Kaseya

Kaseya 2

Network Monitor

Quick Start Guide

for Network Monitor 5.0

October 18, 2013

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULA 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."

©2013 Kaseya. All rights reserved. | www.kaseya.com

Contents

Getting Started

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. How This Quick Start Guide is Organized

1. **Network Monitor** Concepts
2. Installation and Setup
3. Configuring Network Monitor - Provides a step-by-step, "first time" demonstration of how to configure Network Monitor.

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 devices on your network, using the recommendations in **Server Sizing** *(page 2)*. 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.
3. If you choose to use a specified Windows account instead of the default (local system), ensure the Windows account used by the **Network Monitor** service has **sufficient privileges** *(page 2)*.
4. If ODBC logging is going to be enabled, create a ODBC system data source on the **Network Monitor** host machine.
5. If a GSM phone is used, install it and verify that it responds correctly to standard AT commands in a terminal program.

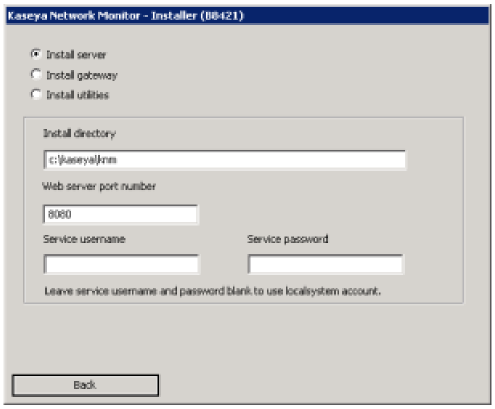
When completed you are ready to install **Network Monitor**. After installing **Network Monitor** and connecting to the web interface for the first time, consult the topic **Running the KNM Startup Guide** *(page 3)*.

Server, Gateway or Utilities Installation

During a `KNMsetup.exe` install, clicking the **Options** button displays the following choices.

- **Install server** - *Selected by default*. If monitoring a single subnet, select this option. **Recommended for first time evaluations.**
- **Install gateway** - If monitoring an additional subnet for a server that is already installed, use this option.
- **Utilities** - Select this option to install specialized utilities. These utilities are not required. There are four utilities installed:
  - `gizmo.exe` - The Gizmo system tray application.
  - `ide.exe` - The Lua Development Environment
  - `dme.exe` - The Dashboard Map Editor.

- `mibcompiler.exe` - The MIB Compiler utility.



Kaseya Network Monitor - Installer (88421)

● Install server
○ Install gateway
○ Install utilities

Install directory: c:\kaseya\knm

Web server port number: 8080

Service username:

Service password:

Leave service username and password blank to use localsystem account.

Server Sizing

Minimum requirements for using the free version of **Network Monitor**.

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

Network Monitor 5.0 Module Requirements

Systems Hosting the Network Monitor Server

- Windows 2003, 2008, or 2008 R2 with the latest service pack
- Network Monitor comes with its own database and HTTP server
- Microsoft .Net Framework 4.5 or later

Supported Browsers

- Microsoft Internet Explorer 7.0 or later
- Opera 9.0 or later
- Firefox 3.5 or later (Recommended for best viewing experience)

The following features must be enabled in your browser settings.

- Accept third party cookies - Cookies are required to keep track of the user session.
- Javascript enabled - Java scripts are used by the web interface and must be enabled.

Dashboard Map Editor utility

- Microsoft .Net Framework 4.0 or later

Selecting a Service Account

`Kaseya Network Monitor` is a Windows service that is installed to logon using a service account.

Using the LocalSystem account

The built-in LocalSystem account is the default service account assigned to the Kaseya Network Monitor service when installing. While the LocalSystem account is the most convenient way to get **Network Monitor** up and running, it has many privileges that are unnecessary to run **Network Monitor** locally.

> **Note:** We recommend the Kaseya Network Monitor service be assigned a service account using the *fewest number of privileges possible.* The **Network Monitor** account manager can then be used to impersonate Windows accounts with elevated permissions when these permissions are required for tests, actions and events.

Network Monitor Required Privileges

Network Monitor requires the service account it is assigned to have the following file system permissions:

- READ, WRITE and EXECUTE to **Network Monitor** base directory
- READ, WRITE, MODIFY to all sub-directories

The service account may also require the Act as part of operating system privilege to enable Windows account impersonations. Consult your Windows documentation to determine if this privilege must be added.

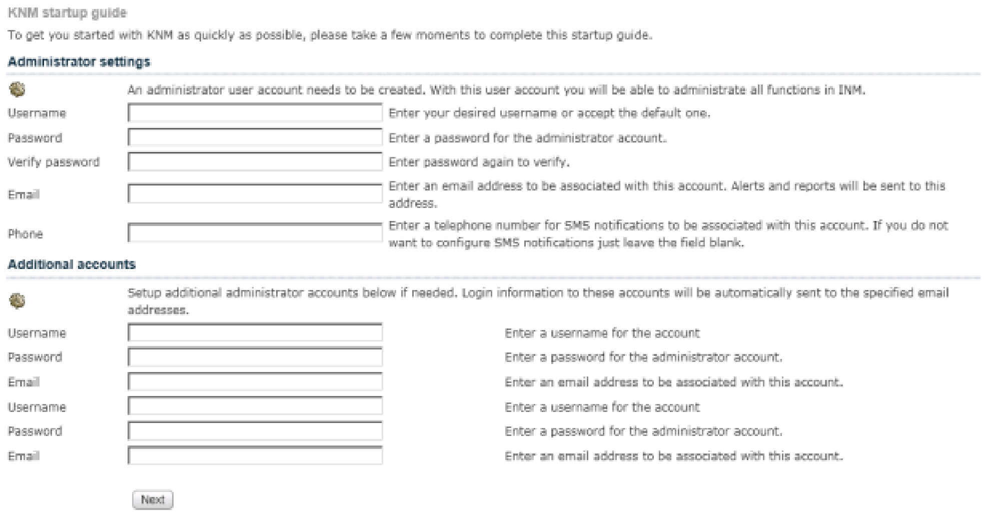
Running the KNM Startup Guide

The **Server install** displays a series of web pages called the **KNM Startup Guide** to help you configure **Network Monitor** for first time use. The **Startup Guide** has five steps.

- **Administrator Settings** *(page 4)*
- **Gateway Server Settings** *(page 4)*
- **Mail Settings** *(page 5)*
- **SMS Device Configuration** *(page 5)*
- **Credentials Used with Network Discovery** *(page 6)*

> **Note:** A person logging into the **Network Monitor** server is referred to as a *user*. Each user can only have one logon *session* open at one time.

Administrator Settings



KNM startup guide

To get you started with KNM as quickly as possible, please take a few moments to complete this startup guide.

Administrator settings

An administrator user account needs to be created. With this user account you will be able to administrate all functions in INM.

Username	Enter your desired username or accept the default one.
Password	Enter a password for the administrator account.
Verify password	Enter password again to verify.
Email	Enter an email address to be associated with this account. Alerts and reports will be sent to this address.
Phone	Enter a telephone number for SMS notifications to be associated with this account. If you do not want to configure SMS notifications just leave the field blank.

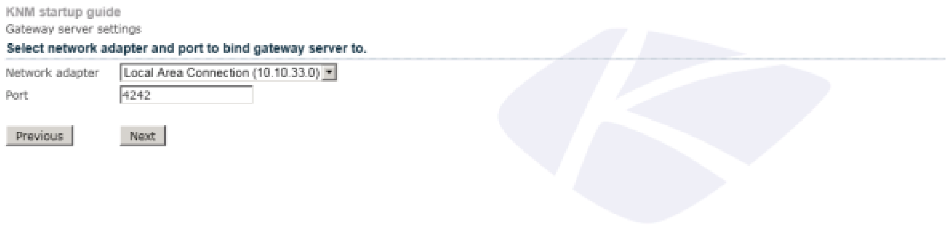
Additional accounts

Setup additional administrator accounts below if needed. Login information to these accounts will be automatically sent to the specified email addresses.

Username	Enter a username for the account
Password	Enter a password for the administrator account.
Email	Enter an email address to be associated with this account.
Username	Enter a username for the account
Password	Enter a password for the administrator account.
Email	Enter an email address to be associated with this account.

1. Enter the username and password of the default **Network Monitor**user. Passwords are case sensitive.
2. Configure an email address for this user. The email address is used when **Network Monitor** is sending notifications or reports.
3. Optionally configure a phone number for this user. The phone number is used when **Network Monitor** is sending SMS notifications.
4. Clicking **Next** creates the default user record you will use to logon to **Network Monitor** after completing the **KNM Startup Guide**.

Gateway Server Settings



KNM startup guide

Gateway server settings

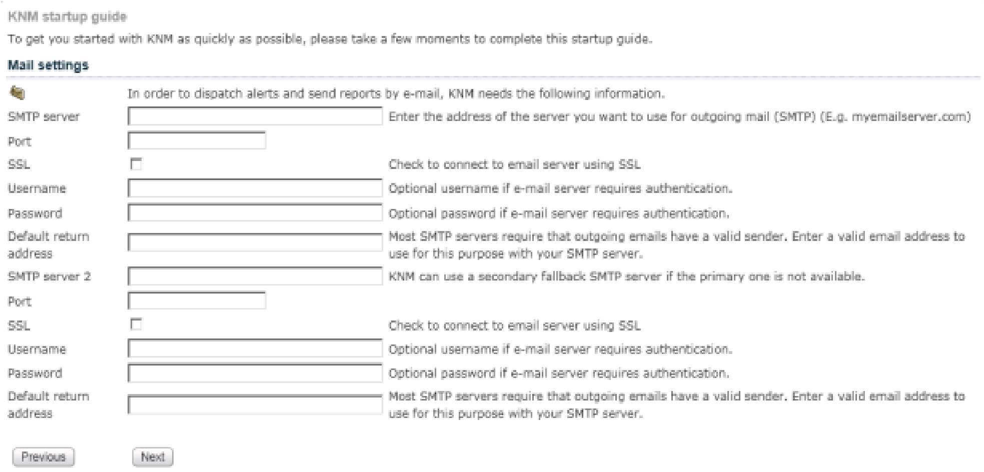
Select network adapter and port to bind gateway server to.

Network adapter	Local Area Connection (10.10.33.0)
Port	4242

This is the IP address and port the *server listens to for incoming gateway data*. All gateways you install are populated with this IP address and port by default.

> **Note:** If the **Network adaptor** drop-down list is blank, *do not proceed*. Without an IP address specified here, the web interface and gateways will not be able to locate the server. Cancel the install and reinstall **Network Monitor** on a different machine that displays a value in this drop-down list.

Mail Settings



KNM startup guide

To get you started with KNM as quickly as possible, please take a few moments to complete this startup guide.

Mail settings

	In order to dispatch alerts and send reports by e-mail, KNM needs the following information.	
SMTP server		Enter the address of the server you want to use for outgoing mail (SMTP) (E.g. myemailserver.com)
Port		
SSL	□	Check to connect to email server using SSL
Username		Optional username if e-mail server requires authentication.
Password		Optional password if e-mail server requires authentication.
Default return address		Most SMTP servers require that outgoing emails have a valid sender. Enter a valid email address to use for this purpose with your SMTP server.
SMTP server 2		KNM can use a secondary fallback SMTP server if the primary one is not available.
Port		
SSL	□	Check to connect to email server using SSL
Username		Optional username if e-mail server requires authentication.
Password		Optional password if e-mail server requires authentication.
Default return address		Most SMTP servers require that outgoing emails have a valid sender. Enter a valid email address to use for this purpose with your SMTP server.

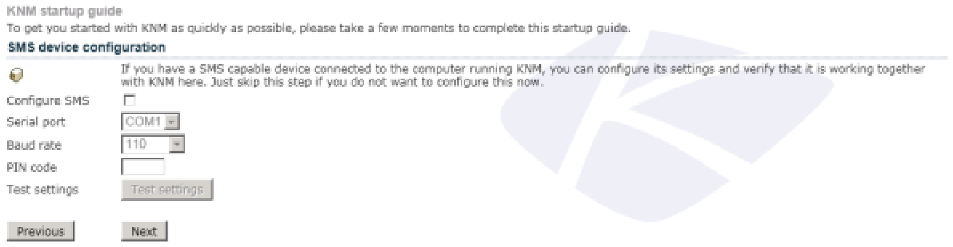
To send email notifications and reports you need to configure the email server settings. Two email servers can be configured: a primary server and a secondary backup server used in case the primary server is unreachable.

- **SMTP server** - Enter the host name of the primary email server. If your server requires credentials when sending mail, enter those below. If you are uncertain leave the username and password fields blank.
- **Port** - Uses 25 if left blank.
- **SSL** - If checked, uses SSL to connect to the email server.
- **User Name** - If required for authentication, enter the username of an account authorized to use the host email server.
- **Password** - If required for authentication, enter the password of the account.
- **Default return address** - Use the format `Display Name <email address>` or just an email address. If no display name is entered, the default display name is `KNM`.

Enter similar information for the **SMTP server 2** set of fields.

If you want to skip this step and configure these parameters later, click **Next** to continue. Use the menu > **Mail, SMS and messaging** page after you logon to update these settings.

SMS Device Configuration



KNM startup guide

To get you started with KNM as quickly as possible, please take a few moments to complete this startup guide.

SMS device configuration

If you have a SMS capable device connected to the computer running KNM, you can configure its settings and verify that it is working together with KNM here. Just skip this step if you do not want to configure this now.

Configure SMS	□
Serial port	COM1
Baud rate	110
PIN code	
Test settings	Test settings

If you have an SMS device connected to a COM port on the **Network Monitor** host you can configure **Network Monitor** to send SMS notifications.

- **Configure SMS** - Select this box if you have an SMS device connected to the **Network Monitor** host.
- **Com port** - Select the serial port the SMS device is connected to.

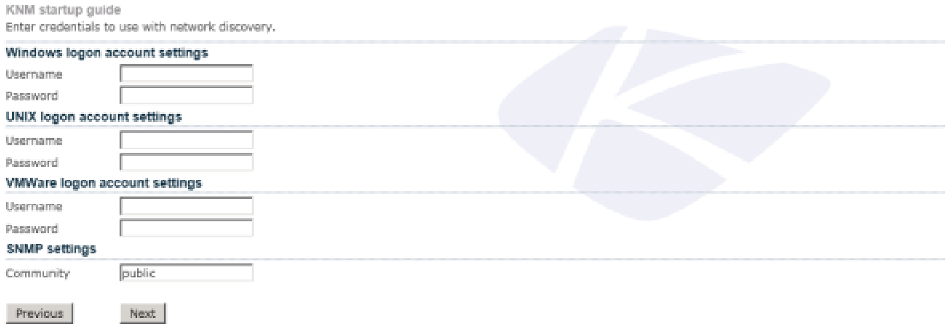
- **Baud rate** - Select the baud rate. This is the speed the SMS device is capable of sending and receiving over the COM port. A setting of 2400 is recommended, if you're not sure what to select.
- **PIN code** - If your SMS device is a GSM phone or modem, you might need to unlock the SIM card with a PIN code. Enter that PIN code in the PIN code field.
- **Test settings** - Click the button to test the configuration, if the test fails make necessary changes or uncheck the **Configure SMS** check box to skip this part of the wizard.

User phone number

If you did not enter a phone number on the **Administrator Settings** *(page 4)* step of the **KNM Startup Guide** you can enter it using the menu > **My settings** page after you logon. Without the phone number in a user record Network Monitor is unable to send an SMS notification to that user.

> **Note:** See SMS settings for information.

Credentials Used with Network Discovery



KNM startup guide

Enter credentials to use with network discovery.

Windows logon account settings

Username

Password

UNIX logon account settings

Username

Password

VMWare logon account settings

Username

Password

SNMP settings

Community: public

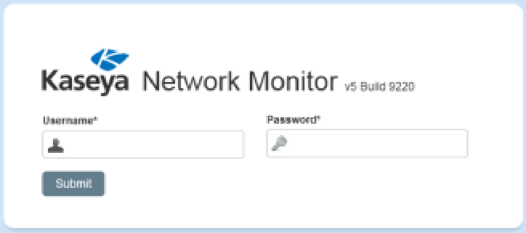
Network discovery is automatically performed on the local network immediately after the install. Enter a set of credentials that matches the devices *on the server's local network.* Credentials can always be added after the install and network discovery run again.

- **Windows logon account settings** - An administrator level Windows credential is required to return some types of scan data from Windows devices. Use the `domain\username` format to enter a domain username.
- **UNIX logon account settings** - An administrator level UNIX credential is required to return some types of scan data from UNIX devices.
- **SNMP settings** - Enter the SNMP community name used by devices *on the server's local subnet*.

> **Note:** The community name, SNMP version, and port used used by Network Monitor to connect to an SNMP device is set on the **Authentication** *(page 33)* tab of a device node. The device node may inherit this setting from a parent node. See the **Installation Checklist** *(page 1)*.

Logging On

After installing Network Monitor, the logon page displays.



Enter the username and password you specified on the **Administrator Settings** *(page 4)* page.

If you closed your browser, you can re-display the logon page using one of the following two methods. From the **Network Monitor** host:

- Click the link to the web interface in the **Network Monitor** program folder in the start menu.
- Use the following link `http://localhost:8080`

> **Note:** This link above assumes you accepted the standard parameters during the installation and the **Network Monitor** web server is running on the default `8080` port. If you have installed **Network Monitor** on a different host, replace the localhost host name with the name of the **Network Monitor** host.

Shutting Down Network Monitor

A standalone **Network Monitor** installation consists of three different services:

- `Kaseya Network Monitor`
- `Kaseya Record Manager`
- `Kaseya Local Gateway`

When upgrading to a new release of **Network Monitor**, you will need to shut down two of these services for the upgrade process to work. Another reason for shutting down **Network Monitor** could be maintenance work, such as moving to another server.

- On the Windows system hosting **Network Monitor** locate the Administrative Tools > Services > `Kaseya Network Monitor` service.
- Right-click the service and select **Stop**.
- Confirm the `Kaseya Record Manager` also stops. This service automatically stops when shutting down the `Kaseya Network Monitor` service.
- If performing maintenance on the server running **Network Monitor**, also stop the `Kaseya Local Gateway` service.
- It can take a while for the `Kaseya Network Monitor` service to shut down. **Network Monitor** has to finish the monitor tests that are currently running.
- The services automatically start again after an upgrade installation finishes.

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULA 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."

©2013 Kaseya. All rights reserved. | www.kaseya.com

Getting Started

In This Section

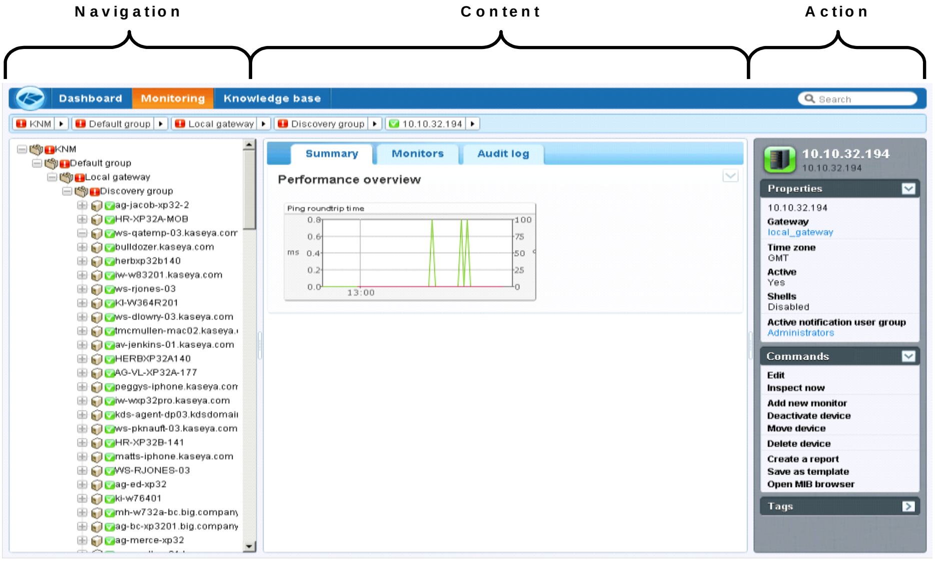
Monitoring

Network Monitor > Monitoring

The **Monitoring** module is the main module you use to configure **Network Monitor**. The **Monitoring** module is organized into three main panels:

- **Navigation** - Selects the group, gateway, device or monitor you want to work with.
- **Content** - Displays user content and settings—such as devices, 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.



10.10.32.194

Gateway
local_gateway

Time zone
GMT

Active
Yes

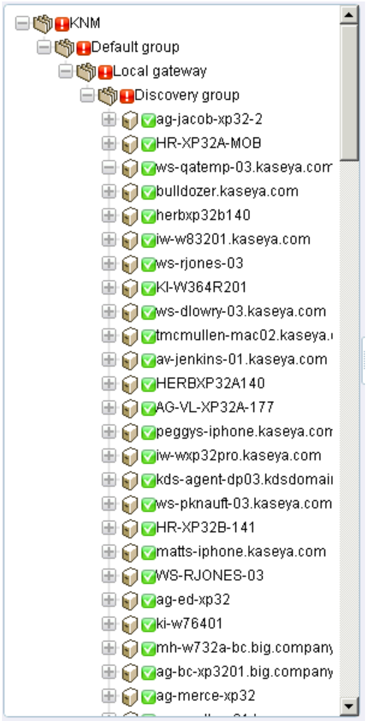
Shells
Disabled

Active notification user group
Administrators

Navigation

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

- **Groups** - Used to group other nodes on the navigation tree. Groups do not correspond to a physical device on a network. Think of them as representing logical business units, such as companies or departments, or a set of devices within a network.
  - ➢ A node cannot be the child of more than one parent. This includes a group node.
  - ➢ Groups can have sub-groups.
  - ➢ Groups can be added above or below a gateway.
- **Gateways** - A gateway monitors devices 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.
- **Devices** - Anything with an IP address. This includes computers, routers, switchers, mobile devices, printers, firewalls, etc.
- **Monitors** - A monitor runs a specific test on a device and reports the result back to the server. A device can have multiple monitors.

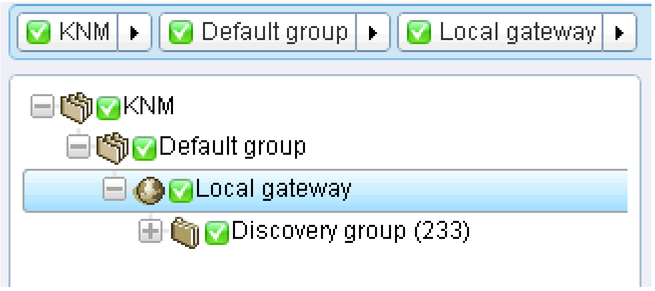


Default Group and Local Gateway

Immediately after a new install of **Network Monitor** v5.0, you'll notice the navigation tree displays a `KNM` at the highest level, then a `Default group`, then a `Local gateway`. All three levels were created for you during the install.

- `Default group` - A **Groups** *(page 25)* typically represents a logical business unit. In this case the `Default group` initially represents *your own business unit.*

- `Local gateway` - A **gateway** *(page 39)* listens to devices on a network. The `Local gateway` listens for devices on *your own network*.

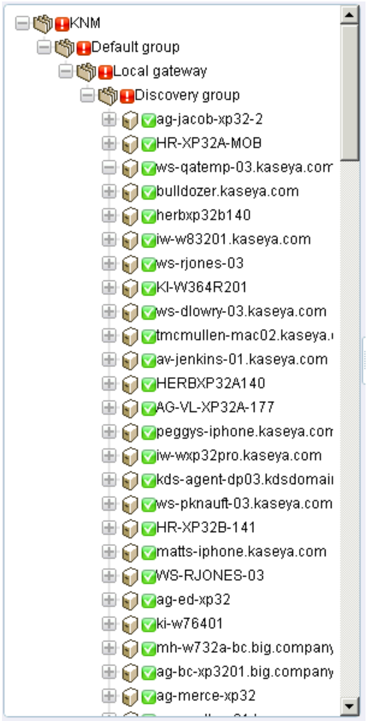


KNM
Default group
Local gateway
Discovery group (233)

If you like, rename both of these nodes to reflect your own business name. Add additional groups and gateways as needed, for the customers you manage.

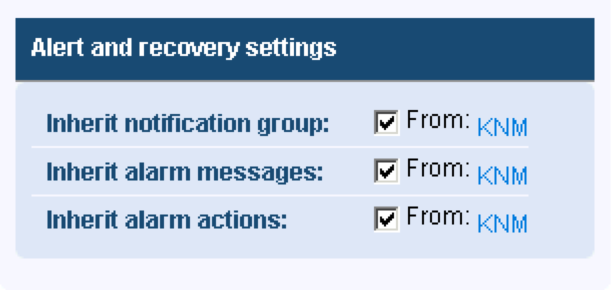
Inheritance

Certain node properties can be **inherited** by nodes at a lower level. This design enhancement, new in KNM v5.0, affects nearly every other aspect of configuration. With inheritance you can propagate configuration changes to hundreds, even thousands, of devices and monitors effortlessly, simply by making changes to a higher level node in the navigation tree.



KNM
Default group
Local gateway
Discovery group
ag-jacob-xp32-2
HR-XP32A-MOB
ws-qatemp-03.kaseya.com
bulldozer.kaseya.com
herbxp32b140
iw-w83201.kaseya.com
ws-rjones-03
KI-W364R201
ws-dlowry-03.kaseya.com
tmcmullen-mac02.kaseya.
av-jenkins-01.kaseya.com
HERBXP32A140
AG-VL-XP32A-177
peggys-iphone.kaseya.com
iw-wxp32pro.kaseya.com
kds-agent-dp03.kdsdomai
ws-pknauft-03.kaseya.com
HR-XP32B-141
matts-iphone.kaseya.com
WS-RJONES-03
ag-ed-xp32
ki-w76401
mh-w732a-bc.big.company
ag-bc-xp3201.big.company
ag-merce-xp32

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



Alert and recovery settings

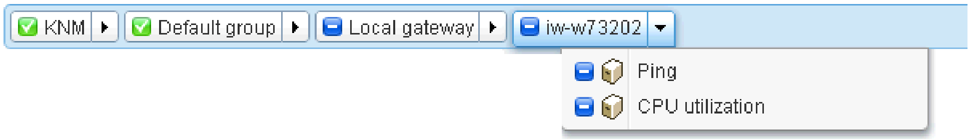
Inherit notification group: ☑ From: KNM

Inherit alarm messages: ☑ From: KNM

Inherit alarm actions: ☑ From: KNM

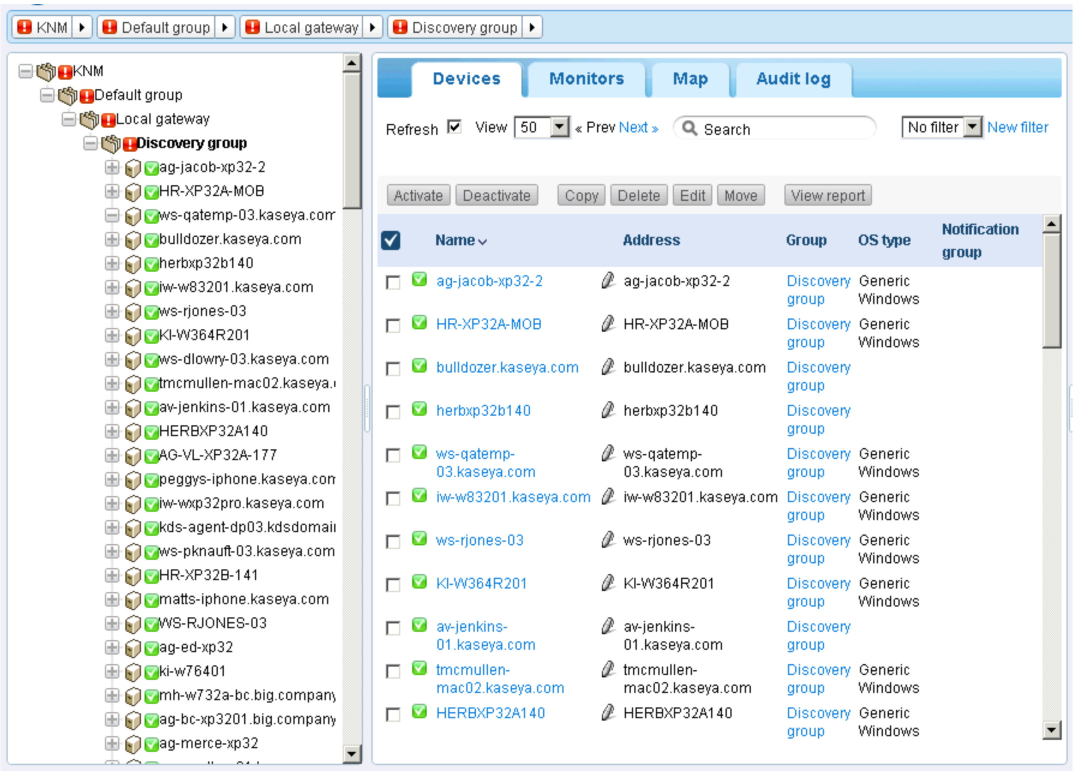
Crumbline

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



Lists Views

The middle panel shows the content of any node selected in the navigation tree. If the selected node is a group, gateway or device, you'll see a list like the one below.



KNM
Default group
Local gateway
Discovery group
ag-jacob-xp32-2
HR-XP32A-MOB
ws-qatemp-03.kaseya.com
bulldozer.kaseya.com
herbxp32b140
iw-w83201.kaseya.com
ws-rjones-03
KI-W364R201
ws-dlowry-03.kaseya.com
tmcmullen-mac02.kaseya.
av-jenkins-01.kaseya.com
HERBXP32A140
AG-VL-XP32A-177
peggys-iphone.kaseya.com
iw-wxp32pro.kaseya.com
kds-agent-dp03.kdsdomai
ws-pknauft-03.kaseya.com
HR-XP32B-141
matts-iphone.kaseya.com
WS-RJONES-03
ag-ed-xp32
ki-w76401
mh-w732a-bc.big.company
ag-bc-xp3201.big.company
ag-merce-xp32

☑		Name	Address	Group	OS type	Notification group
□	✓	ag-jacob-xp32-2	ag-jacob-xp32-2	Discovery group	Generic Windows	
□	✓	HR-XP32A-MOB	HR-XP32A-MOB	Discovery group	Generic Windows	
□	✓	bulldozer.kaseya.com	bulldozer.kaseya.com	Discovery group		
□	✓	herbxp32b140	herbxp32b140	Discovery group		
□	✓	ws-qatemp-03.kaseya.com	ws-qatemp-03.kaseya.com	Discovery group	Generic Windows	
□	✓	iw-w83201.kaseya.com	iw-w83201.kaseya.com	Discovery group	Generic Windows	
□	✓	ws-rjones-03	ws-rjones-03	Discovery group	Generic Windows	
□	✓	KI-W364R201	KI-W364R201	Discovery group	Generic Windows	
□	✓	av-jenkins-01.kaseya.com	av-jenkins-01.kaseya.com	Discovery group		
□	✓	tmcmullen-mac02.kaseya.com	tmcmullen-mac02.kaseya.com	Discovery group	Generic Windows	
□	✓	HERBXP32A140	HERBXP32A140	Discovery group	Generic Windows	

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

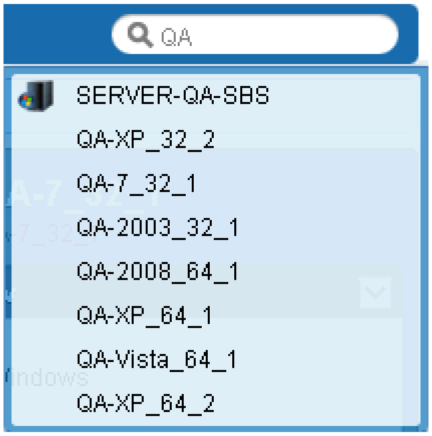
- The **Devices** tab displays all the *devices* that are members of the selected node in the hierarchy.
- The **Monitors** tab displays all the *monitors* that are member of the selected node in the hierarchy.

Searches

A **Search** edit box displays in the upper right hand corner. Enter a string to search the navigation tree for all *group*, *gateway* and *device* 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.

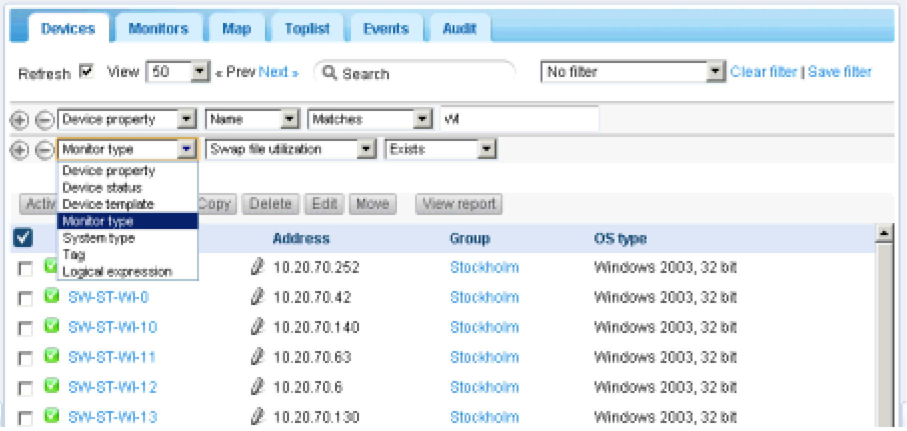


QA

SERVER-QA-SBS
QA-XP_32_2
QA-7_32_1
QA-2003_32_1
QA-2008_64_1
QA-XP_64_1
QA-Vista_64_1
QA-XP_64_2

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 search a list. Click a column header to sort the list by that column.



Device property | Name | Matches | WI

Monitor type | Swap file utilization | Exists

☑		Address	Group	OS type
□		10.20.70.252	Stockholm	Windows 2003, 32 bit
□	SW-ST-WI-0	10.20.70.42	Stockholm	Windows 2003, 32 bit
□	SW-ST-WI-10	10.20.70.140	Stockholm	Windows 2003, 32 bit
□	SW-ST-WI-11	10.20.70.63	Stockholm	Windows 2003, 32 bit
□	SW-ST-WI-12	10.20.70.6	Stockholm	Windows 2003, 32 bit
□	SW-ST-WI-13	10.20.70.130	Stockholm	Windows 2003, 32 bit

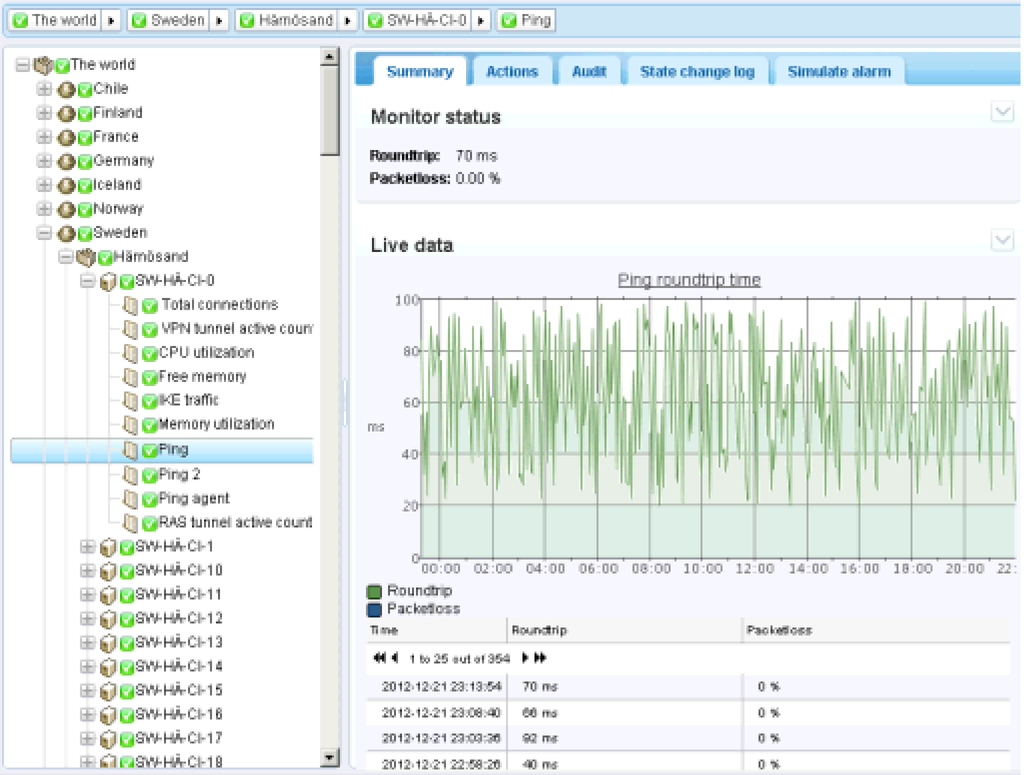
Filtering

Group and gateway list views can be filtered by *multiple conditions*. Types of filters include:

- Device property -
- Device status
- Device template - The device or monitor is or is not associated with a device template.
- System type
- Tag
- Logical expression

Data Views

If the node selected in the navigation tree is a monitor, the middle pane shows the data returned by that monitor.



Monitor status

Roundtrip: 70 ms
Packetloss: 0.00 %

Time	Roundtrip	Packetloss
1 to 25 out of 354		
2012-12-21 23:13:54	70 ms	0 %
2012-12-21 23:08:40	66 ms	0 %
2012-12-21 23:03:36	92 ms	0 %
2012-12-21 22:58:26	40 ms	0 %

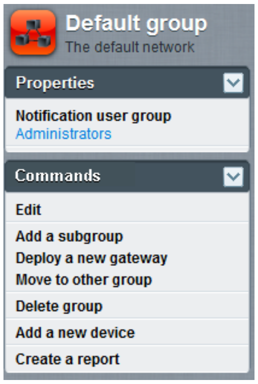
Properties and Commands

When a group, gateway, device 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 subgroup
- Add a new device



Default group
The default network

Properties

Notification user group
Administrators

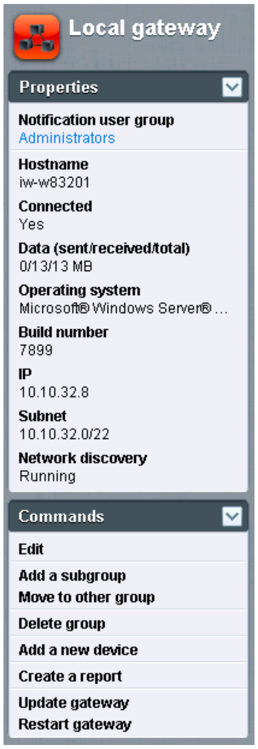
Commands

Edit
Add a subgroup
Deploy a new gateway
Move to other group
Delete group
Add a new device
Create a report

Gateway Commands

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

- Edit
- Add a subgroup
- Add a new device



Local gateway

Properties

Notification user group
Administrators

Hostname
iw-w83201

Connected
Yes

Data (sent/received/total)
0/13/13 MB

Operating system
Microsoft® Windows Server® ...

Build number
7899

IP
10.10.32.8

Subnet
10.10.32.0/22

Network discovery
Running

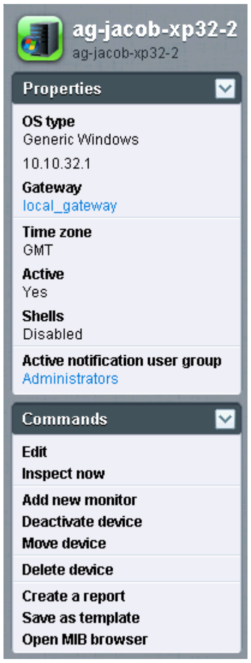
Commands

Edit
Add a subgroup
Move to other group
Delete group
Add a new device
Create a report
Update gateway
Restart gateway

Device Commands

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

- Edit
- Add new monitor



ag-jacob-xp32-2
ag-jacob-xp32-2

Properties

OS type
Generic Windows

10.10.32.1

Gateway
local_gateway

Time zone
GMT

Active
Yes

Shells
Disabled

Active notification user group
Administrators

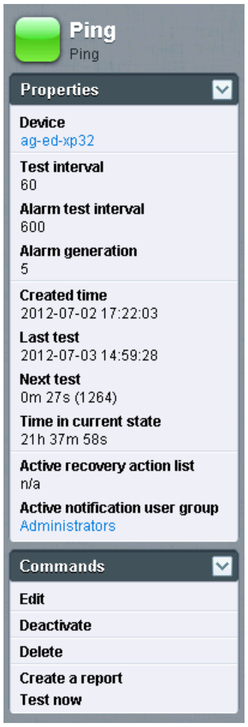
Commands

Edit
Inspect now
Add new monitor
Deactivate device
Move device
Delete device
Create a report
Save as template
Open MIB browser

Monitor Commands

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

- Edit
- Test Now



Ping
Ping

Properties

Device
ag-ed-xp32

Test interval
60

Alarm test interval
600

Alarm generation
5

Created time
2012-07-02 17:22:03

Last test
2012-07-03 14:59:28

Next test
0m 27s (1264)

Time in current state
21h 37m 58s

Active recovery action list
n/a

Active notification user group
Administrators

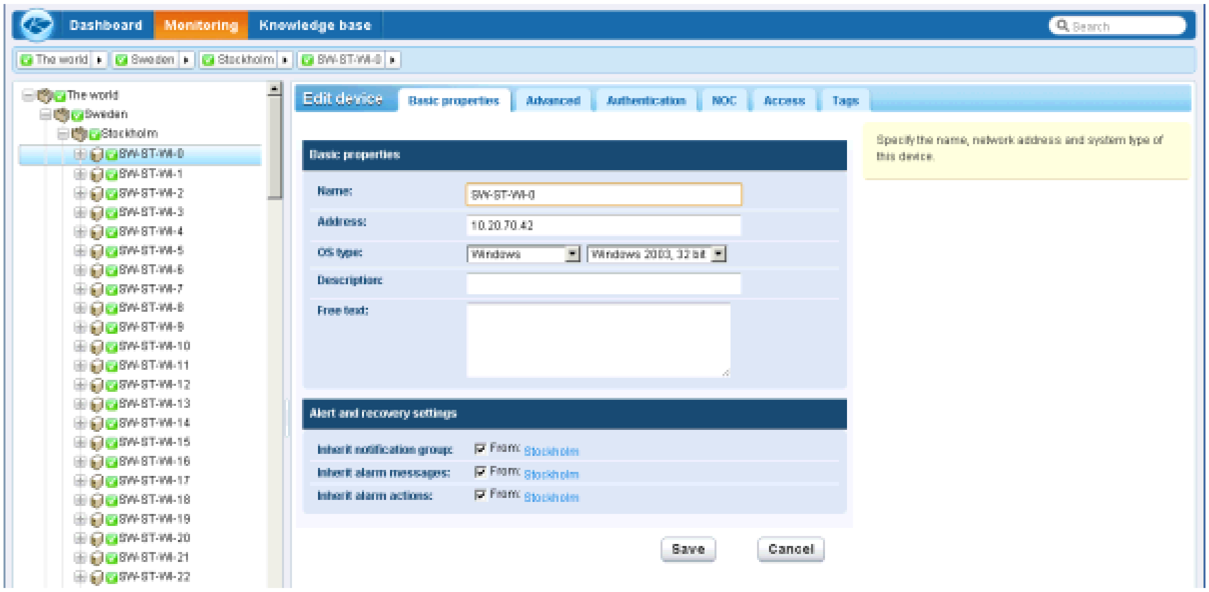
Commands

Edit
Deactivate
Delete
Create a report
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 14)* or **Data View** *(page 16)* of the selected node.



Specify the name, network address and system type of this device.

Basic properties

Name: SW-ST-WI-0

Address: 10.20.70.42

OS type: Windows | Windows 2003, 32 bit

Description:

Free text:

Alert and recovery settings

Inherit notification group: ☑ From: Stockholm

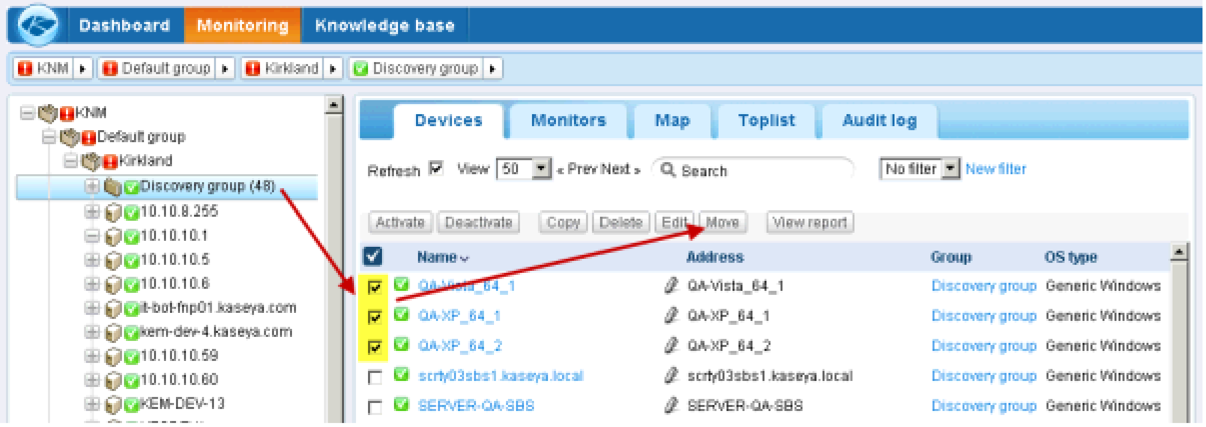
Inherit alarm messages: ☑ From: Stockholm

Inherit alarm actions: ☑ From: Stockholm

Moving Nodes

Let's take a look at how the navigation tree can be reorganized by moving one branch of the navigation tree to the next. We'll use the example of moving discovered devices out of a `Discovery group`.

> **Note: Network discovery** *(page 45)* requires *moving* discovered devices out of any `Discovery group` to start generating alert notifications.



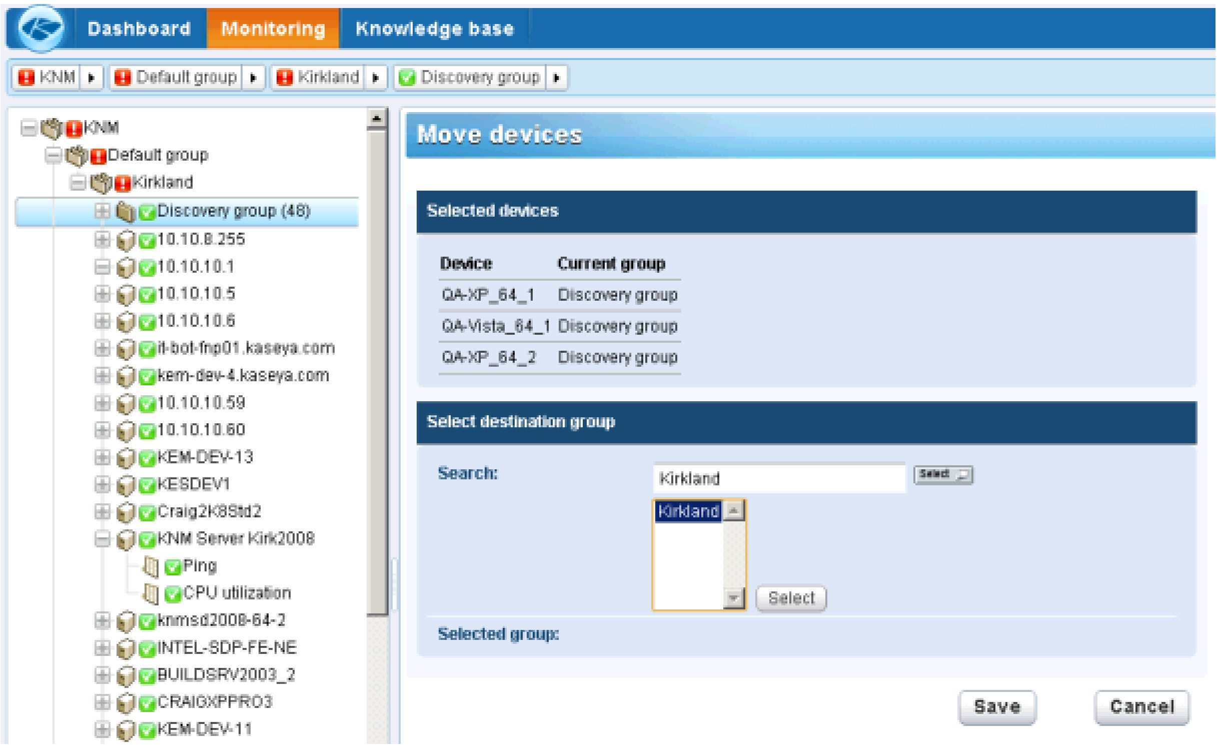
	Name	Address	Group	OS type
☑	QA-Vista_64_1	QA-Vista_64_1	Discovery group	Generic Windows
☑	QA-XP_64_1	QA-XP_64_1	Discovery group	Generic Windows
☑	QA-XP_64_2	QA-XP_64_2	Discovery group	Generic Windows
□	scrty03sbs1.kaseya.local	scrty03sbs1.kaseya.local	Discovery group	Generic Windows
□	SERVER-QA-SBS	SERVER-QA-SBS	Discovery group	Generic Windows

1. Select the `Discovery group` node.

   > **Note:** Use any group of devices to practice this procedure if a `Discovery group` node is not available.

2. Select the devices you want to move from the list view.

3. Click the **Move** button. The **Move devices** page displays.



Selected devices

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

Select destination group

Search: Kirkland

Kirkland

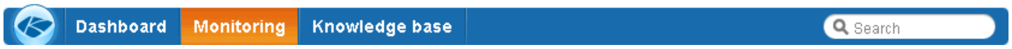
Selected group:

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 navigation tree.

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

Menu Bar

A menu bar is always available at the top of the **Network Monitor** browser window. Click any *module* in the menu bar to access different collections of data, resources and options.

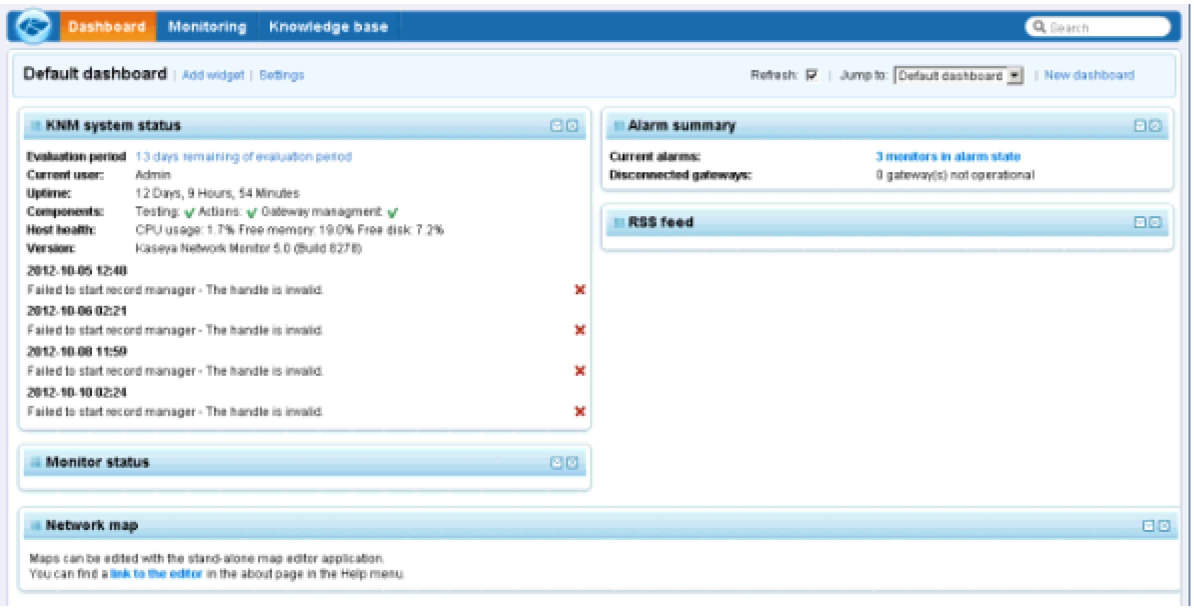


- - The "K" menu defines global settings and values, independent of any one node in the navigation tree.
- **Dashboard** - The **Dashboard** *(page 20)* displays a single page view of the status of all networks and devices you are monitoring
- **Knowledge base** - The **Knowledge base** *(page 22)* provides user-defined articles on how to use **Network Monitor** effectively. Articles can be linked to specific nodes in **Monitoring** navigation tree.

Dashboard

Network Monitor > Dashboard

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



Default dashboard

Jump to: Default dashboard

KNM system status

Evaluation period	13 days remaining of evaluation period
Current user:	Admin
Uptime:	12 Days, 9 Hours, 54 Minutes
Components:	Testing: ✓ Actions: ✓ Gateway managment: ✓
Host health:	CPU usage: 1.7% Free memory: 19.0% Free disk: 7.2%
Version:	Kaseya Network Monitor 5.0 (Build 8278)

2012-10-05 12:40
Failed to start record manager - The handle is invalid. ✖

2012-10-06 02:21
Failed to start record manager - The handle is invalid. ✖

2012-10-08 11:59
Failed to start record manager - The handle is invalid. ✖

2012-10-10 02:24
Failed to start record manager - The handle is invalid. ✖

Alarm summary

Current alarms:	3 monitors in alarm state
Disconnected gateways:	0 gateway(s) not operational

RSS feed

Monitor status

Network map

Maps can be edited with the stand-alone map editor application.
You can find a link to the editor in the about page in the Help menu.

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

- Status widgets
  - Monitor status
  - Device status
  - Group status
  - Gateway status
  - User status
  - System status
  - Alarm summary
  - NOC widget
- Map widgets
  - Network map
  - Network map, small
- Misc widgets
  - Web page
  - Web page, small
  - Favourited items
  - Log entries
  - Toplists
  - Notepad
  - RSS feed - *This is a new type of widget provided with* **Network Monitor** *v5.0.*

Click **Settings** to create or edit a dashboard. Click **Add widget** to add widgets to a dashboard.

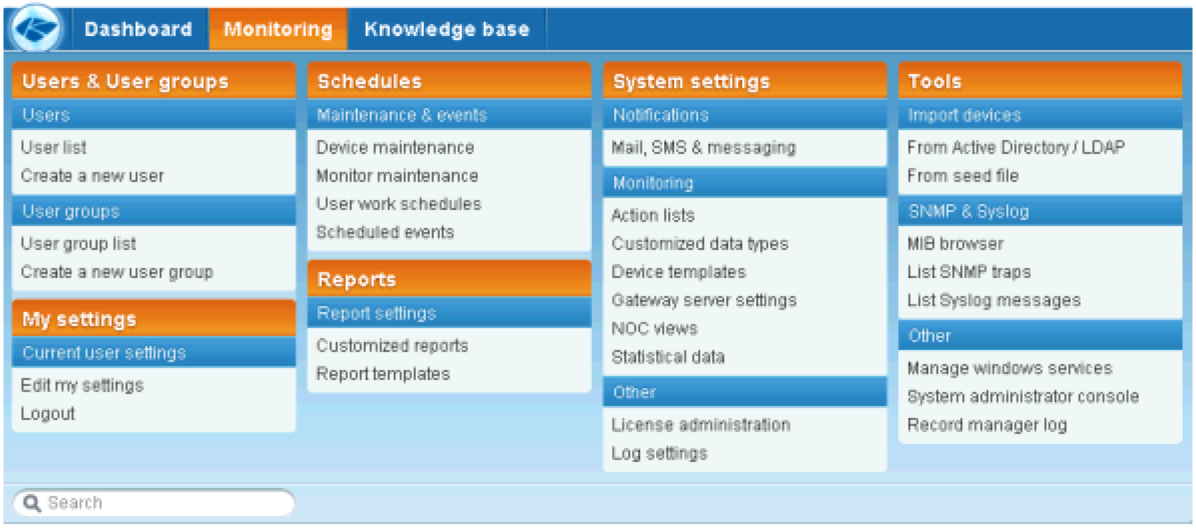
The K Menu

Network Monitor >

The module at the top of the page defines global settings and values, independent of any one node in the navigation tree. Examples include:

- Users and user groups
- Report templates
- Device templates
- Maintenance schedules
- Notifications

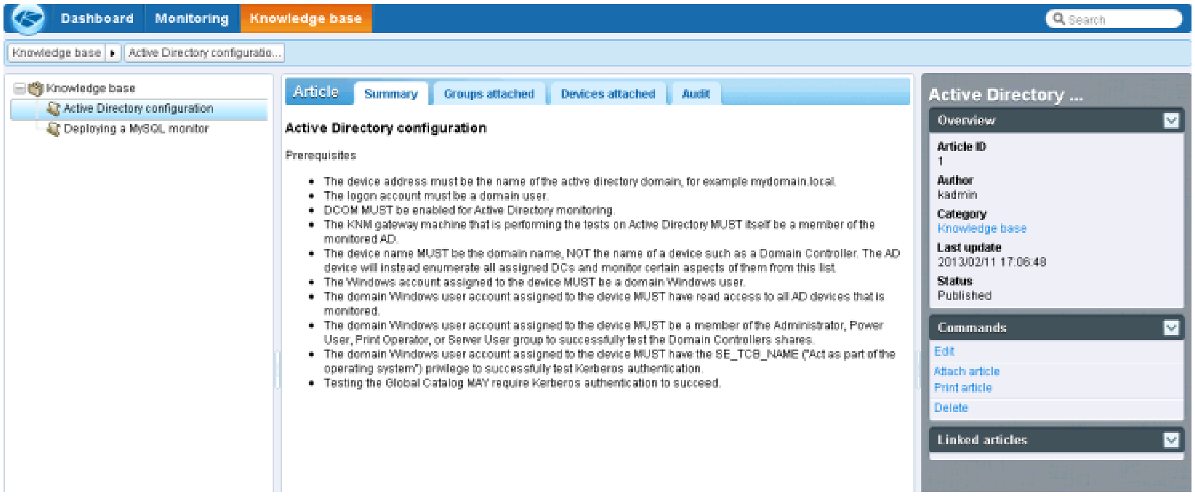
Note: See the K Menu Reference for more information.



Knowledge Base Articles

Network Monitor > Knowledge base

The **Knowledge base** enables you to create a shared set of "how to" articles that can be assigned to any group, gateway, device or monitor. This provides you with instant access the to exact reference material you need to troubleshoot and manage devices. Click any group, gateway or device node and select the **Knowledge** *(page 31)* tab to see the list of **Knowledge base** articles assigned to that node.



Active Directory configuration

Prerequisites

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

Article ID
1
Author
kadmin
Category
Knowledge base
Last update
2013/02/11 17:06:48
Status
Published

Related Topics

- **Knowledge tab** *(page 31)*
- **Knowledge Base Categories** *(page 23)*

View tabs

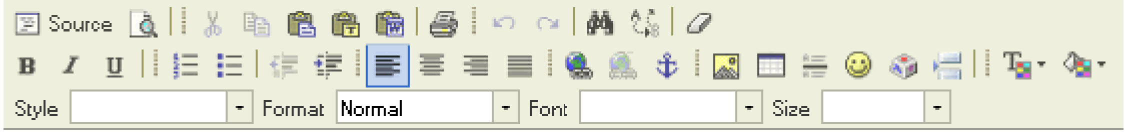
- **Summary** - Displays the article.
- **Groups attached** tab - Lists the groups attached to the current article. Optionally attaches or detaches the current article to groups and devices.
- **Devices attached** tab - Lists the devices attached to the current article. Optionally attaches or detaches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

Commands

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

Edit tabs

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



The more advanced toolbar buttons are described below.

➢ - Source - Enables you to edit the HTML tags controlling the format of the article.

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

See also:

- **Knowledge Base Categories** *(page 23)*
- **Knowledge tab** *(page 31)*

Knowledge Base Categories

A knowledge base **category** is a knowledge base folder containing other categories or knowledge base articles. Clicking an category in the knowledge base tree lists all the articles in the middle panel that are either descendants of that category or *explicitly linked* to that category. Articles are explicitly linked to categories using the **Advanced** *(page 22)* edit tab when editing an article.

Related Topics

- **Knowledge Base Articles** *(page 22)*
- **Knowledge tab** *(page 31)*

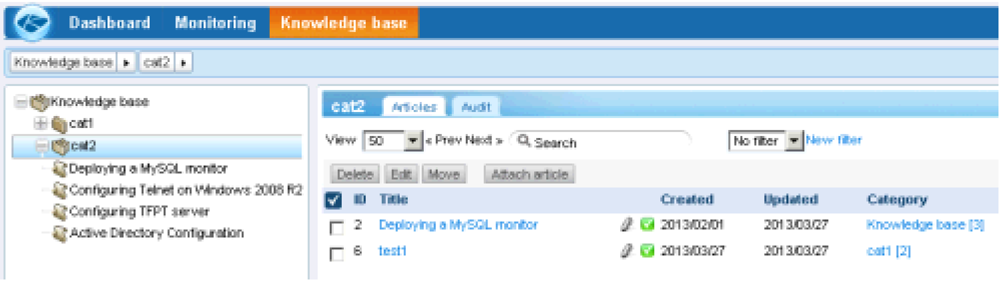
Actions

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

Commands

- **Edit** - Edits a selected article.

- **Add a subcategory** - Adds a subcategory to the current category.
- **Delete category** - Deletes the current category.
- **Create a new article** - Creates a new article subordinate to the current category.



☑	ID	Title		Created	Updated	Category
□	2	Deploying a MySQL monitor	✓	2013/02/01	2013/03/27	Knowledge base [3]
□	6	test1	✓	2013/03/27	2013/03/27	cat1 [2]

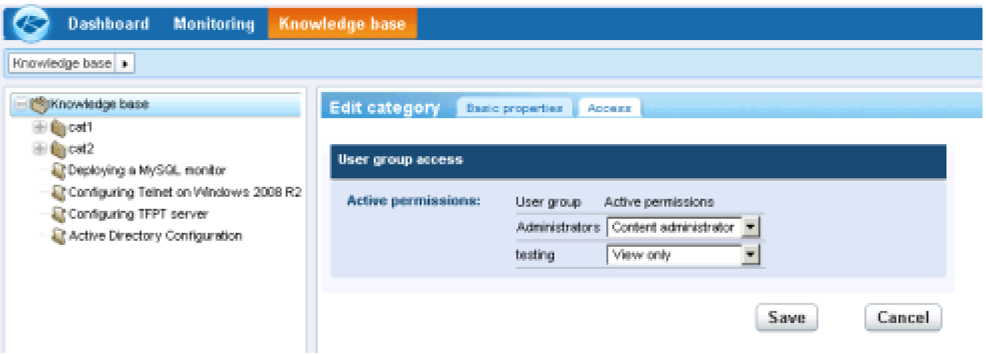
Edit tabs

Basic properties tab

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

Access tab

User rights to view or modify an article are set by category and are optionally *inherited* from higher level categories in the knowledge base tree.



Active permissions:

User group	Active permissions
Administrators	Content administrator
testing	View only

Access permissions are assigned by a combination of user group and category. A *user group* is a set of one or more **Network Monitor** users that can log into **Network Monitor**. For each category, each user group can be assigned one of five types of permissions:

- `Inherit` - Users inherit the permission from the parent category.
- `No access` - Access is not even visible in the navigation tree. See the one exception further down.
- `View only` - The category is visible and its articles can be viewed. Users cannot modify the category or create new articles.
- `Content Administrator` - Users can modify existing articles of the category, but not create or delete articles.
- `Content Creator` - Users can both modify existing articles and create new articles.

For example, if you set the permission for a category and user group to `View only`, users in that group can only display that category and view any data it generates. Since most categories inherit their user group permissions from their parent node, setting permissions for a category also sets the same permissions for sub-categories set to `Inherit`. If a user is a member of multiple user groups, for any one category it is the group with the lowest ranking permission that sets the effective permission for that user.

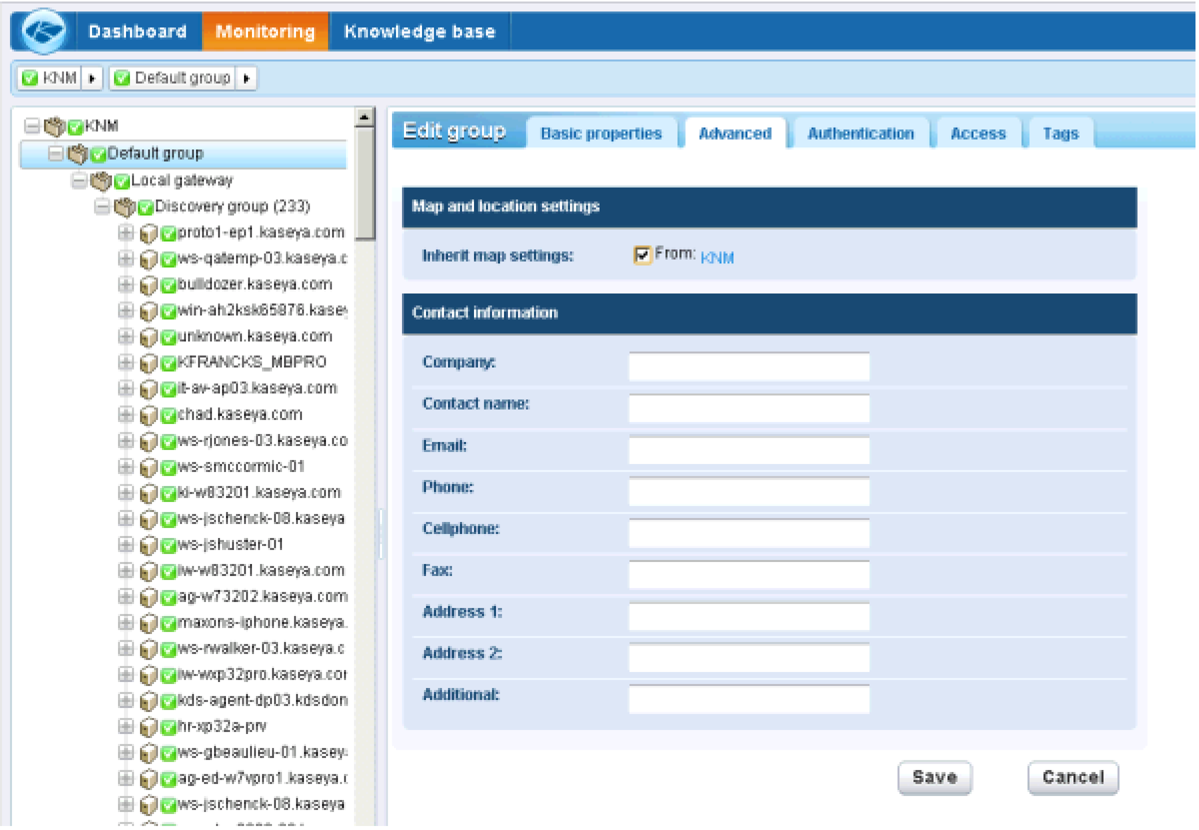
Groups

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

Logical Business Units

Think of groups as representing logical business units. Say you're asked to monitor three gateways for a single business. Create a group with three gateways. Rename the group to reflect the name of the business. Rename the three gateways to reflect their business locations. 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 a device requires on-site intervention, display the devices's closest parent in the navigation tree for the contact information you need.

Groups and sub groups can also be defined *below* gateways. For example, you might have to deliver specialized services to a set of devices within a single subnet. It easiest to distinguish these devices 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.



Map and location settings

Inherit map settings: ☑ From: KNM

Contact information

Company:

Contact name:

Email:

Phone:

Cellphone:

Fax:

Address 1:

Address 2:

Additional:

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 devices of the group using inheritance. This can include subgroups, gateways, devices, and monitors.

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

The Root Node

It might be tempting to think of the root node—called `KNM` by default—as the "server" but it's not. It's just another group. Group properties set for the root note can be *inherited* by lower level nodes, just like any other group. In this case, settings can be potentially inherited *by every other node in the navigation tree.*

In This Section

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 32)* of a group.
- **Add a subgroup** - Creates a **new group** *(page 32)* as a child node.
- **Deploy a new gateway** - Creates a **gateway** *(page 43)* node. *This option only displays if the group has no parent gateways.*
- **Move to other group** - Moves the currently selected group to another group.
- **Delete group** - Deletes the currently selected group.
- **Add a new device** - Adds a **device** *(page 47)* to a group.
- **Add new scheduled event** - Schedules a new **event** *(page 28)*.
- **Create a report** - Creates a **report** *(page 68)*.

Views

Groups and gateways share the same set of views.

- **Devices tab** *(page 26)* - This tab displays with groups and gateways.
- **Monitors tab** *(page 27)* - This tab displays with groups, gateways, and devices.
- **Map tab** *(page 27)* - This tab displays with groups and gateways.
- **Toplist tab** *(page 30)* - This tab displays with groups, gateways, and devices.
- **Schedules tab** *(page 28)* - This tab displays with groups and gateways.
- **Actions tab** *(page 55)* - This tab displays with groups, gateways, devices and monitors.
- **Knowledge tab** *(page 31)* - This tab displays with groups, gateways, and devices.
- **Audit tab** *(page 31)* - This tab displays with groups, gateways, devices and monitors.

Devices tab

This tab displays with groups and gateways.

The **Devices** tab isplays all devices 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 devices are selected.

- **Activate** - Activates selected devices—and all monitors assigned to those devices.
- **Deactivate** - Deactivates selected devices—and all monitors assigned to those devices.
- **Copy** - Copies selected devices—and all monitors assigned to those devices—to another group.
- **Delete** - Deletes selected devices—and all monitors assigned to those devices.

- **Edit** - Edits a selected device. *If multiple devices are selected, edits only those properties shared by those devices.*
- **Move** - Moves selected devices—and all monitors assigned to those devices—to another group.
- **View report** - Generates a **report** *(page 68)* for selected devices.

Table Columns

- **Name** - The name of the device.
- **Address** - The network name or IP address.
- **Group** - The immediate parent node of the device.
- **OS Type** - The system type of the device.

Monitors tab

This tab displays with groups, gateways, and devices.

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.

- **Acknowledge alarm** - **Acknowledges alarms** *(page 68)* on selected monitors.
- **Activate** - Activates selected monitors.
- **Deactivate** - Deactivates selected monitors.
- **Edit** - Edits a selected monitor. *If multiple monitors are selected, edits only those properties shared by those monitors.*
- **Copy** - Copies selected monitors to selected devices.
- **View report** - Generates a **report** *(page 68)* for selected devices.

Table Columns

- **Name** - The name of the monitor. Click the name of a monitor to jump to that node.
- **Device** - The name of the monitor. Click the name of the device to jump to that node.
- **Type** - The type of monitor.
- **Next test** - The next time the test is scheduled to be run.

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 navigation 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 navigation tree.

Smaller Map

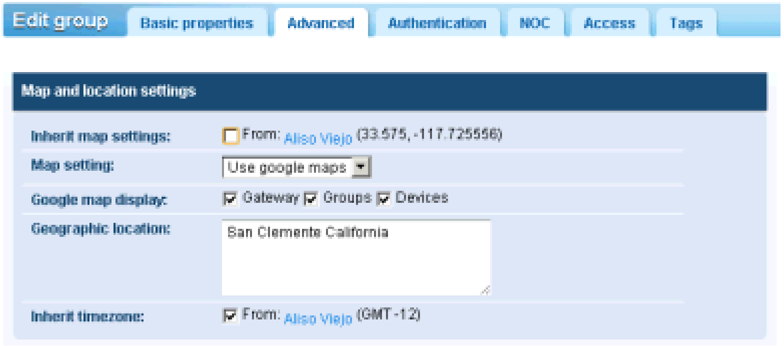
A smaller map, in the lower right hand corner of the page, shows the location of the *currently selected node*.

Inheritance

Groups, gateways and devices 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 devices in the same building.

Configuration

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



Map and location settings

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

Map setting: Use google maps

Google map display: ☑ Gateway ☑ Groups ☑ Devices

Geographic location: San Clemente California

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

Map and location settings

- **Inherit map settings** - If checked, **map settings** *(page 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 devices 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 device's local time.
  - **Inherit time zone** - If checked, inherits time zone settings from the parent node. Uncheck to specify you own time zone settings.

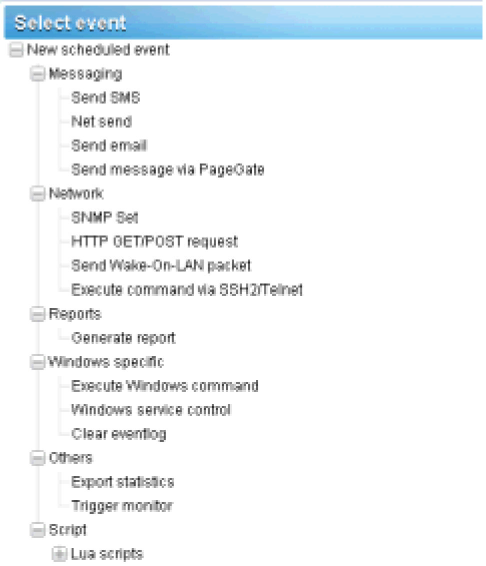
Schedules tab

This tab displays with groups and gateways.

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 one of the parent groups or gateway node of the device you're targeting.* This ensures scheduled events for these devices can be viewed only by users who are authorized to see them.

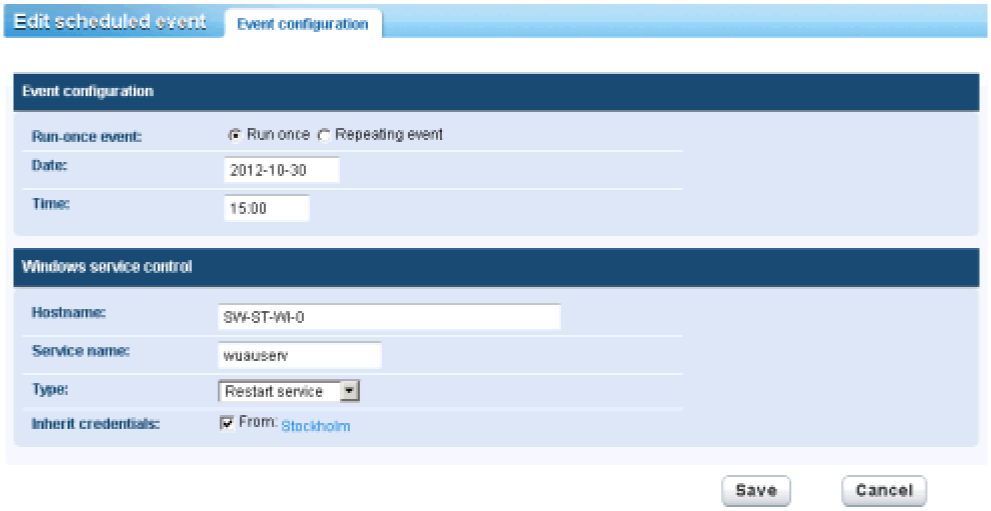
Click the **Schedules** tab for any group or gateway. The tab shows any previously scheduled events. Click the **Add schedule event** command. A list of event actions displays. Click one to edit the event.



Select event

- New scheduled event
  - Messaging
    - Send SMS
    - Net send
    - Send email
    - Send message via PageGate
  - Network
    - SNMP Set
    - HTTP GET/POST request
    - Send Wake-On-LAN packet
    - Execute command via SSH2/Telnet
  - Reports
    - Generate report
  - Windows specific
    - Execute Windows command
    - Windows service control
    - Clear eventlog
  - Others
    - Export statistics
    - Trigger monitor
  - Script
    - Lua scripts

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 device you're targeting is more likely to provide you with the appropriate credential, if one is required.



Edit scheduled event | Event configuration

Event configuration

Run-once event:	● Run once ○ Repeating event
Date:	2012-10-30
Time:	15:00

Windows service control

Hostname:	SW-ST-WI-0
Service name:	wuauserv
Type:	Restart service
Inherit credentials:	☑ From: Stockholm

Scheduling

All events provide the same scheduling options.

Run Once Events

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

Repeating Events

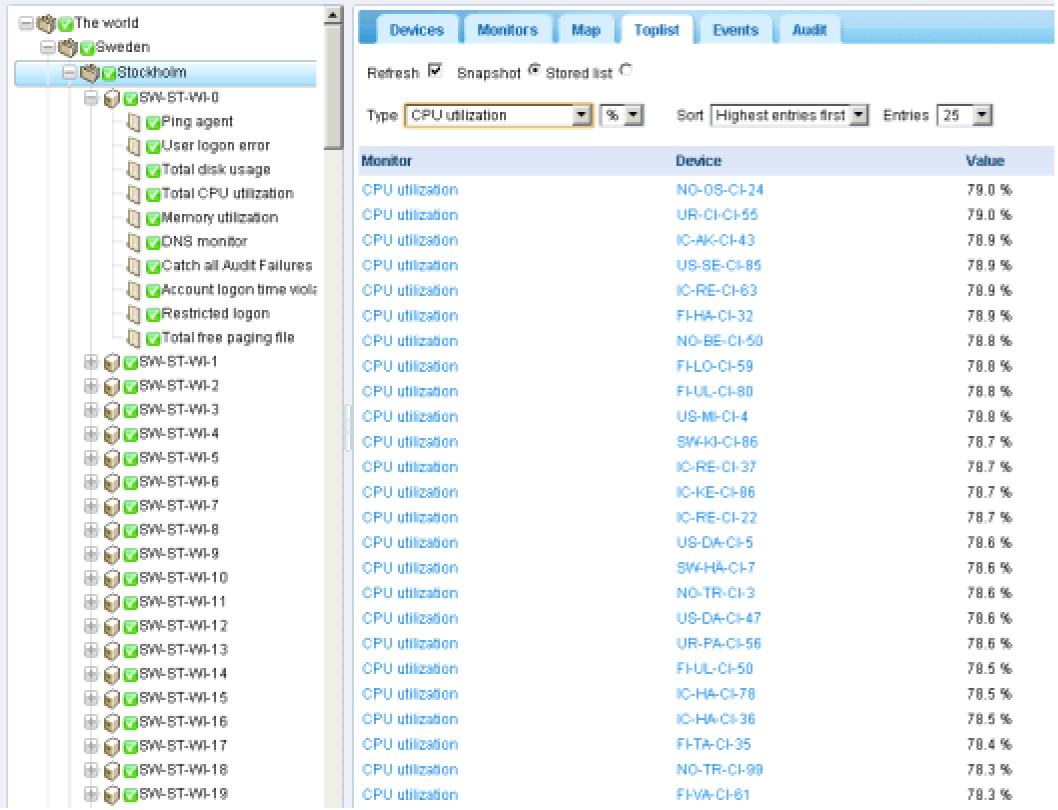
- **Active between** - Specifies the date range the event repeats. Specify the range using a `YYYY-MM-DD` format. If these fields are left empty the event is always repeats.
- **Day of week** - By checking a day, the event repeats only on selected days of the week.

- **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.

Toplist tab

This tab displays with groups, gateways, and devices.

The **Toplist** tab displays the values returned by multiple devices *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 devices are required for a toplist, only groups and gateways displays a **Toplist** tab. Toplists can also be included in reports.



Refresh ☑ Snapshot ● Stored list ○

Type CPU utilization % Sort Highest entries first Entries 25

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

- **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 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.

Knowledge tab

This tab displays with groups, gateways, and devices.

The **Knowledge** tab displays the list of knowledge base articles assigned to that node. Visibility of articles on the **Knowledge** tab is determined by the permissions set on the **Access** *(page 23)* tab of the categories linked to each article.

Actions

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

Related Topics

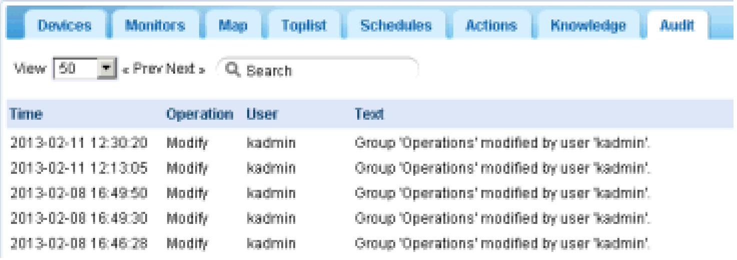
- **Knowledge Base Articles** *(page 22)*
- **Knowledge Base Categories** *(page 23)*

Audit tab

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

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

> **Note:** Searches are case sensitive.



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

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 32)* - Groups, gateways, and devices display a **Basic properties** edit tab.
- **Advanced tab** *(page 32)* - Groups, gateways, devices, and monitors display an **Advanced** edit tab.
- **Authentication tab** *(page 33)* - This edit tab displays with groups, gateways, or devices.
- **NOC tab** *(page 35)* - This edit tab displays with groups, gateways, or devices.
- **Access tab** *(page 36)* - This edit tab displays with groups, gateways, or devices.
- **Tag tab** *(page 37)* - This edit tab displays with groups, gateways, or devices.

Basic properties edit tab - groups

Groups, gateways, and devices 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 groups, gateways and device nodes you can override the default notification *user group* messages are sent to. Monitor nodes use the notification group specified by their parent device node and cannot be overridden.
- **Inherit alarm messages** - Sets the **Alarm Messages** *(page 63)* format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** *(page 55)* of this node.

Advanced edit tab - groups

Groups, gateways, devices, 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 devices 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 device'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

> **Note:** Dependency settings only display for group nodes *below a gateway node* on the navigation tree.

- **Inherit dependency -** This setting determines the currently selected node's **dependency** *(page 51)* on one or more specified monitors. If checked, this node inherits it dependency from the parent node. If blank, you can define a dependency based on a different set of monitors *within the same gateway branch of the navigation 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.

Contact information

Enter contact information for the business unit a group represents. If a device requires on-site intervention, display the devices's closest parent in the navigation tree for the contact information you need.

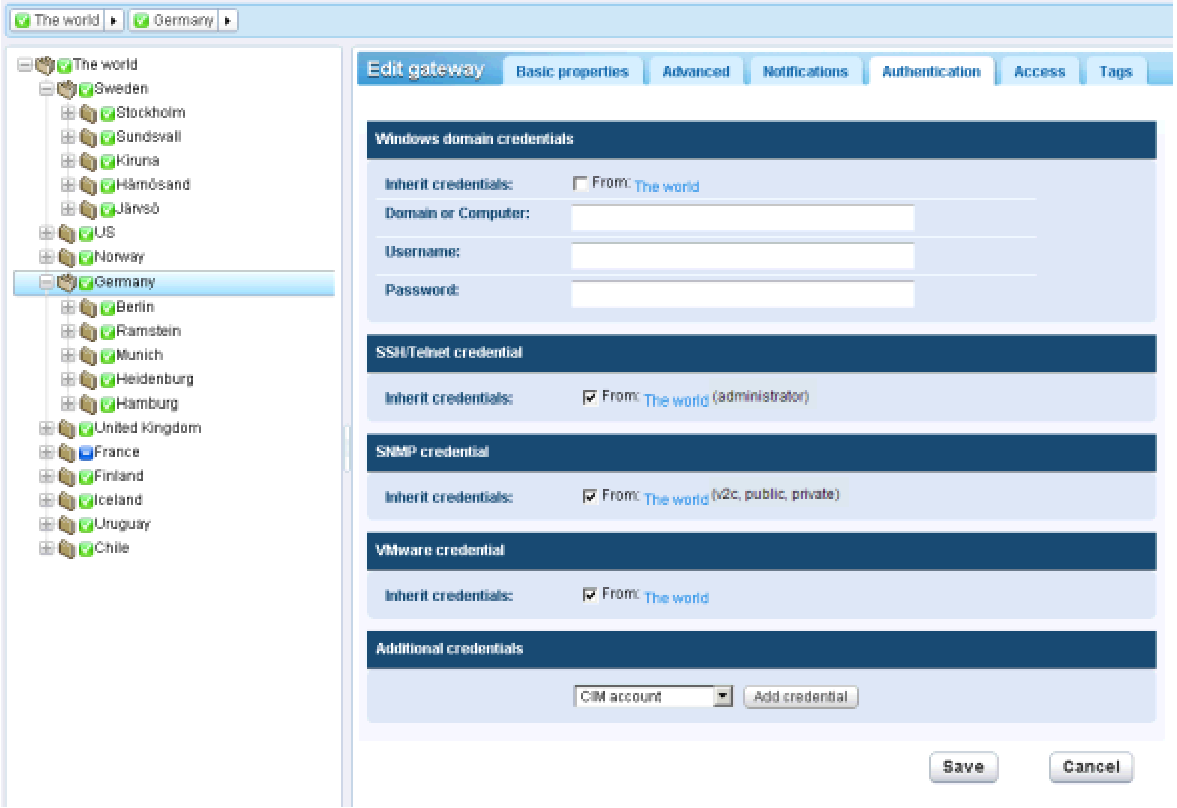
- **Company**
- **Contact name**
- **Email**
- **Phone**
- **Cellphone**
- **Fax**
- **Address 1**
- **Address 2**
- **Additional**

Authentication edit tab

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

The **Authentication** edit tab stores credentials used by **Network Monitor** to authenticate access to network devices.

If you're familiar with earlier versions of **Network Monitor**, you'll recall that credentials were maintained as a single long list. Keeping straight which credentials went with which device and monitor was up to you, no matter how many customers you managed. With **Network Monitor** v5.0, credentials are managed *using inheritance*. That means you can set credentials for a single gateway or group in the navigation tree and all child devices 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.



Windows domain credentials

Inherit credentials: □ From: The world

Domain or Computer:

Username:

Password:

SSH/Telnet credential

Inherit credentials: ☑ From: The world (administrator)

SNMP credential

Inherit credentials: ☑ From: The world (v2c, public, private)

VMware credential

Inherit credentials: ☑ From: The world

Additional credentials

CIM account ▾ Add credential

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 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 device:
  - ➢ **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 device 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 device.
    - ✓ **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
```

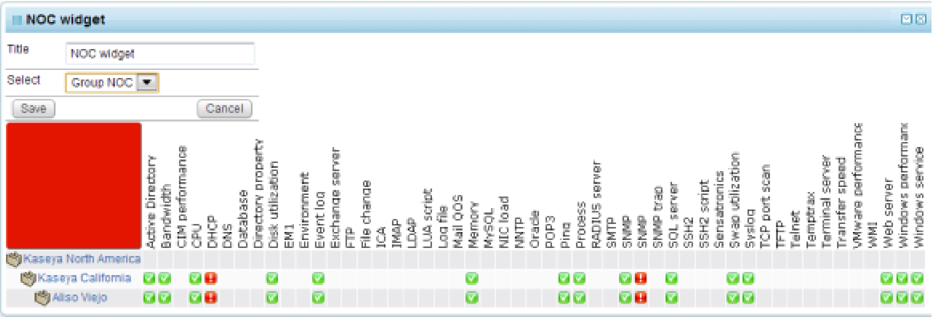
NOC edit tab

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

The **NOC** edit tab assigns a group, gateway or device 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 devices. They are normally displayed on dedicated monitors and are particularly useful in conjunction with the Auto login feature.

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



Title: NOC widget

Select: Group NOC

	Active Directory	Bandwidth	CIM performance	CPU	DHCP	DNS	Database	Directory property	Disk utilization	EM1	Environment	Event log	Exchange server	FTP	File change	ICA	IMAP
Kaseya North America																	
Kaseya California	✓	✓		✓	!				✓			✓					
Aliso Viejo	✓	✓		✓	!				✓			✓					

	LDAP	LUA script	Log file	Mail QOS	Memory	MySQL	NIC load	NNTP	Oracle	POP3	Ping	Process	RADIUS server	SMTP	SNMP	SNMP	SNMP trap
Kaseya North America																	
Kaseya California					✓						✓	✓			✓	!	
Aliso Viejo					✓						✓	✓			✓	!	

	SQL server	SSH2	SSH2 script	Sensatronics	Swap utilization	Syslog	TCP port scan	TFTP	Telnet	Temptrax	Terminal server	Transfer speed	VMware performanc	WMI	Web server	Windows performanc	Windows service
Kaseya North America																	
Kaseya California	✓				✓	✓									✓	✓	✓
Aliso Viejo	✓				✓	✓									✓	✓	✓

Configuring a NOC view and widget

1. The menu > Users & user groups > User list > (to edit) > Dashboard access > **NOC status** checkbox must be checked for each user requiring access.
2. A default **Group NOC** is already defined. To define additional NOC views use the > Monitoring > NOC settings page.
3. A selected group node or gateway node must be assigned to at least one NOC view using the Edit > NOC tab. For example, check the **Group NOC** checkbox checked if that is the only checkbox available.
4. Select Dashboard > Add widget > **NOC widget**.
5. 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.

6. Optionally use the Auto login feature to display a NOC view on a dedicated monitor.

Access edit tab

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

The **Access** tab controls access to different branches of the navigation tree. Click **Edit** for any node down to the device level, then click the **Access** tab to see these settings. As with other aspects of **Network Monitor** this feature can be *inherited* from parent node to child node. This means **Network Monitor** business data security can be intuitively managed using the same navigation tree you use to monitor devices.

> **Note:** A user with the **System admin** checkbox checked has access to all nodes, devices and user interface options, regardless of other access settings.

User Groups and Permissions

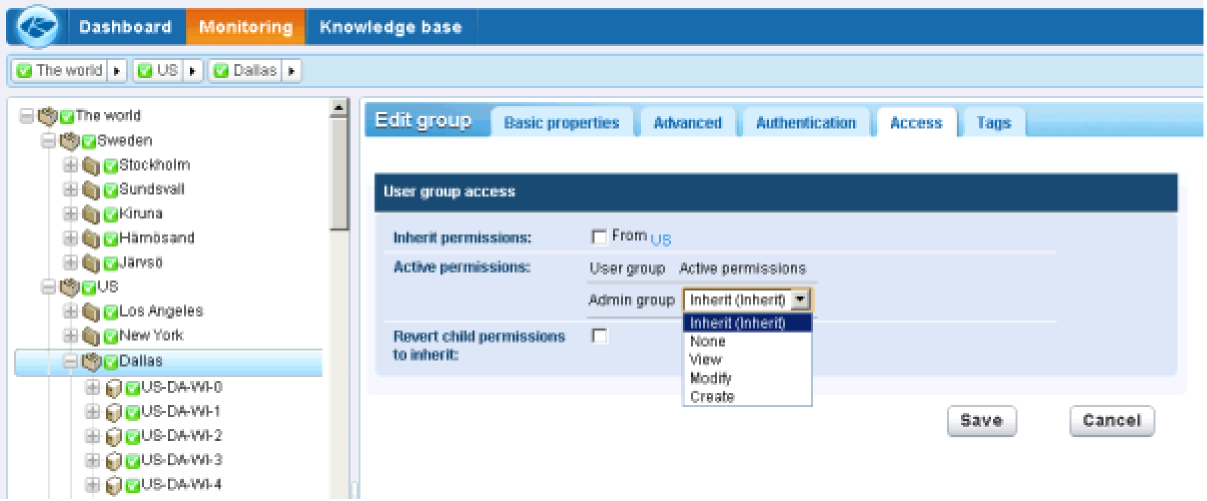
Access permissions are assigned by a combination of user group and node. A *user group* is a set of one or more **Network Monitor** users that can log into **Network Monitor**. For each node, each user group can be assigned one of five types of permissions:

- `Inherit` - Users inherit the permission from the parent node.
- `None` - Access is not even visible in the navigation tree. See the one exception further down.
- `View` - The node is visible and its content can be viewed. Users cannot modify the node or create new content.
- `Modify` - Users can modify existing contents of the node, but not create or delete content.
- `Create` - Users can both modify existing content and create new content.

For example, if you set the permission for a node and user group to `View`, users in that group can only display that node and view any data it generates. Since most nodes inherit their user group permissions from their parent node, setting permissions for a node also sets the same permissions for child devices set to `Inherit`. If a user is a member of multiple user groups, for any one node it is the group with the lowest ranking permission that sets the effective permission for that user.

Revert All Child Permissions

The **Access** tab includes a powerful option call **Revert child permissions to inherit**. This sets *all the descendants* of the current node to inherit. This means you can be confident the permissions you set will be obeyed all the way down the tree from the current node.



Inherit permissions: □ From US

Active permissions: User group Active permissions

Admin group Inherit (Inherit)

Revert child permissions to inherit: □

Creating User Groups

User groups are not created using the navigation tree. Instead click the icon in the upper left hand corner. The menu defines global settings and values, independent of any one node in the navigation tree. Select Create a new user group. Once created you can assign users to each user group. For a new user group permissions are set to `None` for all nodes by default. Adjust the node permissions for a new user group after creation.

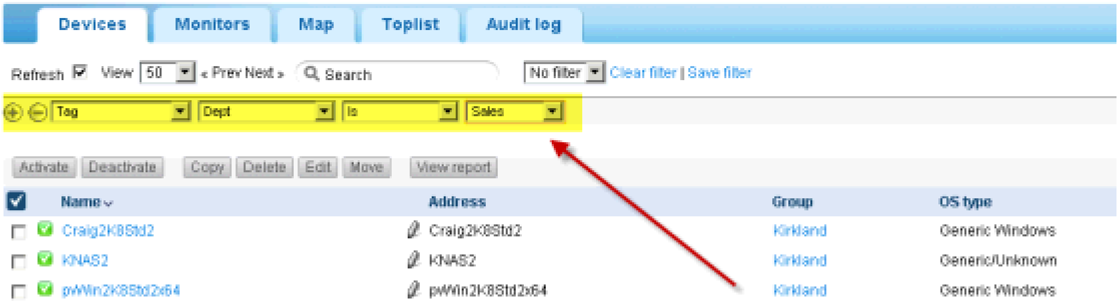
Tags edit tab

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

The **Tags** edit tab creates and edits tags and assigns a node to one or more tags.

A new feature in **Network Monitor** v5.0 is the ability to classify nodes, users and other types of records using one or more user-defined **tags**. The only type of node that cannot be classified using tags are monitors.

For example, you could classify devices 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.

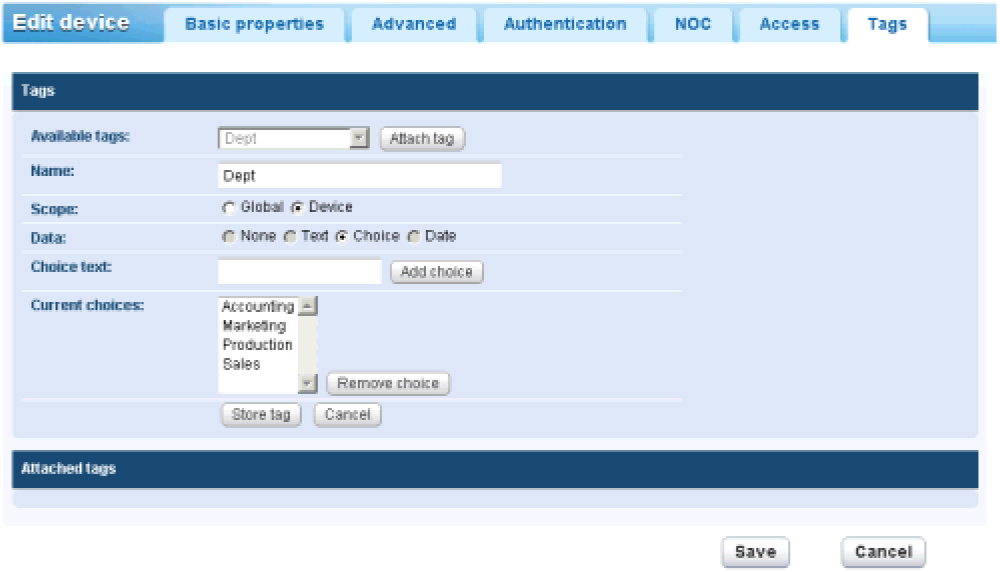


Refresh ☑ View 50 No filter

Tag Dept Is Sales

	Name	Address	Group	OS type
□	Craig2K8Std2	Craig2K8Std2	Kirkland	Generic Windows
□	KNAS2	KNAS2	Kirkland	Generic/Unknown
□	pwWin2K8Std2x64	pwWin2K8Std2x64	Kirkland	Generic Windows

For example, to create and assign tags to a node in the navigation tree, select a group, gateway, or device. Then click **Edit**, then the **Tags** tab.



Tags

Available tags: Dept

Name: Dept

Scope: ○ Global ● Device

Data: ○ None ○ Text ● Choice ○ Date

Choice text:

Current choices: Accounting
Marketing
Production
Sales

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

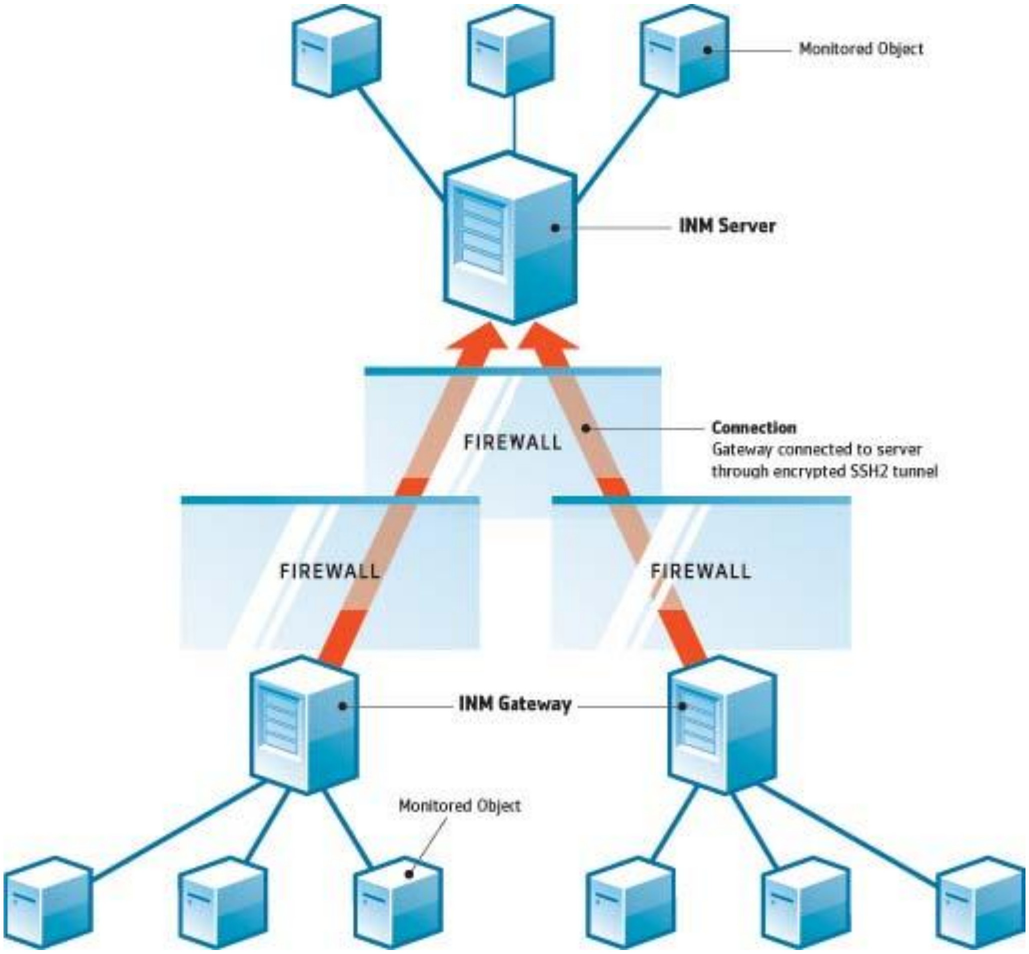
- **Global** - Any type of record can use the tag.
- **Device**, **Group**, or **User** - If a device node has been selected, only other devices can use the tag. If a group or gateway has been selected, only other gateways or groups can use the tag. If a new user has been selected, only other users can 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 a device.

Gateways

Network Monitor supports the monitoring of servers, routers and other types of devices on *multiple networks*. A **gateway** is installed on the server's local network and each remote network managed by **Network Monitor**. Devices 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 devices 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 is a special version of the `KNMsetup.exe` installation that only 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 can be installed on any available machine in the remote network and does not require a dedicated server.

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 navigation tree. Gateway views, commands and properties are similar to **groups** *(page 32)*. Gateway nodes have additional, specialized **properties and commands** *(page 40)* for managing a gateway installed on a network.

In This Section

Gateway Commands and Views

Commands

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

- **Edit** - Edits the **properties** *(page 32)* of a gateway.
- **Add a subgroup** - Creates a **new group** *(page 32)* as a child node.
- **Move to other group** - Moves the currently selected gateway to another group.
- **Delete gateway** - Deletes the currently selected gateway.
- **Add a new device** - Adds a **device** *(page 47)* to the gateway.
- **Add new scheduled event** - Schedules a new **event** *(page 28)*.
- **Create a report** - Creates a **report** *(page 68)*.
- **Download configuration** - Downloads the configuration file, `gateway.nxd`, required for an installed gateway to connect to the server.
- **Push configuration** - Updates the gateway with gateway configuration changes. For example, use this command after adding an IP number to the server address list.

Views

Groups and gateways share the same set of views.

- **Devices tab** *(page 26)* - This tab displays with groups and gateways.

- **Monitors tab** *(page 27)* - This tab displays with groups, gateways, and devices.
- **Map tab** *(page 27)* - This tab displays with groups and gateways.
- **Toplist tab** *(page 30)* - This tab displays with groups, gateways, and devices.
- **Schedules tab** *(page 28)* - This tab displays with groups and gateways.
- **Actions tab** *(page 55)* - This tab displays with groups, gateways, devices and monitors.
- **Knowledge tab** *(page 31)* - This tab displays with groups, gateways, and devices.
- **Audit tab** *(page 31)* - This tab displays with groups, gateways, devices and monitors.

Adding a Gateway

Adding a gateway involves the following main steps.

1. Add and configure a gateway node on the navigation tree.
2. Export the gateway node's configuration to a data file.
3. Use `knmsetup.exe` to install a new gateway on the system hosting the gateway.
4. Copy the configuration file to a directory on the system hosting the installed gateway.
5. Restart the gateway service on the host of the gateway system.

Procedure

1. Select a group that will serve as the parent group of the new **gateway** *(page 39)*.

   > **Note:** The group must be *above or equal in rank* to other gateways that already exist on the tree. You cannot create a gateway *below* another gateway on the same branch.

2. Click the **Deploy a new Gateway** command.
   - The **Edit gateway > Basic properties** tab displays.
3. Enter the **Name** and **Description** of the new gateway.
4. Enter **Address** and **Port** settings for the gateway.
   - If, for evaluation purposes, a **Network Monitor** server and gateway are installed on the same subnet, the **Address** and **Port** fields on this page should match the **Server IP** and **Port** fields on the Gateway server settings page.
   - If the server is installed behind a NAT firewall, specify the *external* IP and port of the NAT firewall. The NAT firewall should then be configured to redirect to the *internal* IP and port specified by the **Server IP** and **Port** fields of the **Gateway server settings** page.
5. Select the new gateway in the tree.
   - A ⊟ icon displays next to the new gateway indicating the gateway is disconnected from the server.
6. Click the **Download configuration** command. Clicking this command creates two files in the `<KaseyaInstallDirectory>/knm/gateways/<GatewayName>` directory of the *server* host machine.
   - `gateway.nxd`
   - `readme.txt`
7. Install **Network Monitor** on the *gateway* host machine using the same `knmsetup.exe` used to install the server.
8. During the install, click the **Options** button and ensure the **Gateway** option is selected.
9. Complete the install. No user interface displays after a gateway is installed.
10. Stop the `Kaseya Network Monitor` service on the gateway host machine.

11. Copy the `gateway.nxd` file from the *server* host machine into the `<KaseyaInstallDirectory>/knm` directory of the *gateway* host machine.
12. Start the `Kaseya Network Monitor` service on the gateway host machine.
13. Check the status of the new gateway in the **Network Monitor** user interface.
    - The new gateway should now display a ✓ icon, indicating it is connected to the server.
    - If the new gateway fails to connect, see **Troubleshooting gateway connections** *(page 42)*.

> **Note:** To *monitor* the gateway add a device node below the gateway node that specifies an address of `localhost` or `127.0.0.1`.

Troubleshooting gateway connections

Troubleshooting gateway connection problems

- Review the gateway configuration. Ensure the correct IP and port number has been entered.
- Ensure all the gateway configuration files in the `KNM\Gateway` directory have been copied to the KNM folder of the host gateway machine.
- If you have reinstalled the server on a new machine, the gateway configuration must be updated to update the public key file. After the gateway configuration is saved, move the gateway configuration files to the `\Gateway` root directory and restart the gateway.
- If you changed the gateway configuration (IP number and port number) move the updated configuration files to the gateway and restart the gateway.
- The server shuts down any gateway that does not match the server version number. Gateways can be updated directly from the **Network Monitor** management interface by choosing the **Update gateway** command on a selected gateway.
- The gateway name is part of the server login session, if you change the gateway name you have to move the gateway configuration files to the gateway for it to be able to reconnect.

Logging debug information

To enable debug logging on the gateway, open the `init.cfg` file on the gateway and enter the following line: `LOG_LEVEL=2`. A debug file called `debuglog.txt` is written to the `\logs` directory.

Running the gateway in debug mode

- **Local gateway** - To run the local gateway in debug mode you first need to stop the Kaseya Local Gateway (`nmservicelg.exe`) service on the system hosting the local gateway. When the service has been stopped start cmd.exe and navigate to the `<KaseyaInstallDirectory>\knm\local_gateway` directory. Start the gateway by entering the following line:

  ```
  nmservicelg.exe -d
  ```
- **Remote gateway** - To run a remote gateway in debug mode you first need to stop the Kaseya Network Monitor (`nmservice.exe`) service on the system hosting the remote gateway. When the service has been stopped start `cmd.exe` and navigate to the `<KNMInstall>` directory. Start the gateway by entering the following line:

  ```
  nmservice.exe -d
  ```

Editing Gateways

Network Monitor > (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 32)*. Gateway nodes have additional, specialized properties and **commands** *(page 40)* for managing a gateway installed on a network.

- **Basic properties tab** *(page 43)* - Groups, gateways, and devices display a **Basic properties** edit tab.
- **Advanced tab** *(page 43)* - Groups, gateways, devices, and monitors display an **Advanced** edit tab.
- **Authentication tab** *(page 33)* - This edit tab displays with groups, gateways, or devices.
- **NOC tab** *(page 35)* - This edit tab displays with groups, gateways, or devices.
- **Access tab** *(page 36)* - This edit tab displays with groups, gateways, or devices.
- **Tag tab** *(page 37)* - This edit tab displays with groups, gateways, or devices.

Basic properties edit tab - gateways

Groups, gateways, and devices 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 groups, gateways and device nodes you can override the default notification *user group* messages are sent to. Monitor nodes use the notification group specified by their parent device node and cannot be overridden.
- **Inherit alarm messages** - Sets the **Alarm Messages** *(page 63)* format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** *(page 55)* of this node.

Advanced edit tab - gateways

Groups, gateways, devices, 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 devices 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 device'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

- **Inherit dependency -** This setting determines the currently selected node's **dependency** *(page 51)* on one or more specified monitors. If checked, this node inherits it dependency from the parent node. If blank, you can define a dependency based on a different set of monitors *within the same* *gateway branch of the navigation 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.

Network discovery

Network discovery can only be run manually from the Advanced tab of a gateway node. See **Network Discovery** *(page 45)*.

1. Click the **Enable** checkbox for the **Network Discovery** section of this tab.
2. Specify up to three subnets. A tooltip displays accepted formats:
   - Using CIDR notation - `192.168.1.0/24`
   - By Range - `192.168.1.0-255`
   - Single IP Address - `192.168.42.0`
3. Click the **Start now** checkbox.
4. You must **move discovered devices out of the Discovery group** *(page 18)* to start generating alert notifications.

Receive Syslog messages

- **Syslog server** - If checked, enables Syslog messages intercepted on the gateway's network to be forwarded to the server. Ensure the **> Other > Other system settings > Syslog checkbox** is also checked. The Syslog monitor requires these two checkboxes be enabled. Once checked, intercepted syslog messages display on the **> Tools >** List syslog messages 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 syslog messages display on the **> Tools >** List syslog 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

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

Network Discovery

Network discovery is run manually from the **Advanced** *(page 43)* edit tab of a gateway node.

Immediately after a new install, you'll notice a `Discovery group` created for the `Local gateway`. The `Discovery group` contains all the devices discovered on your own local network.

- If you **create a** ***new*** **gateway** *(page 41)*, a similar discovery group is created just below that gateway.
- After the initial run, network discovery runs daily at 2:00 AM, gateway time, by default.

One Gateway Per Local Area Network

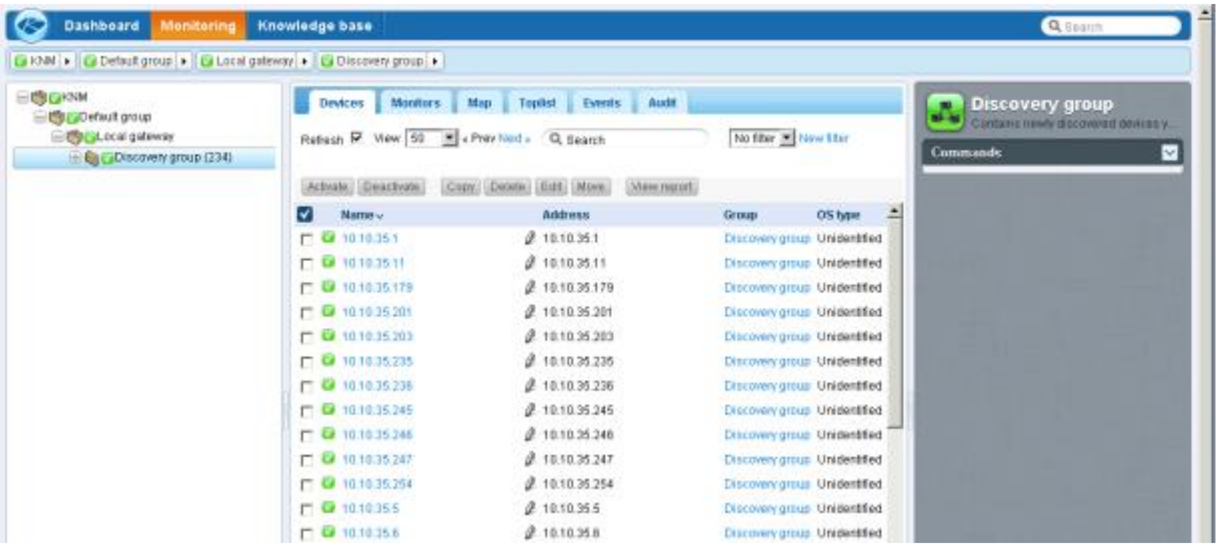
> **The gateway performing the discovery needs to be physically or logically (VLAN) connected to the network that you specify.** Having router access only is not enough. Network discovery uses ARP requests to look up the MAC address of IP addresses, and ARP requests never travel beyond the same local area network (router). There is no way for the the gateway to see the MAC address of devices beyond the local area network. So to get the best possible coverage from network discovery at least one gateway must be placed in each local area network.

Monitoring and Alerts

You can assign monitors to devices in the `Discovery group` and even see the data reported back by the monitor. **But you cannot generate an alert for a device while it is inside the Discovery group.**

Licensing

No monitoring licenses are consumed by a device inside the `Discovery group`. When you move a discovered device out of the `Discovery group`, a license is consumed.



☑	Name	Address	Group	OS type
□	10.10.35.1	10.10.35.1	Discovery group	Unidentified
□	10.10.35.11	10.10.35.11	Discovery group	Unidentified
□	10.10.35.179	10.10.35.179	Discovery group	Unidentified
□	10.10.35.201	10.10.35.201	Discovery group	Unidentified
□	10.10.35.203	10.10.35.203	Discovery group	Unidentified
□	10.10.35.235	10.10.35.235	Discovery group	Unidentified
□	10.10.35.236	10.10.35.236	Discovery group	Unidentified
□	10.10.35.245	10.10.35.245	Discovery group	Unidentified
□	10.10.35.246	10.10.35.246	Discovery group	Unidentified
□	10.10.35.247	10.10.35.247	Discovery group	Unidentified
□	10.10.35.254	10.10.35.254	Discovery group	Unidentified
□	10.10.35.5	10.10.35.5	Discovery group	Unidentified
□	10.10.35.6	10.10.35.6	Discovery group	Unidentified

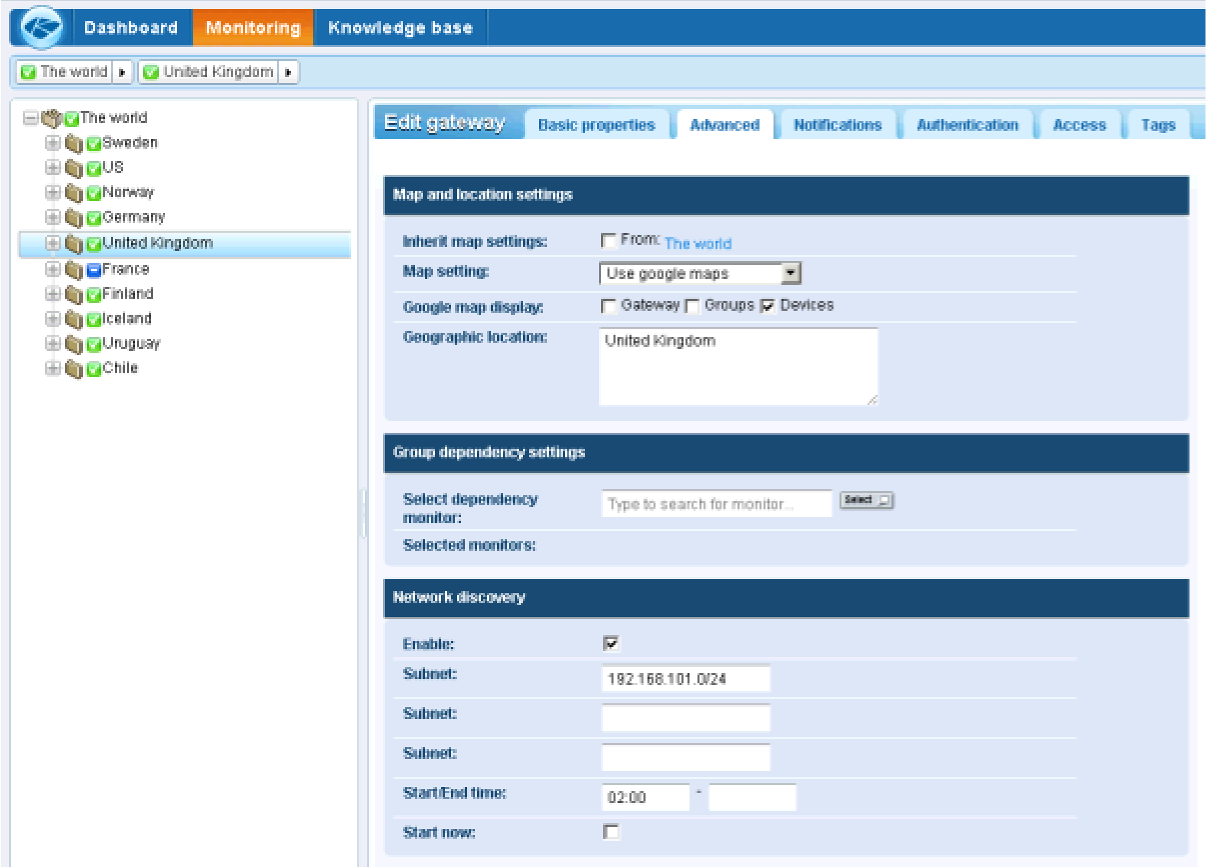
Running Network Discovery Manually

Network discovery can only be run *manually* from the **Advanced tab** *(page 43)* of a *gateway node*.

1. Select a gateway node in the navigation tree.
2. Click **Edit** in the right hand pane.
3. Click the **Advanced** tab.
4. Click the **Enable** checkbox for the **Network Discovery** section of this tab.
5. Specify up to three subnets. A tooltip displays accepted formats:

- Using CIDR notation - `192.168.1.0/24`
- By Range - `192.168.1.0-255`
- Single IP Address - `192.168.42.0`

6. Click the **Start now** checkbox.
7. You must **move discovered devices out of the Discovery group** *(page 18)* to start generating alert notifications.



Map and location settings

Inherit map settings: □ From: The world

Map setting: Use google maps

Google map display: □ Gateway □ Groups ☑ Devices

Geographic location: United Kingdom

Group dependency settings

Select dependency monitor: Type to search for monitor...

Selected monitors:

Network discovery

Enable: ☑

Subnet: 192.168.101.0/24

Subnet:

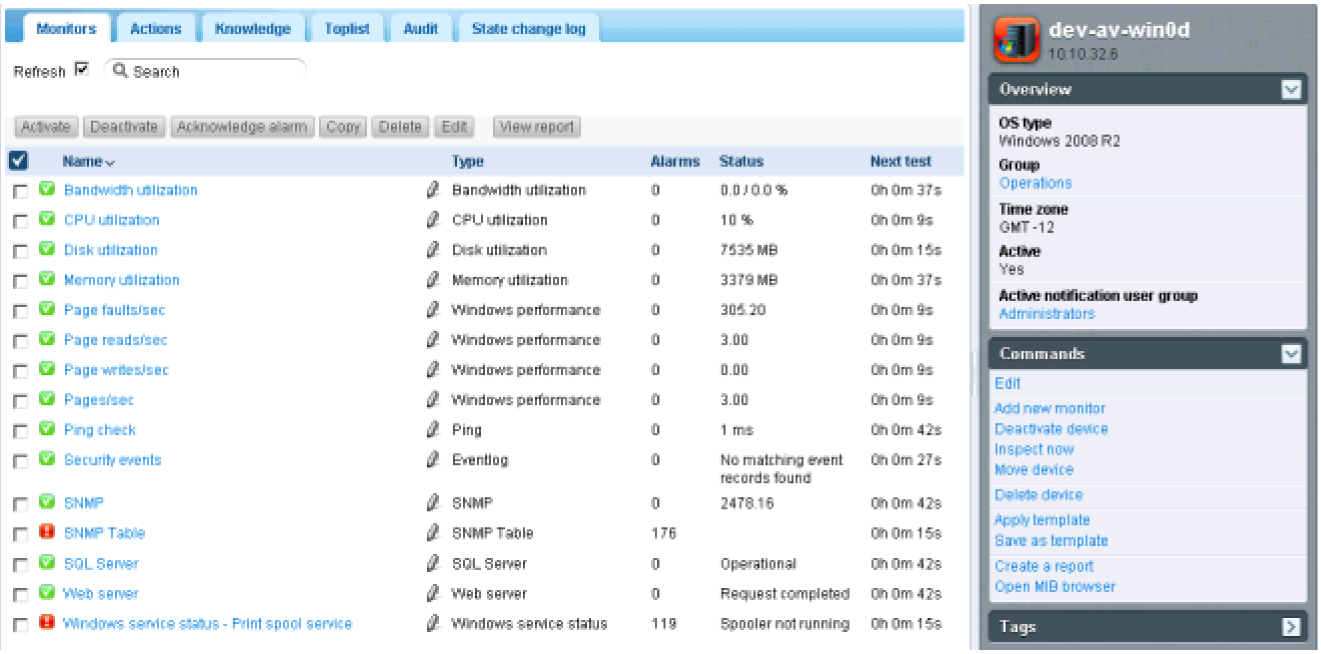
Subnet:

Start/End time: 02:00 -

Start now: □

Devices

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



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

dev-av-win0d
10.10.32.6

Overview

OS type
Windows 2008 R2

Group
Operations

Time zone
GMT -12

Active
Yes

Active notification user group
Administrators

Device Commands and Views

Commands

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

- **Edit** - Edits the **properties** *(page 49)* of the device.
- **Add new monitor** - Adds a new **monitor** *(page 59)* to the device.
- **Deactivate device** - Deactivates the device.
- **Inspect now** - Inspects a device to determine the appropriate pre-configured monitors for the device. This is the same inspection performed on devices during **Network Discovery** *(page 45)*. You may want to run **Inspect Now** if the credentials or configuration of the device have changed. After running **Inspect Now**, click **Add New Monitor** to see the list of pre-configured monitors.
- **Move device** - Moves the device to a different group or gateway.
- **Delete device** - Deletes the device.
- **Apply template** - Applies a **device template** *(page 52)*.
- **Save as template** - Saves the set of monitors as a **device template** *(page 52)*.
- **Create a report** - Views, emails or publishes a **report** *(page 69)*.

Devices

- **Open MIB browser** - Displays the list of OIDs supported by a device that can be monitored using SNMP. A device must be SNMP enabled to display OIDs.

Views

- **Monitor tab** *(page 48)* - This tab displays with groups, gateways, and devices.
- **Actions tab** *(page 55)* - This tab displays with groups, gateways, devices and monitors.
- **Knowledge tab** *(page 31)* - This tab displays with groups, gateways, and devices.
- **Toplist tab** *(page 30)* - This tab displays with groups, gateways, and devices.
- **Audit tab** *(page 31)* - This tab displays with groups, gateways, devices and monitors.
- **State change log tab** *(page 48)* - This tab displays with devices and monitors.

Monitor tab

This tab displays with groups, gateways, and devices.

Actions

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

- **Activate** - Activates selected monitors.
- **Deactivate** - Deactivates selected monitors.
- **Acknowledge alarm** - **Acknowledges alarms** *(page 68)* on selected monitors.
- **Copy** - Creates selected monitors to selected devices.
- **Delete** - Deletes selected monitors.
- **Edit** - Edits a selected monitor. If multiple monitors are selected, edits shared **standard monitor properties** *(page 62)* of these monitors.
- **View report** - Generates a report for selected devices.

Table Columns

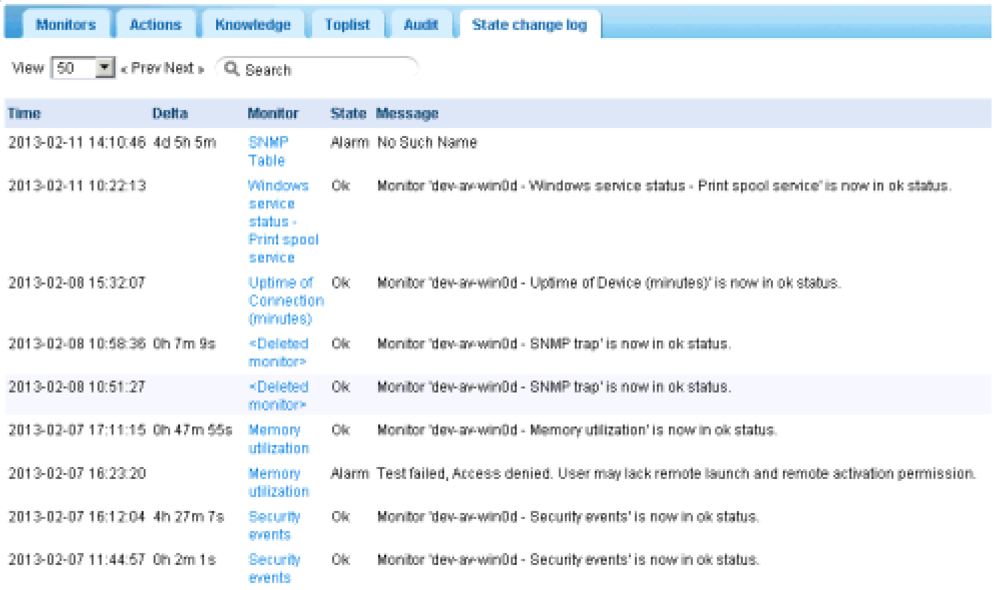
- **Name** - The name of the monitor.
- **Type** - The type of monitor.
- **Alarms** - The **alarm count** *(page 53)*. - This column is only displayed on device nodes.
- **Status** - The latest result returned from the monitor. This column is only displayed on device nodes.
- **Next test** - The next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

State change log tab

This tab displays with devices and monitors.

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

Note: *Searches are case sensitive.*



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

Adding / Editing Devices

<selected group or gateway> > Add a new device > Empty device

<selected device> > Edit

The **New device** page and **Edit device** page display almost the same properties. The **New device** page gives you an additional option of deploying monitors automatically, based on a initial inspection of the device.

- **Basic properties tab** *(page 49)* - Groups, gateways, and devices display a **Basic properties** edit tab.
- **Advanced tab** *(page 50)* - Groups, gateways, devices, and monitors display an **Advanced** edit tab.
- **Authentication tab** *(page 33)* - This edit tab displays with groups, gateways, or devices.
- **NOC tab** *(page 35)* - This edit tab displays with groups, gateways, or devices.
- **Access tab** *(page 36)* - This edit tab displays with groups, gateways, or devices.
- **Tag tab** *(page 37)* - This edit tab displays with groups, gateways, or devices.

Basic properties edit tab - devices

Groups, gateways, and devices display a Basic properties edit tab.

Basic properties

- **Name** - Enter a name for the device. This should be a descriptive name used to identify the device in lists and notifications sent to users.
- **Address** - Enter the network address of the device. This can be a host name or an IPv4 number.
- **Operating system** - Select the device's system type. The operating system determines the type of monitors that can be added to this device. If you do not know what system type the device 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.
- **Device type** - Classifies the type of hardware device. For reference purposes only.

- **Description** - The description field can be used to describe the device 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 device and can also be included in alarm notifications.

Initial monitor deployment

This option only displays on the **New device** *page.*

- **Monitor deployment**
  - `None, add empty device` - Adds the device without adding any monitors.
  - `Automatic, add monitors after inspection` - Adds an appropriate set of monitors for this device after an initial inspection of the device.

Alert and recovery settings

- **Inherit notification group** - Sets the notification group for this node. For groups, gateways and device nodes you can override the default notification *user group* messages are sent to. Monitor nodes use the notification group specified by their parent device node and cannot be overridden.
- **Inherit alarm messages** - Sets the **Alarm Messages** *(page 63)* format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** *(page 55)* of this node.

Advanced edit tab - devices

Groups, gateways, devices, and monitor display an Advanced edit tab.

Advanced

- **Active** - If checked the device is considered active. Active devices test their monitors. This option is checked by default.
- **SSH2 connect. sharing** - If checked, enables persistent SSH2 connections for this device. Normally only one connection is opened and then shared among all monitors using SSH2 with this device. 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 device. Normally **Network Monitor** performs a device inventory of all devices regularly, to discover hardware and attached devices.
- **Use WMI** - If a device is a Windows system type, the following monitor types use WMI when the device 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 devices 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 device's local time.
- **Inherit time zone** - If checked, inherits time zone settings from the parent node. Uncheck to specify you own time zone settings.

Device dependency settings

- **Inherit dependency -** This setting determines the currently selected node's **dependency** *(page 51)* on one or more specified monitors. If checked, this node inherits it dependency from the parent node. If blank, you can define a dependency based on a different set of monitors *within the same gateway branch of the navigation 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* device.

> **Note:** Use > Schedules > Device maintenance to specify maintenance schedules for *multiple* devices.

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

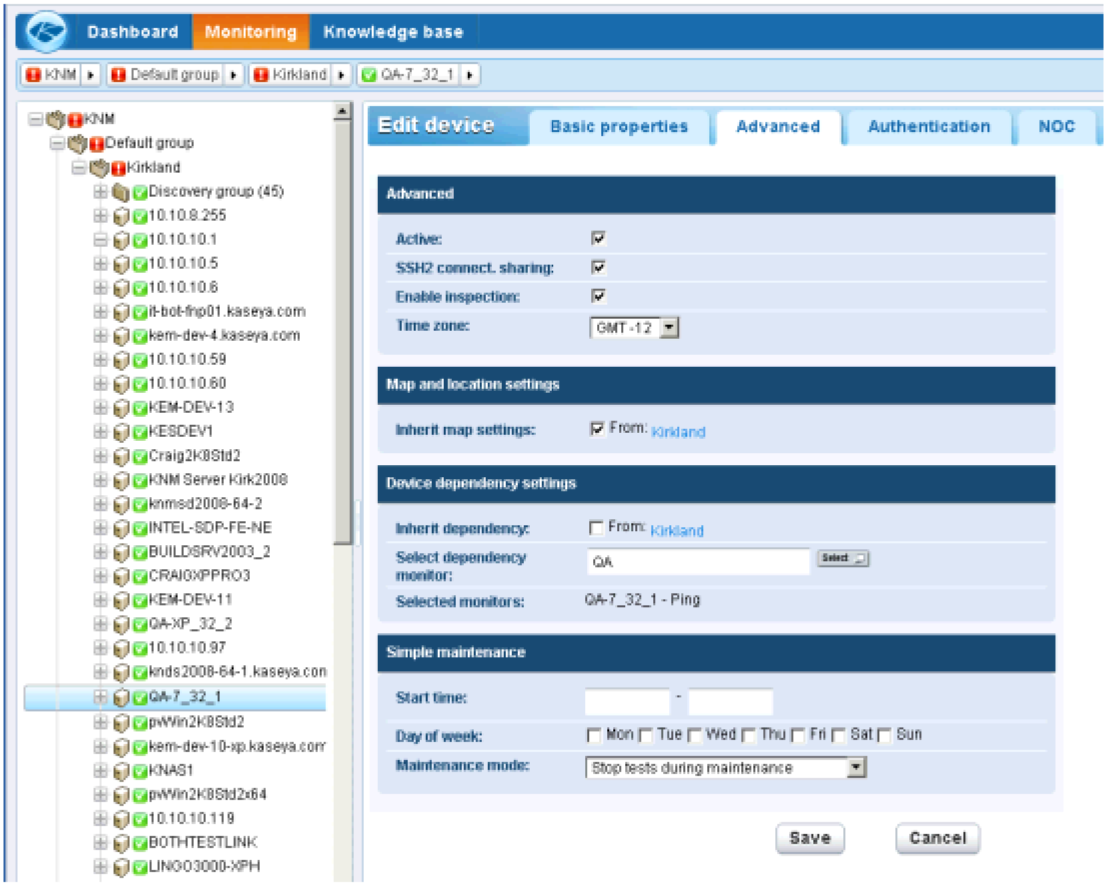
Dependency Testing

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

If you're familiar with earlier versions of **Network Monitor** you might recall that the alert status of one monitor could be made dependent on the alert status of another monitor *assigned to the same device.* With **Network Monitor** v5.0 this dependency feature has been expanded to include *any part of the local gateway branch*.

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 devices on that same network depend on that same router. When the router fails to connect, those dependent devices can't help but fail to connect as well. An entire branch of the navigation tree reports monitoring failures even though the problem is really a single device. Those dependent devices 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.

Click **Edit** for any node, then click the **Advanced** tab. Use **Device 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.



Advanced

Active: ☑

SSH2 connect. sharing: ☑

Enable inspection: ☑

Time zone: GMT -12

Map and location settings

Inherit map settings: ☑ From: Kirkland

Device dependency settings

Inherit dependency: □ From: Kirkland

Select dependency monitor: QA

Selected monitors: QA-7_32_1 - Ping

Simple maintenance

Start time: -

Day of week: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Maintenance mode: Stop tests during maintenance

Device Templates

Device templates are configured using > Monitoring > Device templates

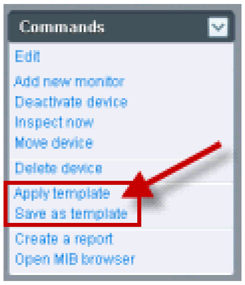
Configuring one monitor at a time for thousands of devices isn't practical. Instead configure a *set of monitors* using a device template, then assign the device template to the appropriate device. You should have a device template for each type of device you manage.

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

Note: There is an ever-growing set of built-in "system" device templates available. This includes several OS-specific devices templates that are applied when you run **Network Discovery** *(page 45)* or **inspect** *(page 47)* a device.

Applying Device Templates to Devices

Once you have configured a device template, you only have to select a device and click the **Apply template** option. Then select the device template. All the monitors in the device template will be assigned to the selected device and begin returning data.



Monitors

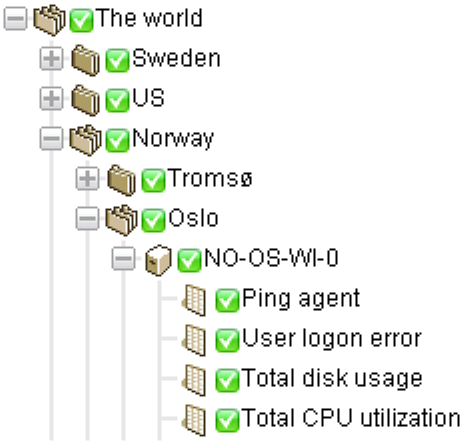
A **monitor** tests a specific function in a device. Most monitors are capable of collecting various statistical data for reporting purposes. When a monitor test fails consecutively a specified number of times, the monitor enters an *Alarm* state and executes a set of actions.

The alert status of each monitor—along with all other active monitors—is reported all the way up the navigation 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

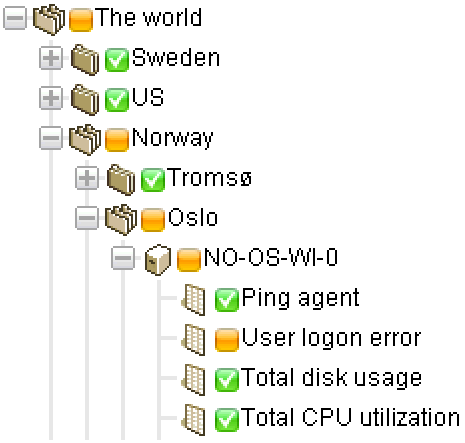
OK Status

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



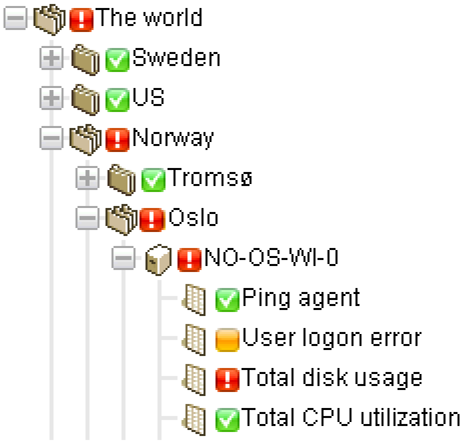
Failed Status

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



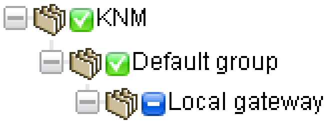
Alarm Status

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 navigation 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 navigation 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. Check the Server gateway settings page on the menu to ensure the gateway and server can communicate.



In This Section

Monitor Commands and Views

Commands

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

- **Edit** - Edits the **properties** *(page 49)* of the device.
- **Deactivate** - Deactivates the monitor.
- **Copy** - Copies the monitor to selected devices.
- **Inspect now** - Tests all monitors assigned to the device immediately.
- **Delete** - Deletes the monitor.
- **Create a report** - Views, emails or publishes a **report** *(page 69)*.
- **Test now** - Tests the monitor immediately.

Views

- **Summary tab** *(page 48)* - This tab displays with monitors.
- **Actions tab** *(page 55)* - This tab displays with groups, gateways, devices and monitors.
- **Audit tab** *(page 31)* - This tab displays with groups, gateways, devices and monitors.
- **State change log tab** *(page 48)* - This tab displays with devices and monitors.
- **Simulate alarm tab** *(page 59)* - This tab displays with monitors.

Summary tab

This tab displays with monitors.

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

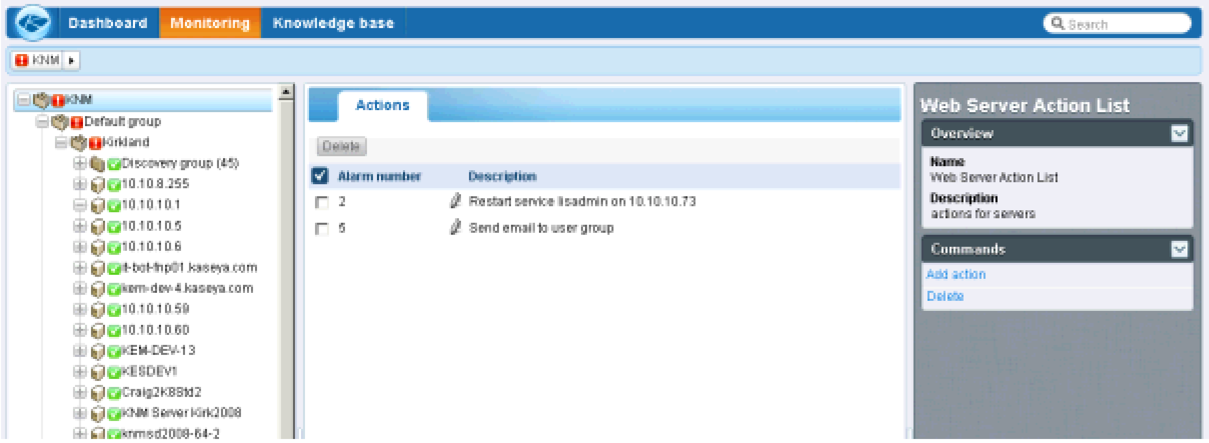
- **Monitor status** - Displays the latest value and the threshold to trigger a *Failed* state.
- **Live data** - A chart of the latest test values returned by the monitor. The time period the chart is set when you configure the monitor.
- **Monitor Log** - A log of every test value returned by the monitor.

Actions tab

This tab displays with groups, gateways, devices 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.



☑	Alarm number	Description
□	2	Restart service iisadmin on 10.10.10.73
□	5	Send email to user group

Name
Web Server Action List
Description
actions for servers

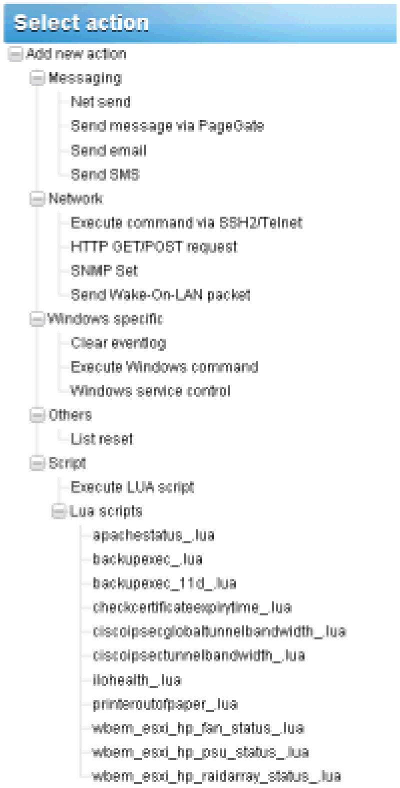
Recovery Actions

An administrator may have to intervene to correct a device in an *Alarm* state, or the device 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.

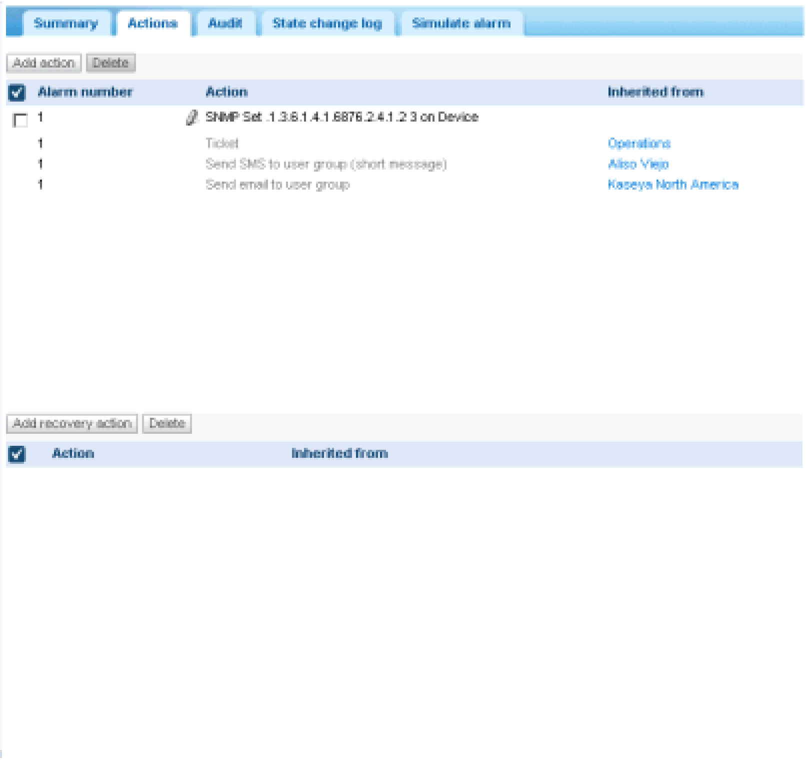


Select action

- Add new action
  - Messaging
    - Net send
    - Send message via PageGate
    - Send email
    - Send SMS
  - Network
    - Execute command via SSH2/Telnet
    - HTTP GET/POST request
    - SNMP Set
    - Send Wake-On-LAN packet
  - Windows specific
    - Clear eventlog
    - Execute Windows command
    - Windows service control
  - Others
    - List reset
  - Script
    - Execute LUA script
    - Lua scripts
      - apachestatus_.lua
      - backupexec_.lua
      - backupexec_11d_.lua
      - checkcertificateexpirytime_.lua
      - ciscoipsecglobaltunnelbandwidth_.lua
      - ciscoipsectunnelbandwidth_.lua
      - ilohealth_.lua
      - printeroutofpaper_.lua
      - wbem_esxi_hp_fan_status_.lua
      - wbem_esxi_hp_psu_status_.lua
      - wbem_esxi_hp_raidarray_status_.lua

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.

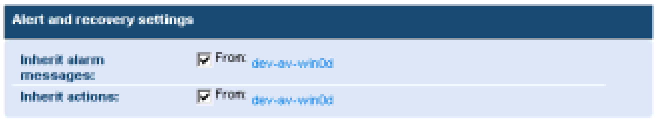


☑ Alarm number	Action	Inherited from
□ 1	SNMP Set .1.3.6.1.4.1.6876.2.4.1.2.3 on Device	
1	Ticket	Operations
1	Send SMS to user group (short message)	Aliso Viejo
1	Send email to user group	Kaseya North America

☑ Action	Inherited from

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.


Alert and recovery settings

Inherit alarm messages: ☑ From: dev-av-win0d

Inherit actions: ☑ From: dev-av-win0d

Managing Customer-Specific Actions and Recovery Actions

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

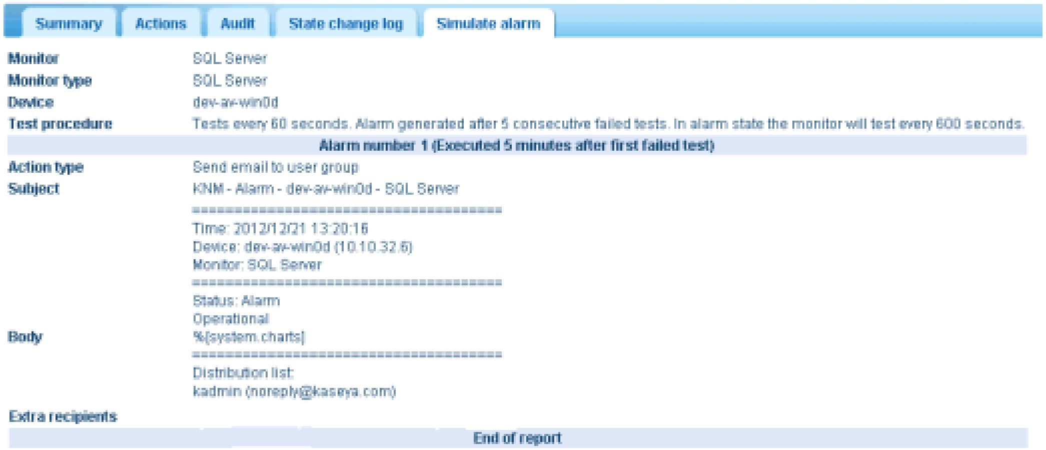
All other actions are executed on the gateway.

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.



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

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

Adding / Editing Monitors

<selected device > > Add a new monitor > <select monitor>

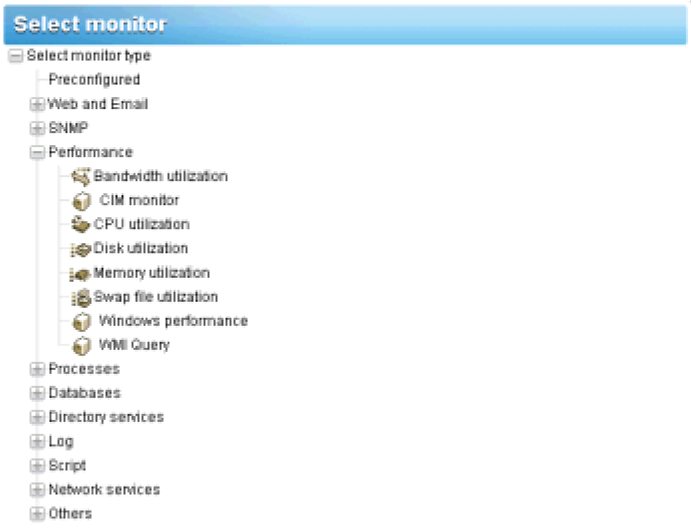
<selected monitor> > Edit

The **Edit monitor** tab sets the monitoring attributes for monitors assigned to devices.

- **Basic tab** *(page 62)* - This edit tab displays with monitors.
- **Advanced tab** *(page 62)* - Groups, gateways, devices, and monitors display an **Advanced** edit tab.
- **Alarm filtering tab** *(page 63)* - This edit tab displays with monitors.
- **Statistics tab** *(page 63)* - This edit tab displays with monitors.

Adding a Monitor - An Example

To begin monitoring, select any device node in the navigation tree, then select the **Add new monitor** command. The following list of monitor types—more than 40 and growing—displays. See Monitor Reference to identify which operating systems support which monitors.

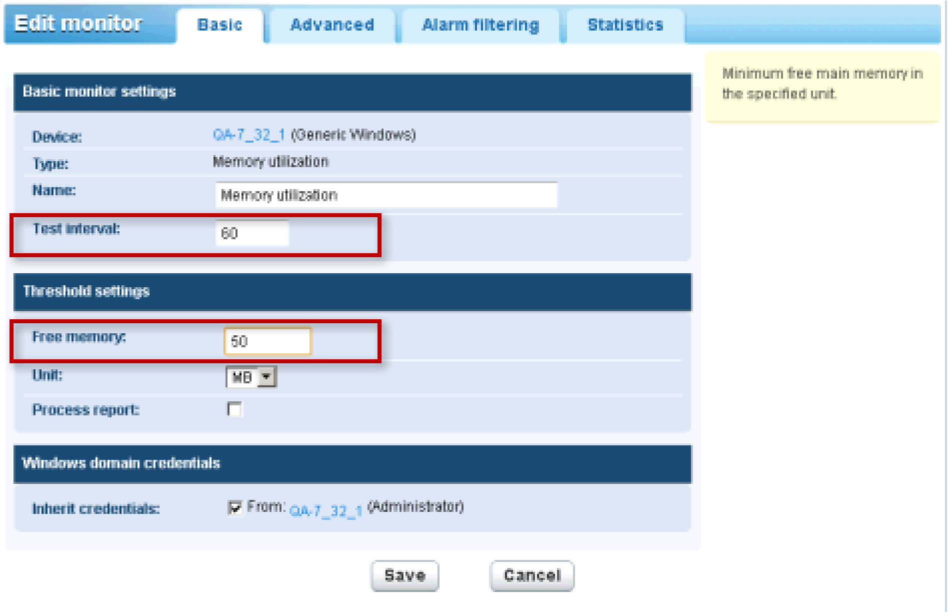


Select monitor

- Select monitor type
  - Preconfigured
  - Web and Email
  - SNMP
  - Performance
    - Bandwidth utilization
    - CIM monitor
    - CPU utilization
    - Disk utilization
    - Memory utilization
    - Swap file utilization
    - Windows performance
    - WMI Query
  - Processes
  - Databases
  - Directory services
  - Log
  - Script
  - Network services
  - Others

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*.



Basic monitor settings

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

Threshold settings

Free memory:	50
Unit:	MB
Process report:	□

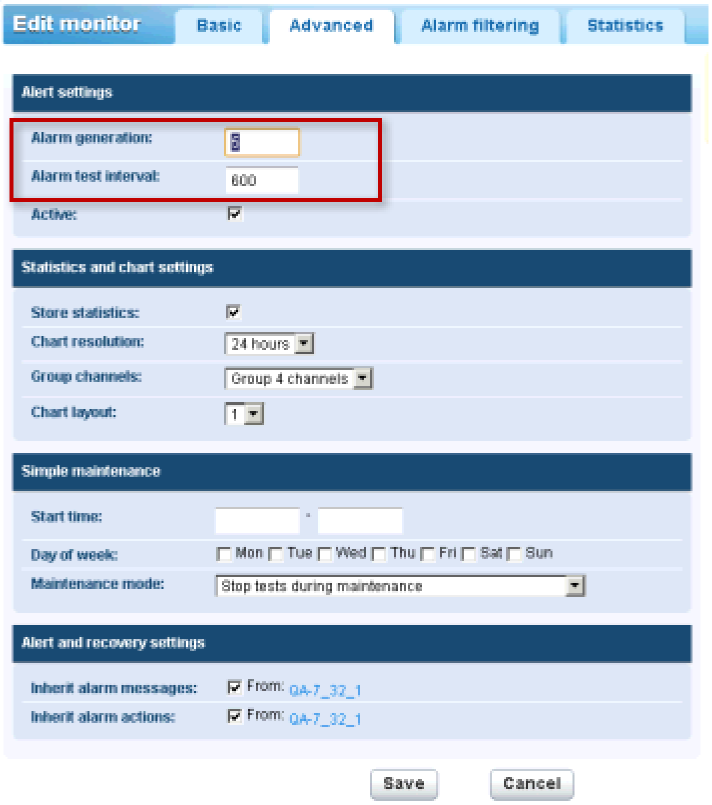
Windows domain credentials

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

Minimum free main memory in the specified unit.

- 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.



Alert settings

Alarm generation: 5

Alarm test interval: 600

Active: ☑

Statistics and chart settings

Store statistics: ☑

Chart resolution: 24 hours

Group channels: Group 4 channels

Chart layout: 1

Simple maintenance

Start time: -

Day of week: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Maintenance mode: Stop tests during maintenance

Alert and recovery settings

Inherit alarm messages: ☑ From: QA-7_32_1

Inherit alarm actions: ☑ From: QA-7_32_1

- 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 **Monitor Status Progression** *(page 53)*:
  - ➢ The first time a monitor fails a test it begins displaying a warning 🟧 icon next to the monitor in the navigation 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 navigation 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

- **Device** - The name of the device.
- **Type** - The type of monitor. The identified operating system determines the type of monitors that can be added to a device.
- **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, devices, 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 > 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 63)* format for this node.
- **Inherit actions** - If checked, inherited actions and inherited recovery actions are included on the **Actions tab** *(page 55)* 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.

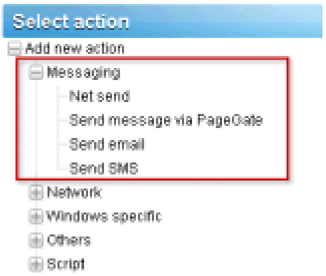
> **Note:** The following *standard monitor settings* display on most monitors. See the Monitor reference for *monitor-specific settings*.

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.

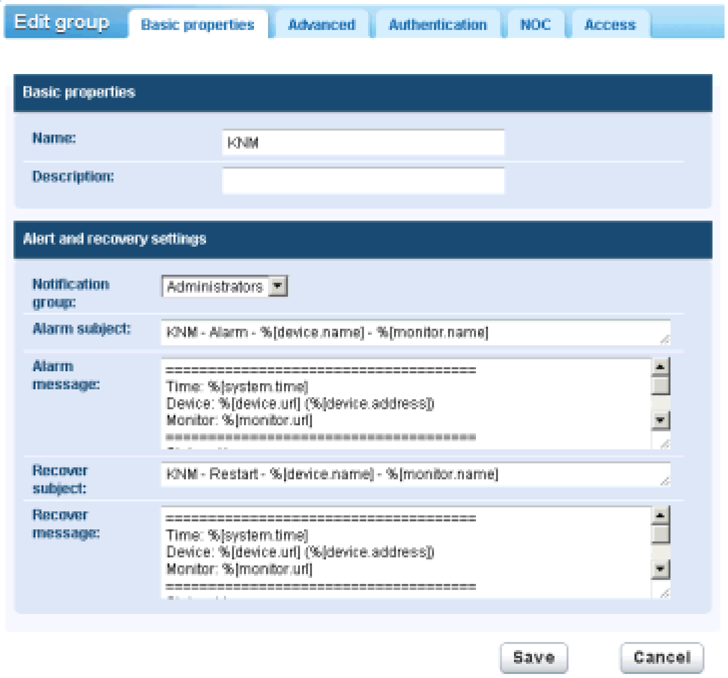
Alarm Messages

Alarm messages can be specified for groups, gateways, devices, 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 navigation 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 65)* available to use.



Basic properties

Name: KNM

Description:

Alert and recovery settings

Notification group: Administrators

Alarm subject: KNM - Alarm - %[device.name] - %[monitor.name]

Alarm message:

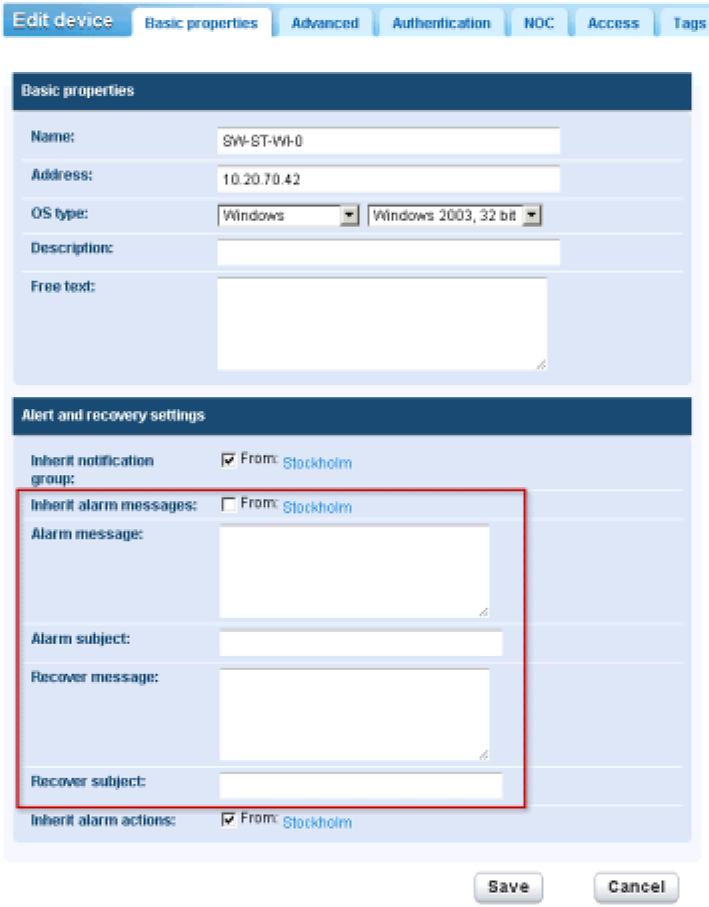
```
========================================
Time: %[system.time]
Device: %[device.url] (%[device.address])
Monitor: %[monitor.url]
========================================
```

Recover subject: KNM - Restart - %[device.name] - %[monitor.name]

Recover message:

```
========================================
Time: %[system.time]
Device: %[device.url] (%[device.address])
Monitor: %[monitor.url]
========================================
```

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.



Basic properties

Name: SW-ST-WI-0

Address: 10.20.70.42

OS type: Windows | Windows 2003, 32 bit

Description:

Free text:

Alert and recovery settings

Inherit notification group: ☑ From: Stockholm

Inherit alarm messages: □ From: Stockholm

Alarm message:

Alarm subject:

Recover message:

Recover subject:

Inherit alarm actions: ☑ From: Stockholm

Format Variables

All outgoing messages in **Network Monitor** can include formatting variables in the text of the message.

Email messages can also contain special formatting codes known as *BB codes* that can be used to improve the look of the mail.

BB codes

BB codes are a semi-standard used by many forum systems to format messages without the need of embedding HTML. It works similar to HTML, having a start and an end tag, and supports nested tags. BB codes are translated to HTML for all users that have selected to receive emails from **Network Monitor** in either the HTML or Simple HTML format. Users that have selected to receive plain text messages will have the BB codes stripped out from their messages.

Start	End	Description
[hr]		Horizontal ruler. This tag does not have a closing tag.
[b]	[/b]	Bold text

[i]	[/i]	Italic text
[u]	[/u]	Underline text
[quote]	[/quote]	Quote text (translates to the html <blockquote> markup tag)
[size=X]	[/size]	Sets the size to X pixels [size=12] Example Text [/size]
[font=X]	[/font]	Sets the text in scope to use the font "X" [font=verdana] Example Text [/font]
[color=X]	[/color]	Sets the text in the scope to use a color. The color can be any type of HTML color definition. [color=red] Example Text [/color]
[url=X]	[/url]	Creates a link to URL X [url=http://www.kaseya.com] Example URL [/url]
[img=X]	[/img]	Inlines an image located at URL X [img=http://myurl/mypic.png][/img]

Format Variables

Format flags are used to expand information in messages before they are processed and sent to their recipient. Most of these flags are context sensitive. For example, the flag `%[monitor.error]` expands the latest alarm report for the monitor triggering the action, and would not be expanded 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

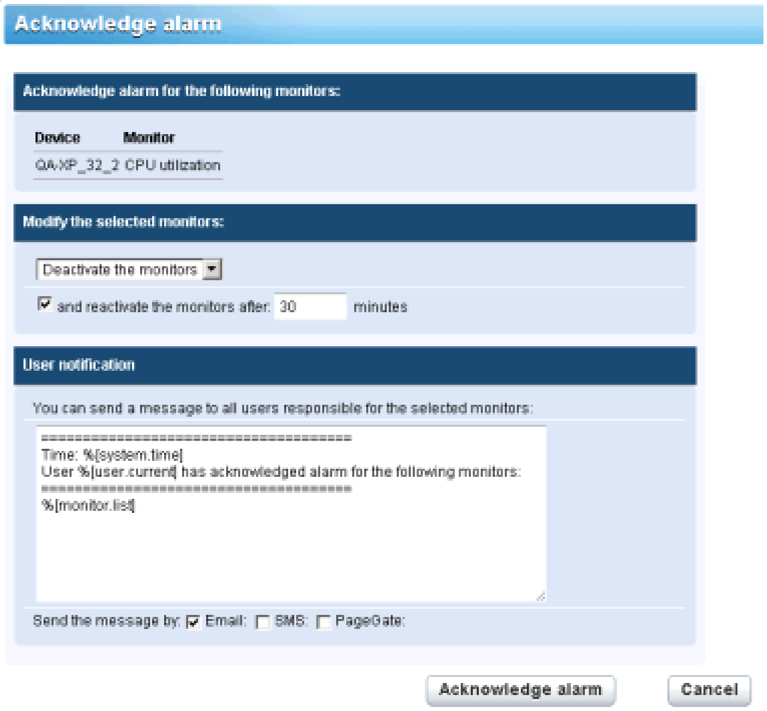
%[group.email]	group/company email
%[group.phone]	group/company phone
%[group.cellphone]	group/company cell phone
%[group.fax]	group/company fax
%[group.address1]	group/company address1
%[group.address2]	group/company address 2
%[device.local_time]	device local time
%[device.name]	name
%[device.id]	unique id of device
%[device.free_text]	
%[device.address]	
%[device.ip]	
%[device.description]	
%[device.notification_group]	
%[device.mac]	
%[device.url]	link to device
%[device.kb_article_url]	link to articles for the current device
%[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
%[system.charts]	monitor realtime charts
%[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 group, gateway or device node.

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

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



Acknowledge alarm

Acknowledge alarm for the following monitors:

Device	Monitor
QA-XP_32_2	CPU utilization

Modify the selected monitors:

Deactivate the monitors ▾

☑ and reactivate the monitors after: 30 minutes

User notification

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

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

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

Acknowledge Notification Format

The format of the acknowledge notification message is *not inherited down the navigation tree*. Instead, the default notification format is specified using the menu at the top of the page and applies to all nodes. Click the **Mail, SMS & messaging** option, then click the **Default Messages** tab to view or update this format.

> **Note:** The **Format Variables** *(page 65)* 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 viewing and publishing different types of reports.

Viewing Report Templates

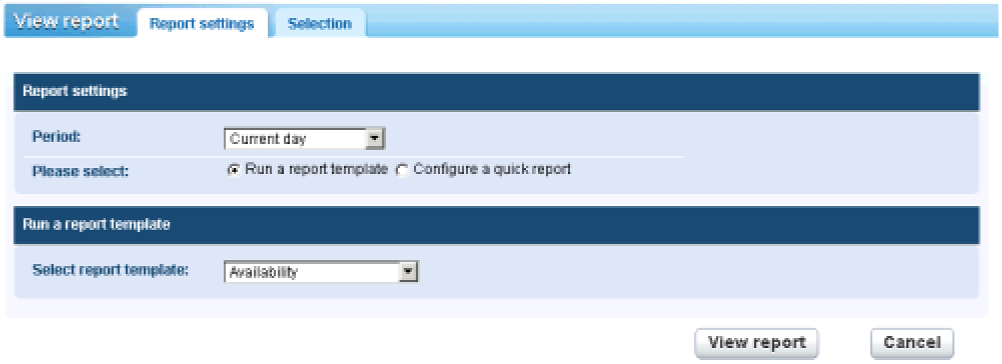
<Select a node> > Create a report > View in Browser

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

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

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

1. Select any node in the navigation tree, typically a group. Depending on the type of node, either devices 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

Period: Current day

Please select: ● Run a report template ○ Configure a quick report

Run a report template

Select report template: Availability

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 using the menu. The type of data and design elements are already selected in a report template, so the only choice you have to make is which report template to run.
- **Configure a quick report** - We recommend you select specific monitors before selecting this option. If you do, the **quick report** *(page 70)* includes a set of compatible design elements by default for the monitors you have selected. If no monitors are selected before selecting this option, you must add each design element manually.

Selection

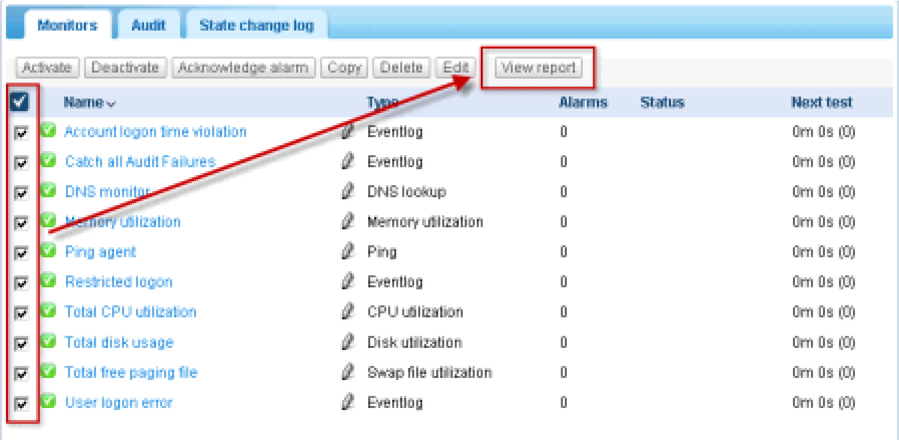
Use the **Selection** tab on the **View report** page to override the default selection of groups, devices and monitors selected for either type of report.

Viewing Quick Reports

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

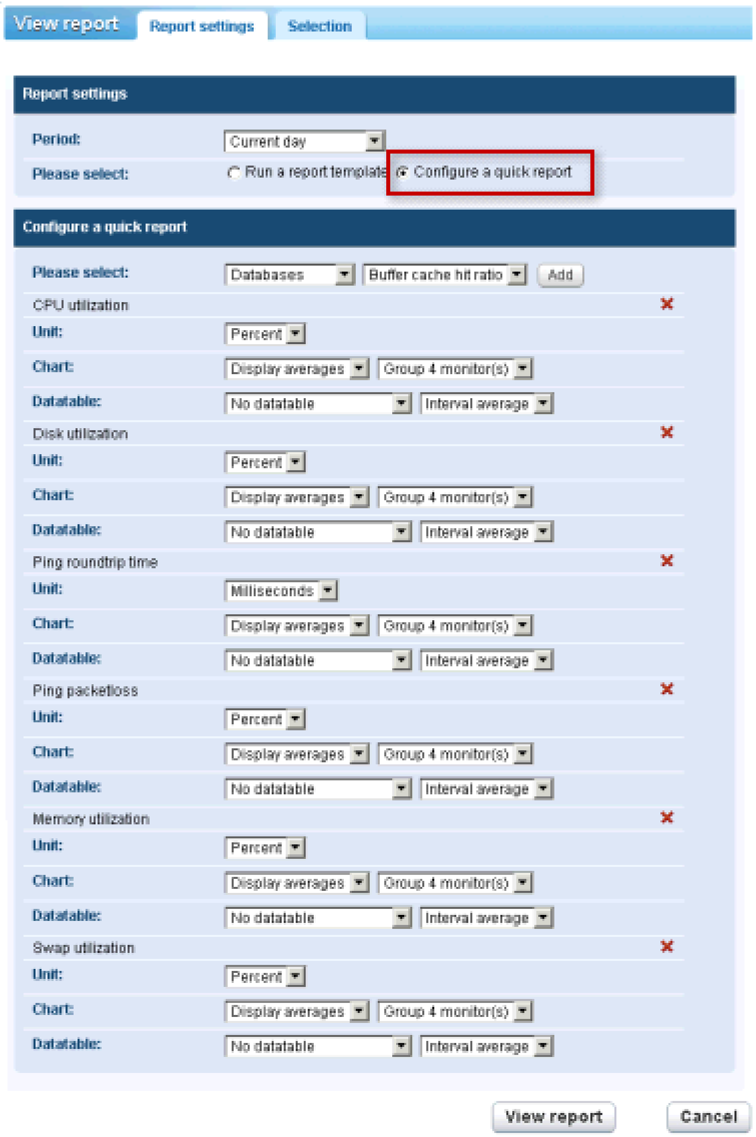
Once devices are assigned different types of monitors, run a **Quick report** to *compare data from different types of monitors.* When multiple devices are selected, data for the same monitor type is grouped together on the same graph.

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



☑	Name	Type	Alarms	Status	Next test
☑	Account logon time violation	Eventlog	0		0m 0s (0)
☑	Catch all Audit Failures	Eventlog	0		0m 0s (0)
☑	DNS monitor	DNS lookup	0		0m 0s (0)
☑	Memory utilization	Memory utilization	0		0m 0s (0)
☑	Ping agent	Ping	0		0m 0s (0)
☑	Restricted logon	Eventlog	0		0m 0s (0)
☑	Total CPU utilization	CPU utilization	0		0m 0s (0)
☑	Total disk usage	Disk utilization	0		0m 0s (0)
☑	Total free paging file	Swap file utilization	0		0m 0s (0)
☑	User logon error	Eventlog	0		0m 0s (0)

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.



Report settings

Period:	Current day
Please select:	○ Run a report template ● Configure a quick report

Configure a quick report

Please select:	Databases	Buffer cache hit ratio	Add
CPU utilization			✖
Unit:	Percent		
Chart:	Display averages	Group 4 monitor(s)	
Datatable:	No datatable	Interval average	
Disk utilization			✖
Unit:	Percent		
Chart:	Display averages	Group 4 monitor(s)	
Datatable:	No datatable	Interval average	
Ping roundtrip time			✖
Unit:	Milliseconds		
Chart:	Display averages	Group 4 monitor(s)	
Datatable:	No datatable	Interval average	
Ping packetloss			✖
Unit:	Percent		
Chart:	Display averages	Group 4 monitor(s)	
Datatable:	No datatable	Interval average	
Memory utilization			✖
Unit:	Percent		
Chart:	Display averages	Group 4 monitor(s)	
Datatable:	No datatable	Interval average	
Swap utilization			✖
Unit:	Percent		
Chart:	Display averages	Group 4 monitor(s)	
Datatable:	No datatable	Interval average	

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 **menu > Edit my settings > Interface options > 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, devices and monitors.

> **Note:** You can also select the **Run a report template** option to run a report with a pre-defined layout for the devices 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, devices and monitors.* For that reason customized reports are not run by first selecting a node in the navigation tree. *Instead you both create and run customized reports by selecting* **> 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, devices and monitors.

Emailing and publishing reports

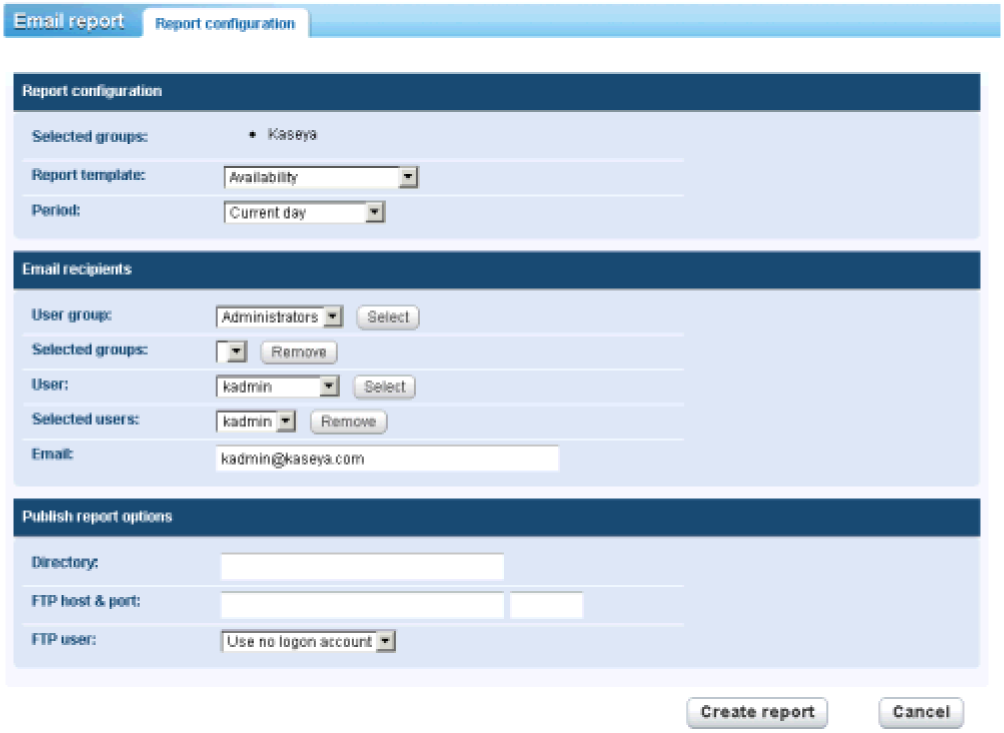
<Select a node> > Create a report > Email or publish

> 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, devices or monitors *first*.

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



Email report | Report configuration

Report configuration

Selected groups:	• Kaseya
Report template:	Availability
Period:	Current day

Email recipients

User group:	Administrators [Select]
Selected groups:	[Remove]
User:	kadmin [Select]
Selected users:	kadmin [Remove]
Email:	kadmin@kaseya.com

Publish report options

Directory:	
FTP host & port:	
FTP user:	Use no logon account

Report configuration

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

Email recipients

- **Select devices / Selected devices** - Enter text matching the any part of a the name of device. Select one or more devices from the **Select devices** 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 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 28)* section. Documentation for the Generate report event specifically can be found in the **Scheduled event reference** section.

Configuration Summary

If you're new to **Network Monitor** v5.0, 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. Run through the **Installation Checklist** *(page 1)*.
2. **Install Network Monitor v5.0** *(page 1)* on a network with other devices you can test with.
   - Use the **Server install** option. A `Local gateway` will be installed as well.
3. Run through the **KNM Startup Guide** *(page 3)* after **Network Monitor** is installed.
   - Ensure the **Gateway Server Settings** *(page 4)* page is configured with an IP address and port.
4. **Logon** *(page 6)* to **Network Monitor**.
5. Review the list of devices found by **Network Discovery** *(page 45)* in the `Discovery group`.
   - Run Network Discovery again for a other subnets that share the same LAN as the `Local gateway`.
6. **Move** *(page 18)* one or more devices out of the `Discovery group` to the `Local gateway`.
   - *Devices must be moved out of the Discovery group to enable the generation of alarms.*
7. Add **monitors** *(page 59)* to any device outside of a `Discovery group`.
8. Change the settings for the monitor threshold so as to force the monitor test to fail. This will enable you to watch the **Monitor Status Progression** *(page 53)*.
9. Define **actions** *(page 55)* that are executed when a monitor fails a test a consecutive number of times.
10. Test the monitor by creating a **Simulate Alarm** *(page 59)* report to confirm the alarm is configured as you expect.