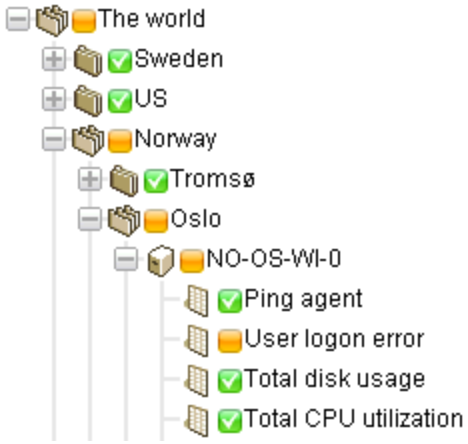
During normal operation, when a monitor is in the *OK* state, a green status icon displays next to the monitor in the monitor tree. Here is what the monitor tree looks like when all monitors are in the *OK*

state.



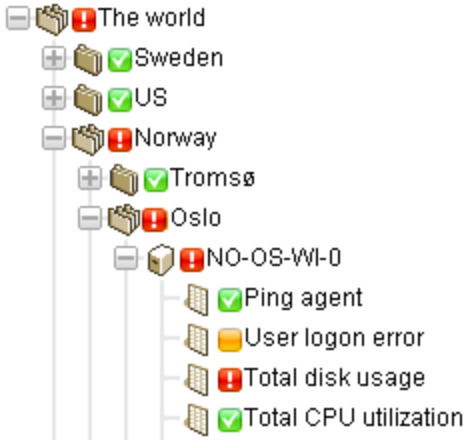
Failed Status

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.



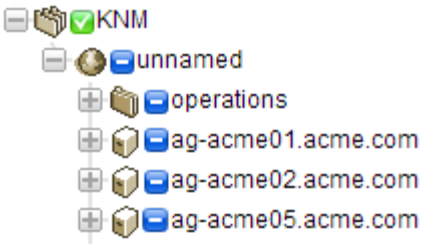
Alarm Status

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	48
Adding Monitors	52
Adding Preconfigured Monitors	53
Editing Monitors	54
Alarm Messages	58
Format Variables	59
Acknowledging Alarms	61

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 42)* 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 62)*.
- **Test now** - Tests the monitor immediately.

Views

- **Summary tab** *(page 41)* - This tab displays with monitors.
- **Actions tab** *(page 49)* - This tab displays with gateways, groups, assets, and monitors.
- **Audit tab** *(page 32)* - This tab displays with gateways, groups, assets, and monitors.
- **State change log tab** *(page 41)* - This tab displays with assets and monitors.
- **Simulate alarm tab** *(page 52)* - 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.

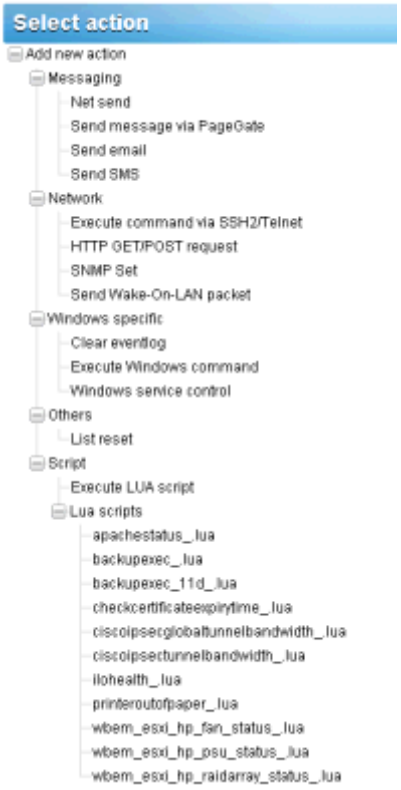
Recovery Actions

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.*

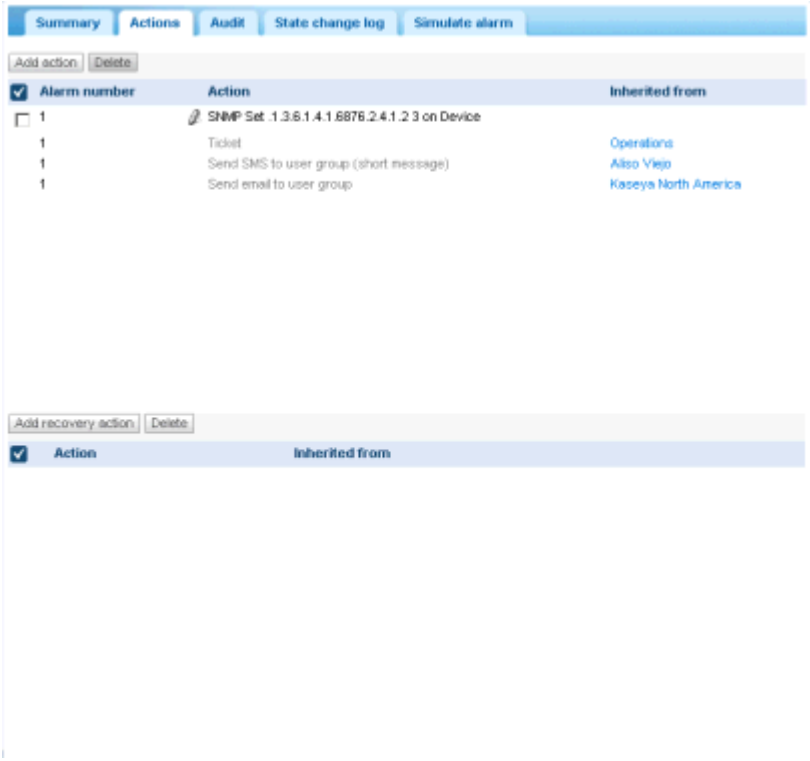
Adding Actions to the Actions tab

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 you can select.



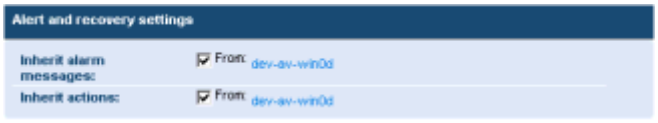
Managing Hierarchies of Actions and Recovery Actions

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.



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.



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.

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

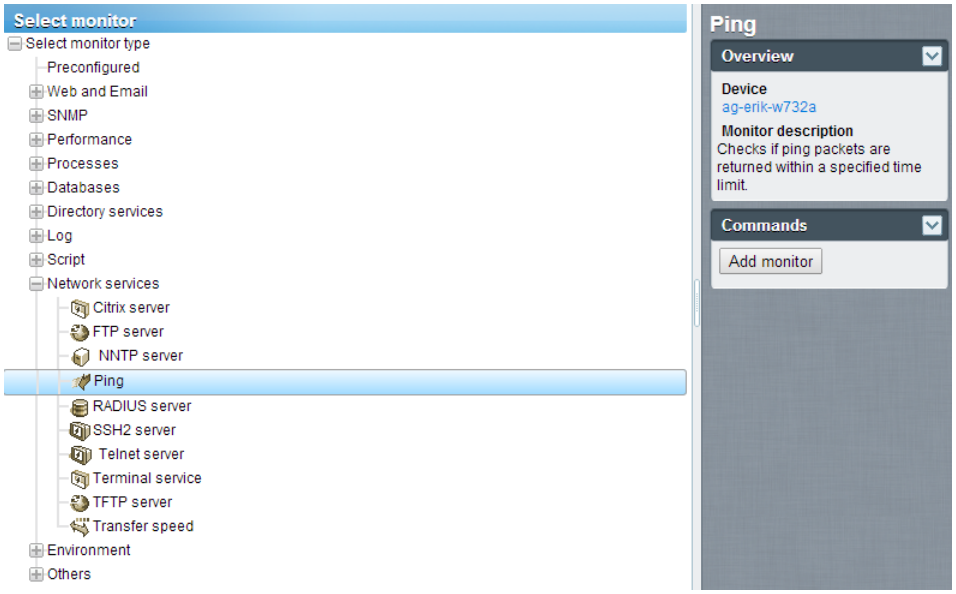
Adding Monitors

`<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—more than 40 and growing—displays. See Monitor Reference 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 54)*.

> **Note: Adding preconfigured monitors** *(page 53)* 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.

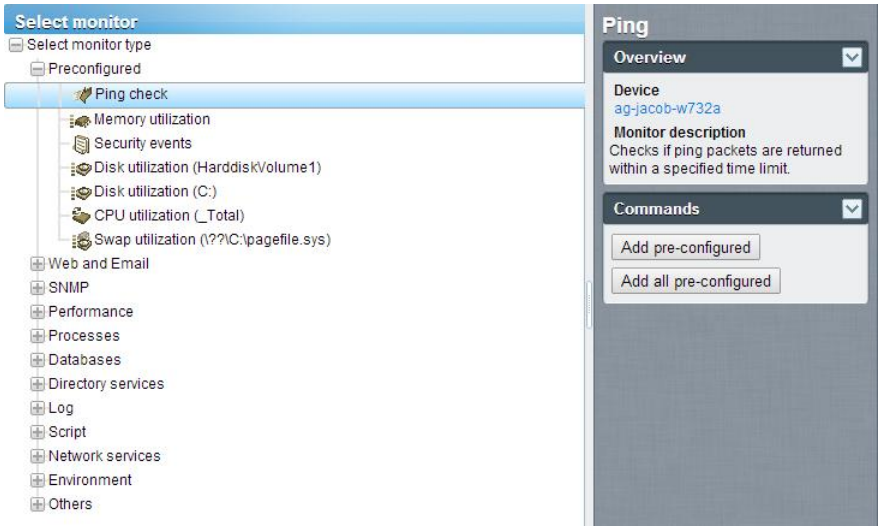
To add preconfigured monitors to an asset:

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 26)*.

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`

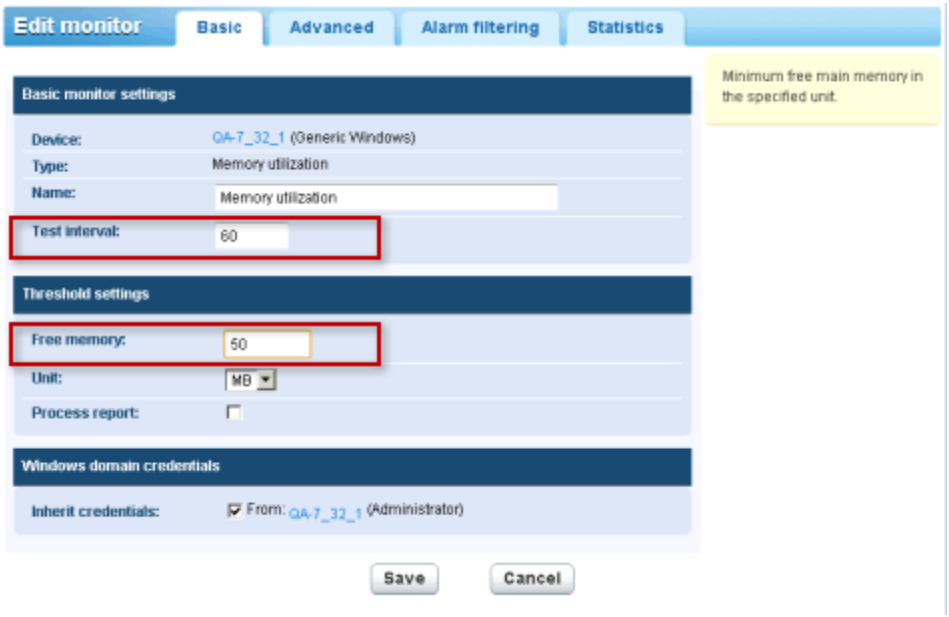
The **Edit monitor** tab sets the properties for monitors assigned to assets.

- **Basic tab** *(page 56)* - This edit tab displays with monitors.
- **Advanced tab** *(page 56)* - Gateways, groups, assets, and monitors display an **Advanced** edit tab.
- **Alarm filtering tab** *(page 57)* - This edit tab displays with monitors.
- **Statistics tab** *(page 57)* - This edit tab displays with monitors.

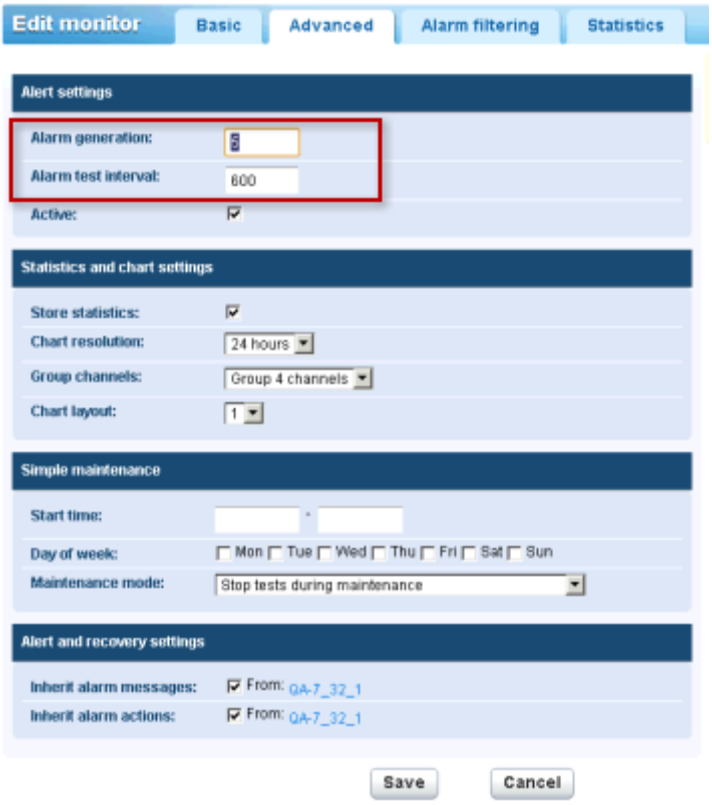
Example

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 for *monitor-specific settings*.



- 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.



- 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 then 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 46)*:
  - 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 for *monitor-specific settings*.

Basic tab

- **Asset** - The name of the asset.
- **Type** - The type of monitor. The identified operating system 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 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 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 then 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 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 58)* format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** *(page 49)* 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 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.

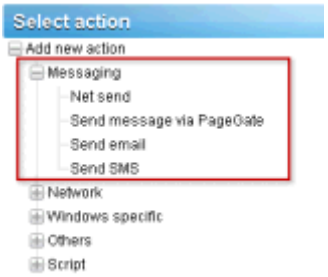
> **Note:** The following *standard monitor settings* display on most monitors. See the Monitor reference for *monitor-specific settings*.

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.

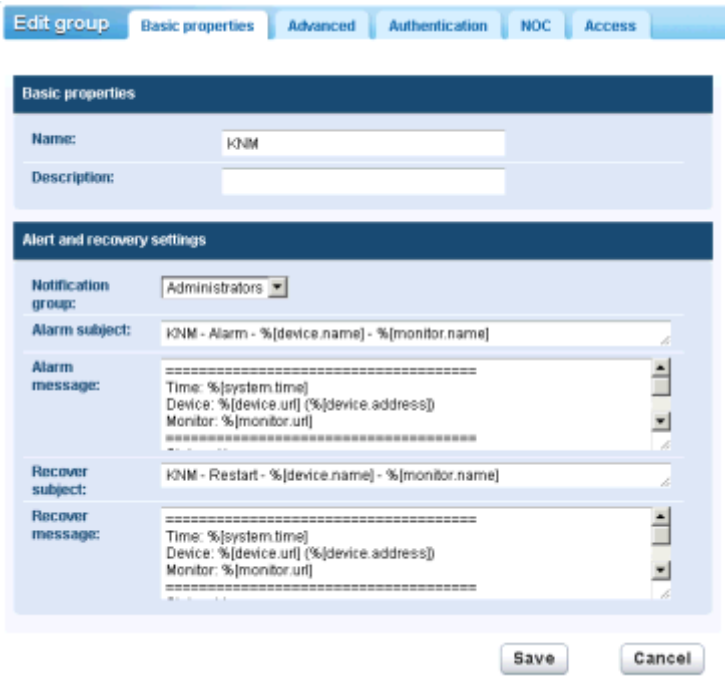
Alarm Messages

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

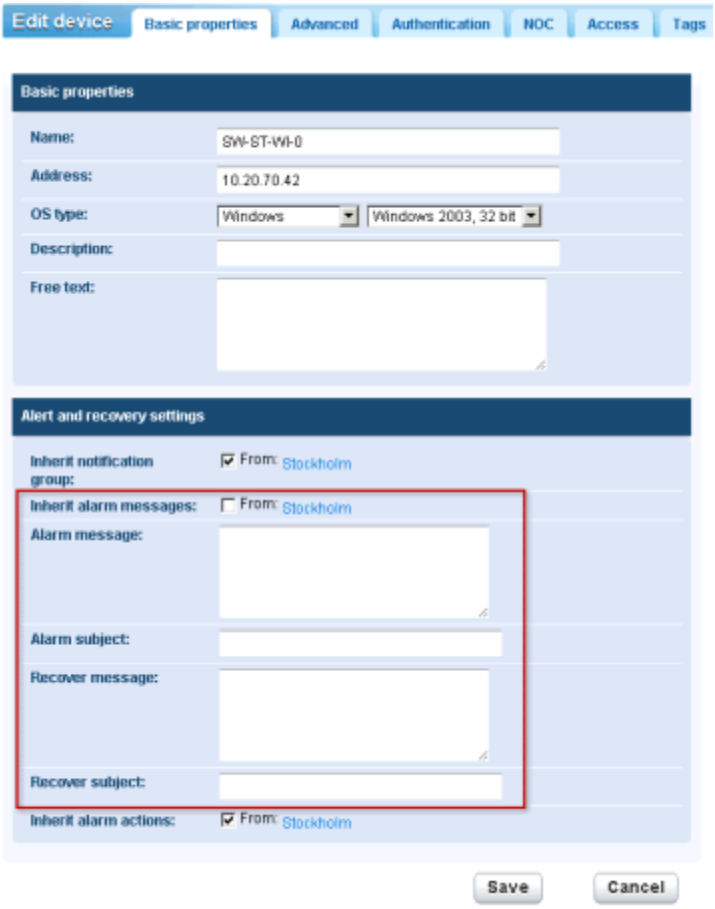
Several of the actions you can execute when an alarm fails a consecutive number of tests is the sending of messages.



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 59)* available to use.



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.



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.

%[system.time]	current time
%[system.time_hour]	24 hours formatting
%[system.time_hour2]	12 hours formatting
%[system.time_minute]	including minutes
%[system.time_second]	including seconds
%[system.date]	current date
%[system.date_year]	current date with full year
%[system.date_year2]	year without century
%[system.date_month]	month as number 01 - 12

%[system.date_day_of_month]	day of the month 01 - 31
%[system.date_weekday]	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
%[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 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 tab and applies to all nodes.

> **Note:** The **Format Variables** *(page 59)* 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, toplists, 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

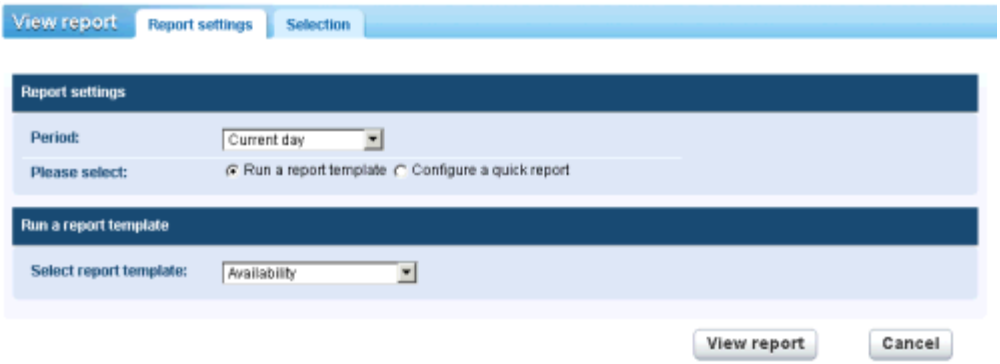
`<Select a node> > Create a report > View in Browser`

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 63)* 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

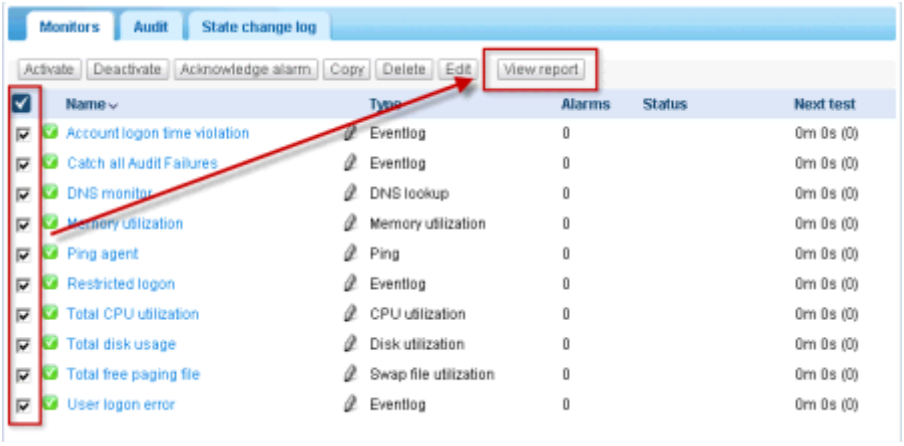
Use the **Selection** tab on the **View report** page to override the default selection of gateway or group, assets and monitors selected for either type of report.

Viewing Quick Reports

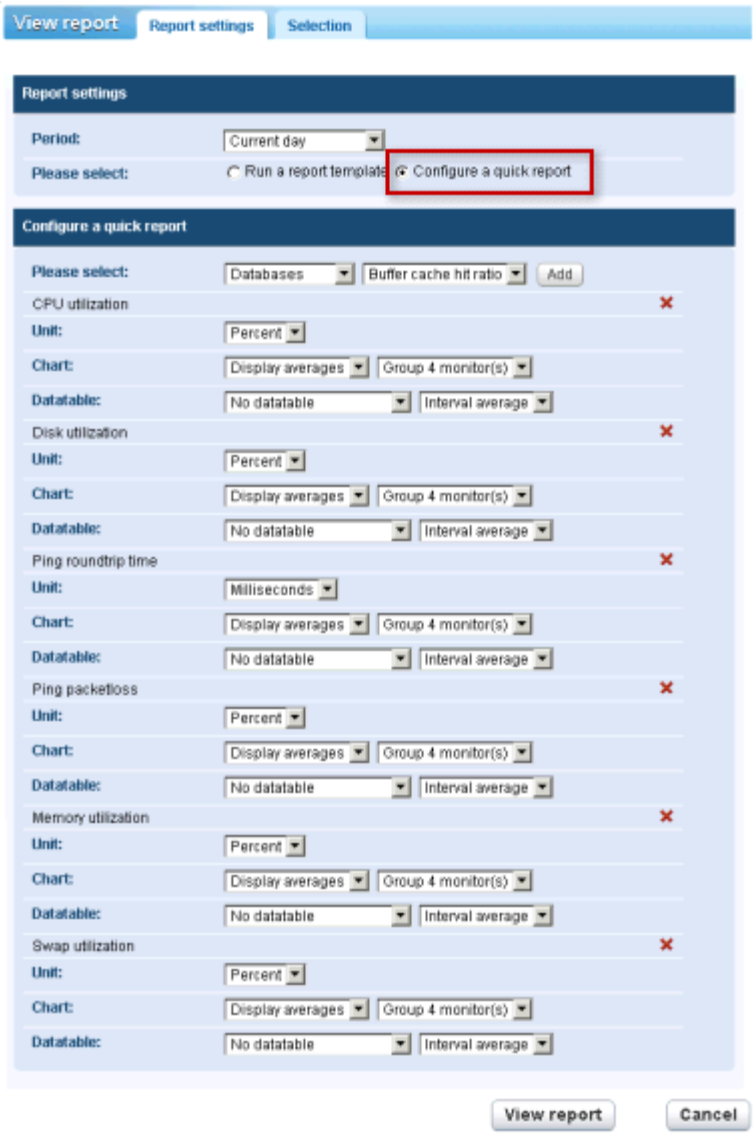
<Select a node> > <select monitors> > View report

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.



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.

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

Emailing and publishing reports

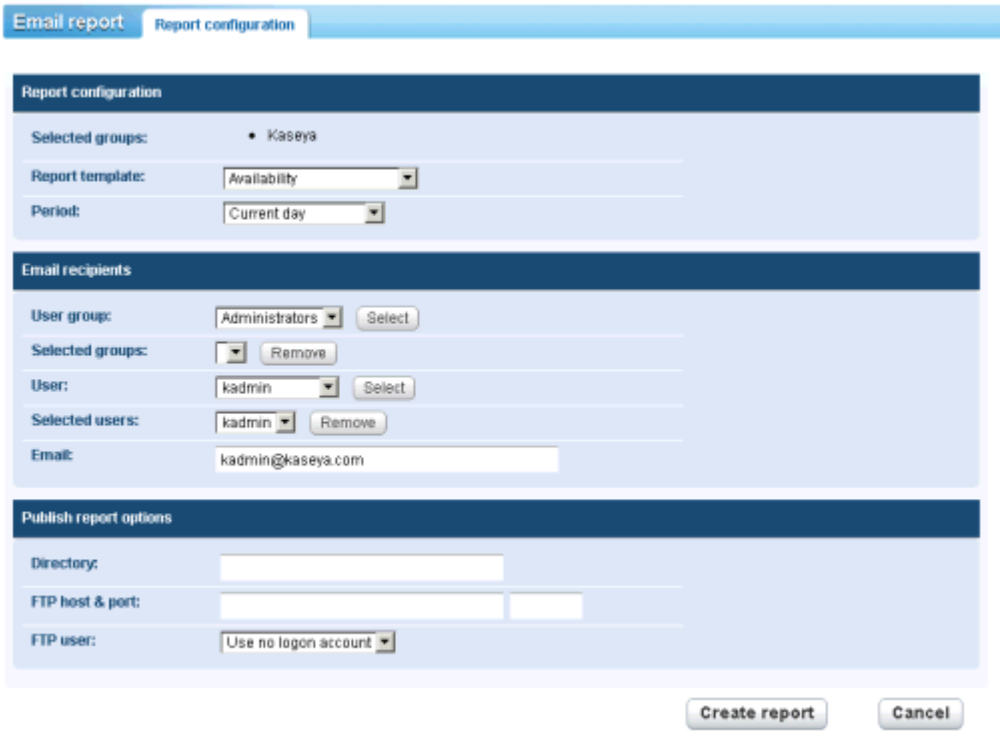
<Select a node> > Create a report > Email or publish

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

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.



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

Index

A

Acknowledging Alarms • 61
Actions tab • 49
Adding / Editing Groups • 37
Adding Monitors • 52
Adding Preconfigured Monitors • 53
Advanced edit tab - assets • 43
Advanced edit tab - gateways • 33
Advanced edit tab - groups • 38
Advanced edit tab - monitors • 56
Alarm filtering edit tab - monitors • 57
Alarm Messages • 58
Asset Commands and Views • 40
Asset Templates • 45
Assets • 40
Assets tab • 26
Audit tab • 32
Authentication edit tab • 34

B

Basic edit tab - monitors • 56
Basic properties edit tab - assets • 42
Basic properties edit tab - gateways • 33
Basic properties edit tab - groups • 38

C

Configuration Summary • 7
Crumbline • 10

D

Data Views • 13
Dependency Testing • 44

E

Edit Menus • 15
Editing Assets • 42
Editing Gateways • 32
Editing Monitors • 54
Emailing and publishing reports • 65

F

Format Variables • 59

G

Gateway Commands and Views • 25
Gateway Nodes and Network Discovery • 20
Gateways • 24
Getting Started • 8
Group Commands and Views • 37
Groups • 36

I

Inheritance • 10
Installing a New Instance of Network Monitor R91 • 3
Installing/Uninstalling Gateways • 21
Integration with Discovery • 19

K

Knowledge tab • 32

L

List View Controls • 12
List View Filtering • 12
Lists Views • 10

M

Map tab • 27
Migration of KNM standalone to KNM integrated • 4
Monitor Commands and Views • 48
Monitor tab • 41
Monitor tree • 9
Monitors • 46
Monitors tab • 27
Moving Nodes • 16

N

Navigation Panel Overview • 17
Network Monitor Licensing in the VSA • 24
Network Monitor Module Requirements • 2
Network Monitor Overview • 1
NOC edit tab • 35
Node and User Search • 11

O

Organizations and Machine Groups • 21

P

Pre-Installation Checklist • 2
Properties and Commands • 15

R

Renaming Gateways and Assets • 22
Reports • 62

S

Schedules tab • 30
Scheduling reports • 66
Server Sizing • 3
Simulate alarm tab • 52
State change log tab • 41
Statistics edit tab - monitors • 57
Summary tab • 49

T

Tags edit tab • 39
The Monitoring View • 8
Ticket action • 23
Toplist tab • 29

U

User Integration • 23

V

Viewing Customized Reports • 65
Viewing Quick Reports • 63
Viewing Report Templates • 62
VSA Integration • 17