Kaseya 2

# IIS Monitor

## Quick Start Guide

for Network Monitor 4.1

June 5, 2012

## About Kaseya

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

# 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.

### IIS Monitor

This quick start guide demonstrates how to configure the *monitoring of Microsoft Internet Information Server (IIS) webservers* using **Network Monitor**. Except for the limited number of objects you can configure using the free version of **Network Monitor**, you have access to most of the advanced monitoring features **Network Monitor** has to offer.

**Network Monitor** uses *object templates* to quickly configure and assign a *set of monitors* to an IIS server. Types of monitors include:

- Bytes Total/sec
- CGI Requests/sec
- CPU utilization
- Current connections
- File Cache Hits %
- Get Requests/sec
- ISAPI Requests/sec
- Memory usage
- Post Requests/sec
- Service running
- URI Cache Hits %

### How This Quick Start Guide is Organized

1. **Network Monitor** Concepts
2. **Installation and Setup** *(page 4)*
3. **Configuring IIS Monitor** *(page 10)* - Provides a step-by-step, "first time" demonstration of how to configure IIS Monitor.

# Network Monitor Concepts

Familiarize yourself with the following terms and concepts to help quick start your understanding of **Network Monitor**.

- **Object** - An object represents a computer or any other device that can be *addressed by an IP number or host name*. An object contains settings that are common to all monitors in that object.
- **Network** - Within **Network Monitor** the term *network* refers to user-defined grouping of objects. *Member objects of a* **Network Monitor** *network do not have to belong to the same physical network.* **Network Monitor** networks can be compared to a folder in a file system. Every object must be a member of a **Network Monitor** network. You can activate and deactivate an entire network of objects.
- **Monitor** - A monitor tests a specific function in an object. Most monitors are capable of collecting various statistical data for reporting purposes. *If a monitor fails a test it firsts enter a failed state. After a number of consecutive failed tests it then enters an alarm state. When entering an alarm*

*state a monitor executes a number of actions specified in the alarm action list used by the particular monitor.*

- **Action list** - An action list defines a number of actions to be executed as a monitor enters, or recovers from, an alarm state.
- **Operator** - **Network Monitor** users are called operators. An operator contains login information, contact information and privileges. An operator can be a member of one or more operator groups.
- **Operator group** - An operator group is a collection of operators. Each object in **Network Monitor** is assigned to one operator group. Notifications sent as a response to a monitor entering an alarm state are normally sent to the object's operator group.
- **Account** - An account is a set of credentials used by a monitor, action or event to carry out an operation.

### Status Icons

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

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

Additional guidelines:

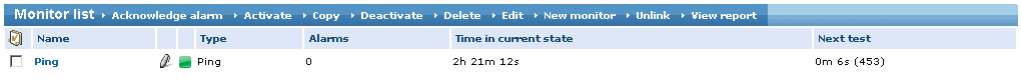
- Any state other than deactivated is an activated state.
- An activated monitor tests its object.
- Deactivating any or all monitors of an object does not deactivate the object.
- Deactivating any or all objects of a network does not deactivate their parent network.
- Deactivating an object deactivates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

### Other Commonly Used Icons

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

# Monitor status progression

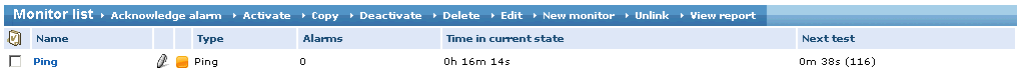
During normal operation, a monitor in **Network Monitor** is in the *Ok* state, displayed in the management interface with a green status icon. Here is an example from the monitor list view.




*A monitor during normal operation is displayed with a green status icon.*

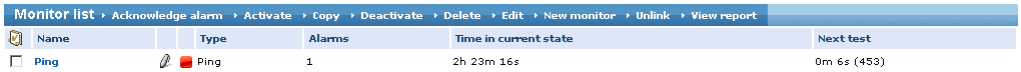
Whenever a monitor fails its test, it changes to the *Failed* state, displayed in the management interface

with an orange status icon.




*A monitor in failed state is displayed with an orange status icon.*

When a monitor keeps failing tests, it eventually changes into the *Alarm* state, displayed with a red status icon. The number of failed tests required for an Alarm state depends on the **Alarm generation** parameter for each monitor. Increasing the **Alarm generation** parameter makes the monitor less sensitive to temporary outages, and decreasing the parameter makes it more sensitive.

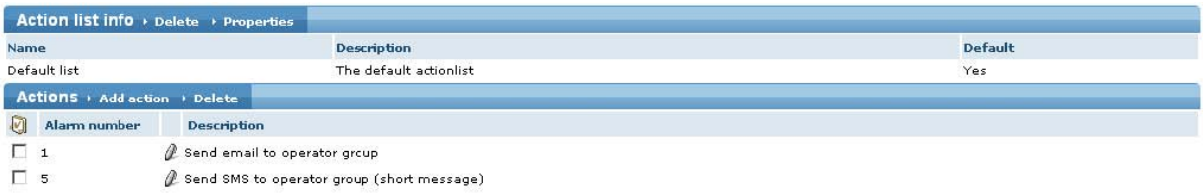



*A monitor in alarm state is displayed with a red status icon.*

When a monitor first enters an alarm state, the **Alarms** column displays a `1`. This is the *alarm count*. This means that the monitor has now generated one alarm. When the monitor is tested the next time and still fails its test, the number of alarms will be two, and so on. The alarm count is very important, because it controls what actions are taken in response to alarms.

# Responding to alarms

An **action list** is a collection of actions executed in response to an *alarm count*. Every monitor in **Network Monitor** has an action list, either defined directly by a *monitor's* properties, or indirectly by a *object's* properties. For each alarm count in an alarm list, **Network Monitor** executes all actions specified for that alarm count. It is possible—and common— to define several actions for the same alarm count.




*Actions example*

In the example above, there are two actions shown. The first action, for the *first* alarm, is a **Send email** action. The next action, configured for the *fifth* alarm, is a **Send SMS** action.

For details on how to edit and configure action lists and actions, see the Action lists topic.

# Recovering from alarms

A monitor may recover from an Alarm state *by itself*. If so, **Network Monitor** is able to react to this event. For example, if a monitor is currently in an Alarm state and performs a test that succeeds, the monitor status automatically *changes back to an Ok state*. When a monitor recovers, **Network Monitor** can execute a **recover action list**, if one is specified. A recover action list can be specified by a *monitor* or indirectly by the *object* of a monitor.

When the monitor recovers, *all* actions defined in the recover action list are executed, regardless of the alarm number. Creating separate action lists to serve as recover action lists is recommended.

# Installation and Setup

**In This Section**



# Installation Checklist

We recommend that you complete the following pre-installation checklist before installing **Network Monitor**.

1. Estimate the memory required by **Network Monitor** to monitor the number of objects on your network, using the recommendations in **Server Sizing** *(page 5)*. Ensure the system hosting the **Network Monitor** server has enough free memory to run **Network Monitor**.
2. Check that the system hosting the **Network Monitor** server meets **all software and hardware requirements** *(page 5)*.
3. Ensure the Windows account used by the **Network Monitor** service has **sufficient privileges** *(page 5)*.
4. If SNMP is used, install and start the Windows SNMP service on the **Network Monitor** host machine. The SNMP service on the host machine must specify the same communities used by **Network Monitor**.
5. If ODBC logging is going to be enabled using Settings > Program settings > Log settings, create a ODBC system data source on the **Network Monitor** host machine.
6. If a GSM phone is used, install it and verify that it responds correctly to standard AT commands in a terminal program.

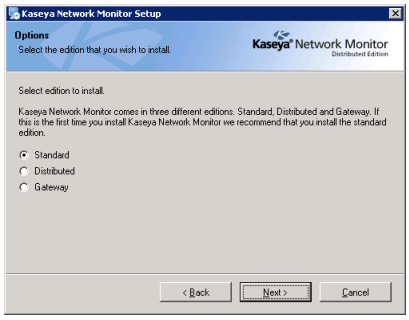
When completed you are ready to install **Network Monitor**. After installing **Network Monitor** and connecting to the web interface for the first time, consult the topic **Running the Startup Guide** *(page 6)*.

# Standard, Distributed and Gateway Installs

During a `KNMsetup.exe` install you are asked to select one of the following options. The Distributed and Gateway options only apply if you are monitoring multiple subnets.

- **Standard** - Selected by default. If monitoring a single subnet, select this option. *Recommended for first time evaluations.*
- **Distributed** - If monitoring multiple subnets, select this option if installing the server all gateways send data to.

- **Gateway** - If monitoring multiple subnets, select this option if sending data to a distributed server.




# 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 System 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.

Supported Browsers

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

The following features must be enabled in your browser settings.

- Accept third party cookies
- Javascript enabled

Cookies are required to keep track of the user session. Java scripts are used by the web interface and must be enabled.

# 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.

# Logging On

After installing **Network Monitor** the next step is to logon to the web interface. Use either of the following two methods to display the web interface logon page.

- Click the link to the web interface in the **Network Monitor** program folder in the start menu.
- Use the following link if you are configuring **Network Monitor** from the **Network Monitor** host.
  `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.

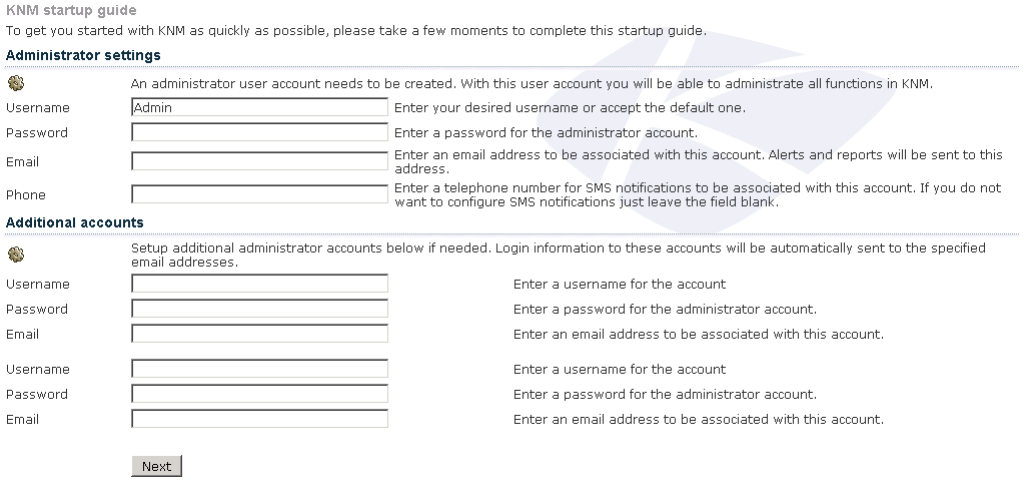
# Running the Startup Guide

Logging on the first time to the web interface displays a step-by-step **Startup Guide** to help you get **Network Monitor** ready to use. The **Startup Guide** has five steps.

- **Administrator settings** *(page 7)*
- **Network discovery settings** *(page 7)*
- **Mail settings** *(page 8)*
- **SMS device configuration** *(page 8)*
- **Review and Save Settings** *(page 9)*

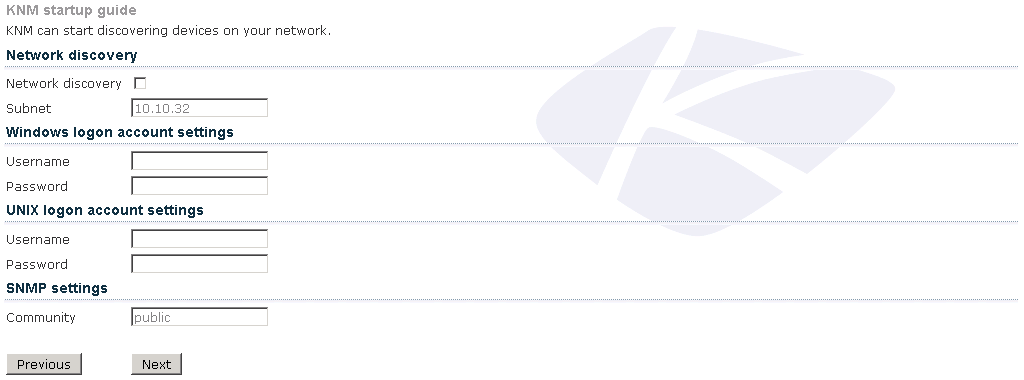
> **Note:** A person logging into the **Network Monitor** server is referred to as an *operator*. Each operator can only have one logon *session* open at one time.

# Administrator settings




1. Enter the username and password of the default **Network Monitor** operator. Remember that the password is case sensitive.
2. Configure an email address for this operator. The email address is used when **Network Monitor** is sending notifications or reports.
3. (Optional) Configure an phone number for this operator. The phone number is used when **Network Monitor** is sending SMS notifications.
4. Clicking **Next** creates the default operator you will use to logon to **Network Monitor** after completing the **Startup Guide**.

# Network Discovery settings

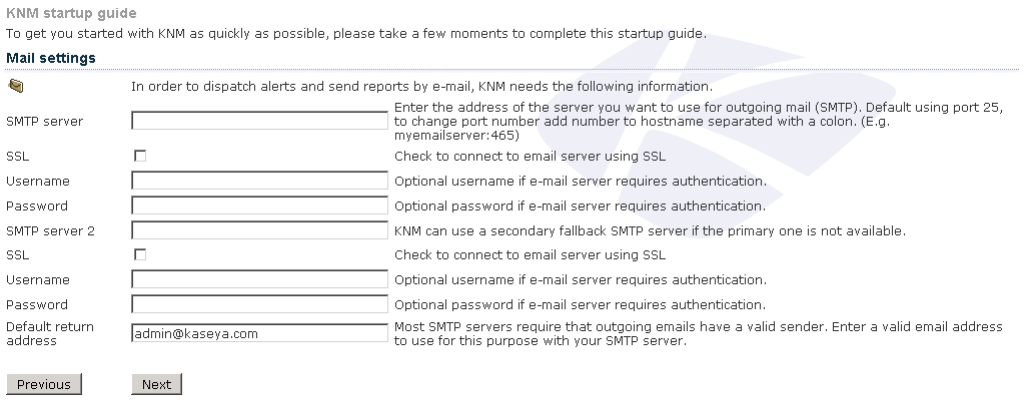



If you would like to discover objects on a network immediately, enter values for the following.

- **Network discovery** - Specify the first 3 octets of a subnet.
- **Windows logon account settings** - An administrator level Windows credential is required to return some types of scan data from Windows objects. 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 objects.
- **SNMP settings** - Enter the SNMP community name used by devices on this subnet.

> **Note:** The system hosting the **Network Monitor** server must have the Windows `SNMP Service` running to use SNMP monitoring. Any community specified by **Network Monitor** for monitoring must also be specified by the `SNMP Service` on the host machine. See **Installation Checklist** *(page 4)*.

# Mail settings

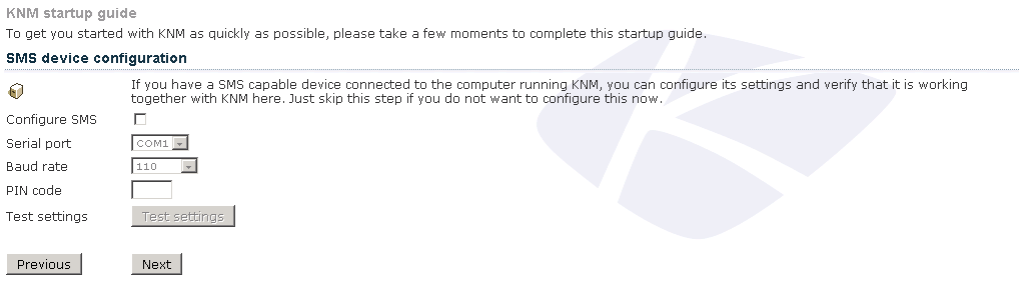



To send email notifications and reports you need to configure the email server settings. Two email servers can be configured: a primary server and a secondary backup server used in case the primary server is unreachable.

- **Primary 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.
- **(Optionally) Secondary server** - Enter the host name of the server and optionally credentials used when **Network Monitor** sends an email. This server is used by **Network Monitor** if the primary SMTP server is unreachable.
- **Default return address** - Enter an address that **Network Monitor** uses as its From address.

If you want to skip this step and configure these parameters later, click **Next** to continue. To display these settings again later, select Settings > Program settings > Email & SMS settings.

# SMS device configuration




If 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.

### Operator phone number

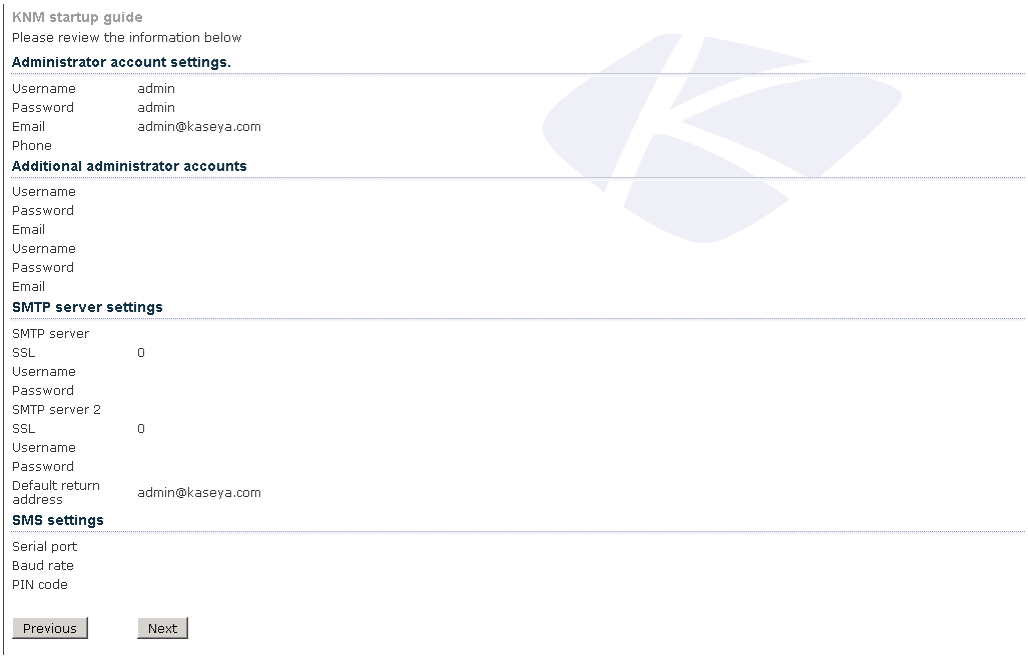
If you did not enter a phone number on the first step in the startup guide you can enter it in the My settings page, without the phone number. **Network Monitor** is unable to send the operator an SMS notification. You are able to access the **My settings** page when you logon after the startup guide is completed.

### Tested SMS devices

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

In addition to this list almost all modern GSM phones and modem works. The requirement is that the device should support Text mode sms and that it can be connected to a com port. It may also be connected to an USB port but the device driver must be able to emulate a standard serial port so it can be discovered by **Network Monitor**.

## Review and Save Settings


KNM startup guide

Please review the information below

**Administrator account settings.**

| | |
|---|---|
| Username | admin |
| Password | admin |
| Email | admin@kaseya.com |
| Phone | |

**Additional administrator accounts**

| | |
|---|---|
| Username | |
| Password | |
| Email | |
| Username | |
| Password | |
| Email | |

**SMTP server settings**

| | |
|---|---|
| SMTP server | |
| SSL | 0 |
| Username | |
| Password | |
| SMTP server 2 | |
| SSL | 0 |
| Username | |
| Password | |
| Default return address | admin@kaseya.com |

**SMS settings**

| | |
|---|---|
| Serial port | |
| Baud rate | |
| PIN code | |

Previous Next

1. The final step of this startup guide is confirming the information you have filled in previous pages. If you want to change any of the information, click the **Previous** button to go back.
2. Clicking the **Next** button redirects you to the login page and asks for the username and password that you entered in the first page.

# Configuring IIS Monitor

The following procedures provide a step-by-step, "first time" demonstration of how to configure a *IIS Monitor* within **Network Monitor**. Not all options for each step are described, but should be enough to get you started.

*These procedures should be followed in the order presented.*

**Note:** These procedures assume you've completed the **Installation and Setup** *(page 4)* of **Network Monitor**.

**In This Section**



# Configuring Operators

A person logging into the **Network Monitor** server is referred to as an *operator*. Each operator can only have one logon *session* open at one time.

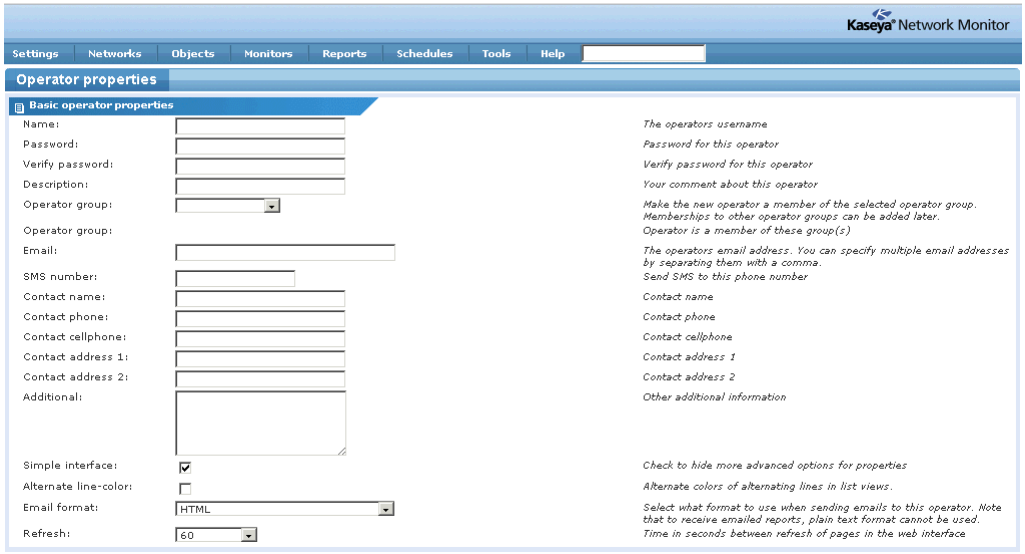
Each operator can be a member of one or more *operator groups* and must be a member of at least one. Each object in **Network Monitor** always belongs to one operator group. In this way, an operator group in **Network Monitor** can be thought of as being in charge of an object. Normally, alerts for a monitor are sent to the operator group responsible for the object.

**Note:** *Logon accounts* should not be confused with the logons created for operators who administer **Network Monitor**. Logon accounts are used by some monitors and actions to authenticate against remote hosts. A logon account is always tied to an operator group. A logon account is only accessible to members of the logon account's specified operator group.

In this procedure, you create a new operator for yourself.

1. Click Settings > **Operators**.

2. Click **New operator**.



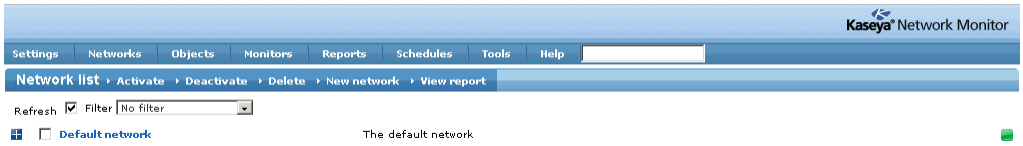

3. Enter values for the following fields.
   - **Name**
   - **Password**
   - **Verify password**
   - **Operator group** - Select `Administrators`. You can select a different operator group later.
   - **Email** - Enter your email address.
4. Click **System administrator** button. This will auto-populate many of the other options on this page.
5. Click **Save** to save your settings.

**Note:** If you like, you can click Settings > **Operator group** to create a new operator group and add operators to that new operator group. All the procedures in this quick start guide assume you are a member of the default `Administrators` operator group.

# Configuring Networks

In this procedure you ensure the default network provided by **Network Monitor** is activated.

1. Select Networks > List.




2. Ensure the `Default Network` has an *activated* icon. If not, check the checkbox next to `Default Network` and click **Activate**.
   - A **Network Monitor** network is a user-defined collection of objects that you choose to manage as a group. *A* **Network Monitor** *network should not be confused with the physical networks that computers and devices belong to.*
   - Each object you monitor must belong to a **Network Monitor** network.
   - **Network Monitor** provides a single `Default Network` for you to use. You can create additional networks if you like.

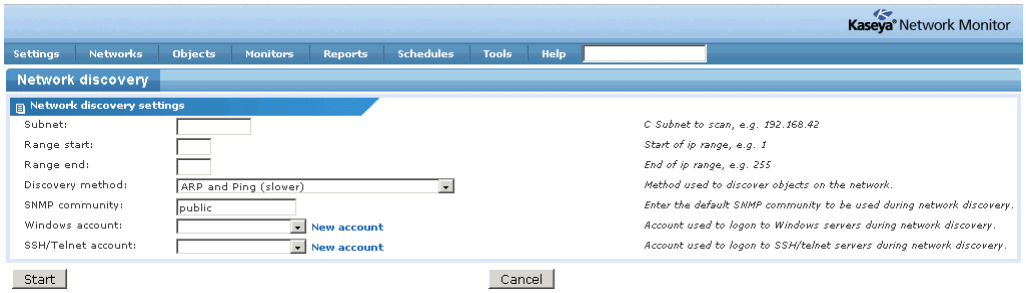
- *Activating* `Default Network` ensures any object that belongs to it can be activated for monitoring.

3. Click `Default Network` to see network details, including any objects that already belong to this **Network Monitor** network.

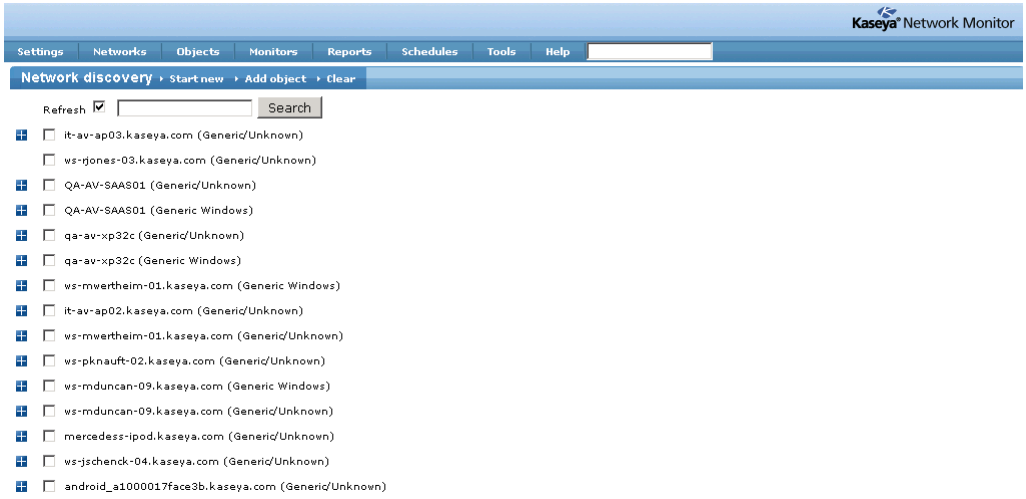
# Adding Objects using Network Discovery

In this procedure you discover computers and devices by scanning your local area network. Then you configure a discovered object and add it to your default **Network Monitor** network. *A discovered machine or device must be configured as an object and added to a network before it can be monitored.*

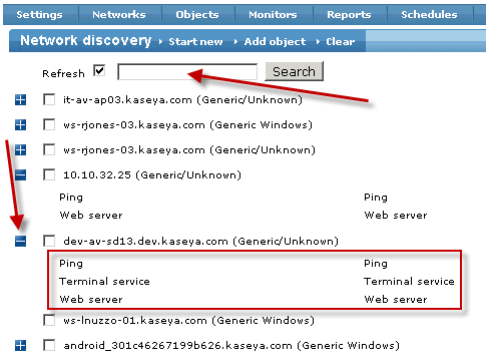
1. Select Tools > Network Discovery > Start New.




2. Specify a subnet to scan.
   - Enter the first three octets of the subnet. For example: `192.168.1`.
   - For the fourth octet, enter a range between, or equal to, `1` and `255`.
   - Select the `ARP only` scanning option to generate the quickest results.
   - No other options are required.
   - Click **Start** to start the scan. *It may take several minutes to return a list of discovered objects.*

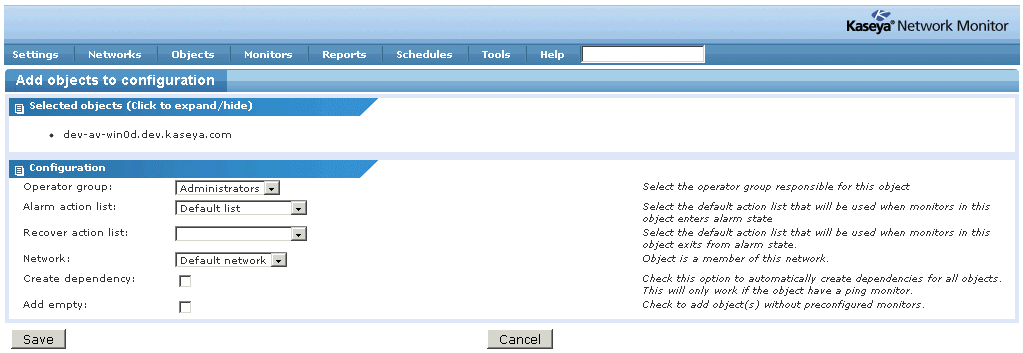



3. Select a *Windows* computer that you know is running a Microsoft Internet Information Server (IIS) webserver. If you're not sure which of the discovered Windows computers listed are running IIS, a Windows computer running IIS typically has the `Web server` monitor automatically assigned to it. Use the *search* method described below to find all machines automatically assigned a preconfigured `Web server` monitor.
   - You can determine the monitor types automatically assigned to a machine or device by clicking the plus icon ⊞ next to the name of the machine or device. A list of monitor types displays.




- You can also search for all machines and devices automatically assigned a monitor type by entering the name of the monitor type in the search edit box and clicking the **Search** button.

4. Click the **Add object** link on the **Network discovery** section menu.
   - *A discovered machine or device must be configured as an object and added to a network before it can be monitored.*
5. Accept the default values assigned to the object on the **Add objects to configuration** page.

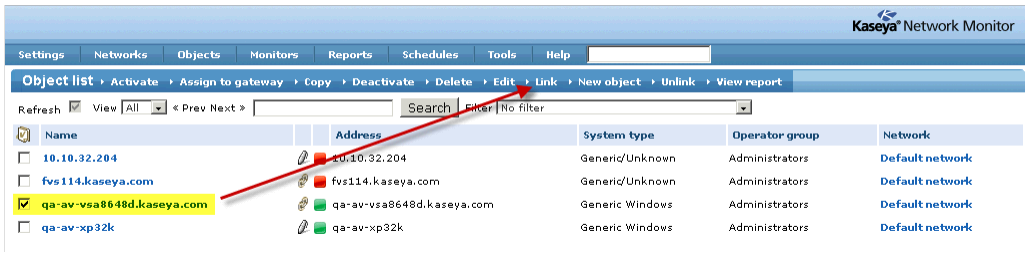



- Accept the default **Operator Group** (**Network Monitor** user group) to assign the object.
- Accept the default **Alarm action list** to assign the object. An alarm action list determines the actions that occur in response to an alarm condition.
- *Leave the* **Recover action list** *blank for now.*
- Accept the `Default network` **Network**.
- *Leave the* **Create dependency** checkbox *blank for now.*
- *Leave the* **Add empty** *checkbox blank.*
- Click **Save** to complete the configuration of the object.

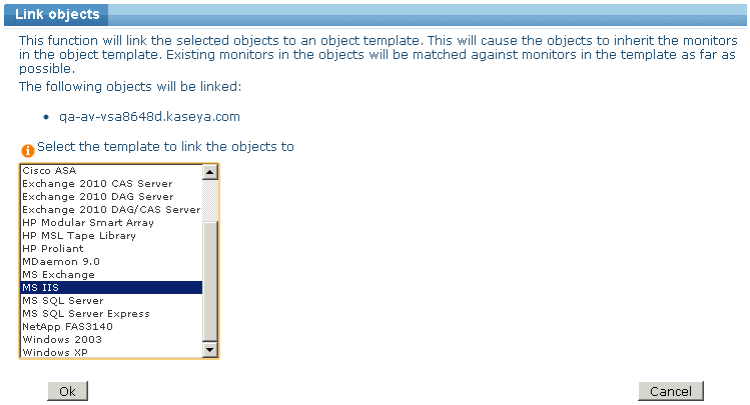
# Adding Monitors by Object Template

In this procedure you link the new object you just created to an *object template*. Linking an object template adds a specialized set of monitors to the ones already assigned to your new object. In this case, the object template is called the `MS IIS` object template and is used to monitor performance metrics on Windows computers running IIS.

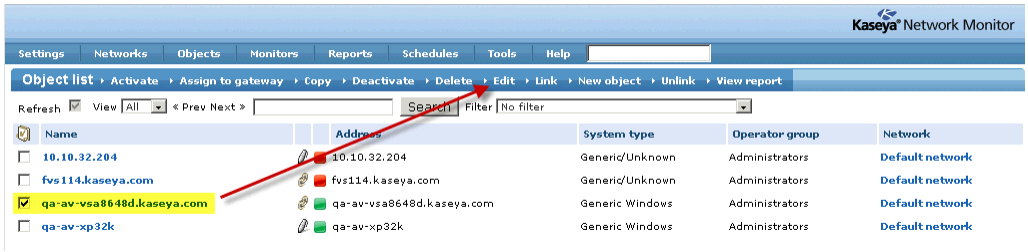
1. Select Objects > List. All objects in all networks display.




2. Check the checkbox next to the name of the object you just added. Then click the **Link** option in the **Object list** section menu.

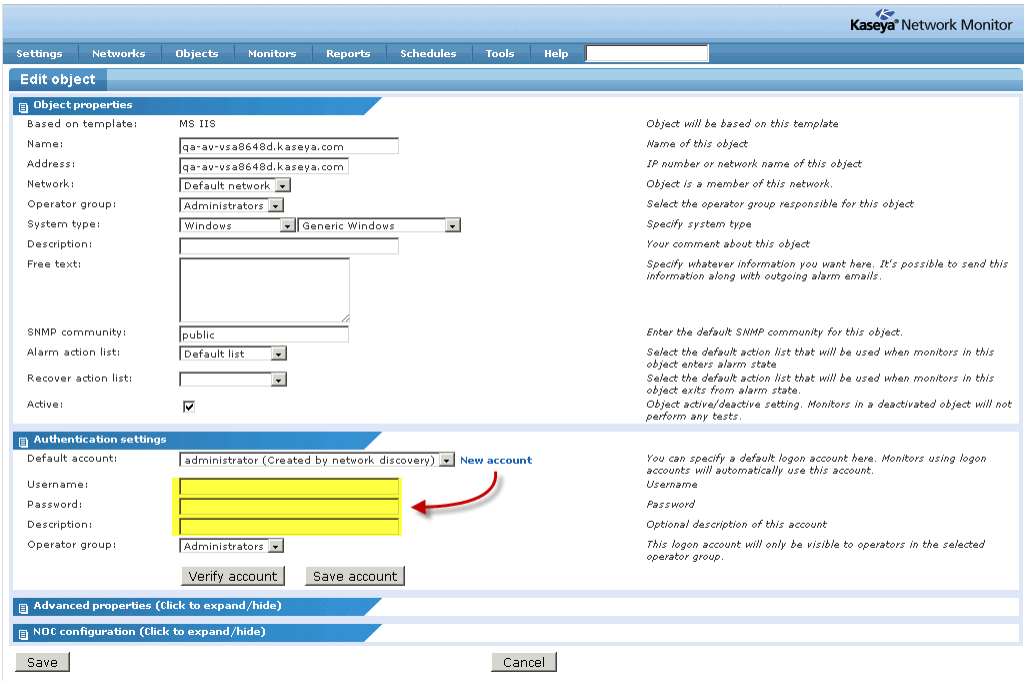



3. Select `MS IIS` in the scrollable drop-down list, then click the **Ok** button.
   - The set of monitors in the `MS IIS` object template has been added to the object you selected.
   - Because these are Windows performance monitors, an administrator level credential must be added to the object to provide access for these monitors. You create this credential in the next step.
4. On the same **Object list** page check the checkbox next to the name of the object you just added. This time click the **Edit** option in the **Object list** section menu.



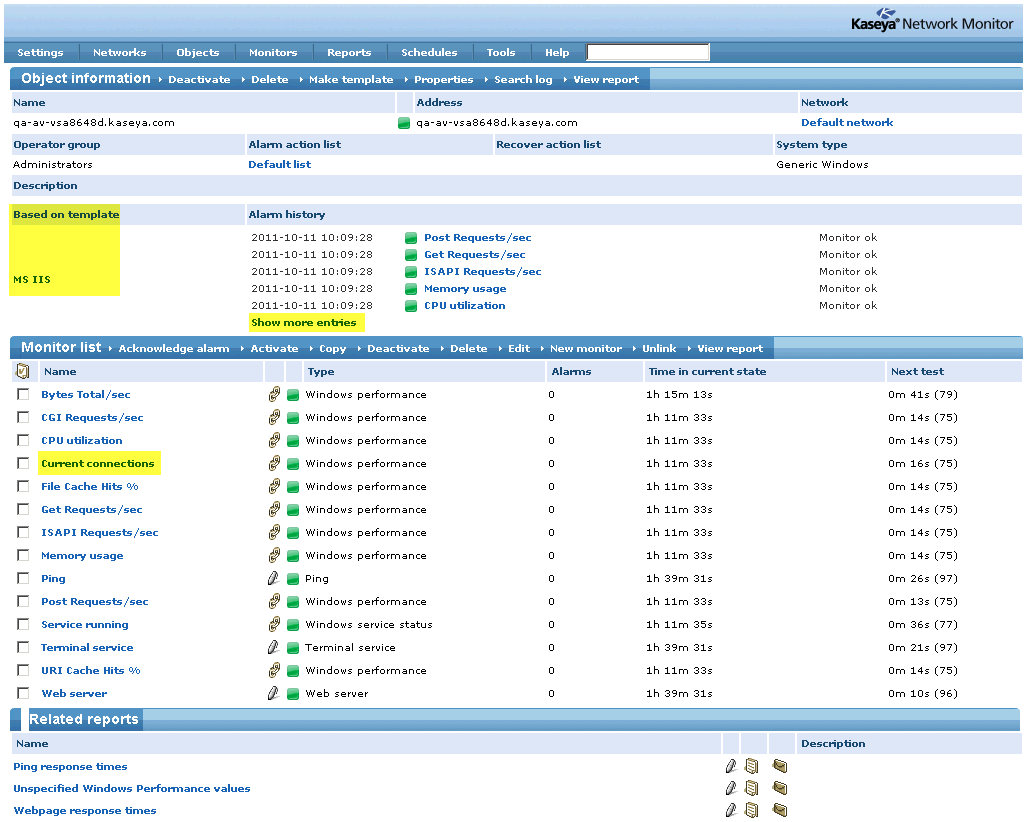

5. Click the **New account** phrase in the **Authentication settings** section to expand this section. Enter a **Username**, **Password** and **Description**. Click **Verify account** to test the credential before you click the **Save account** button.

**Note:** Ensure the **Default account** drop down list has your *new credential selected* before you **Save** and close the **Edit object** page.



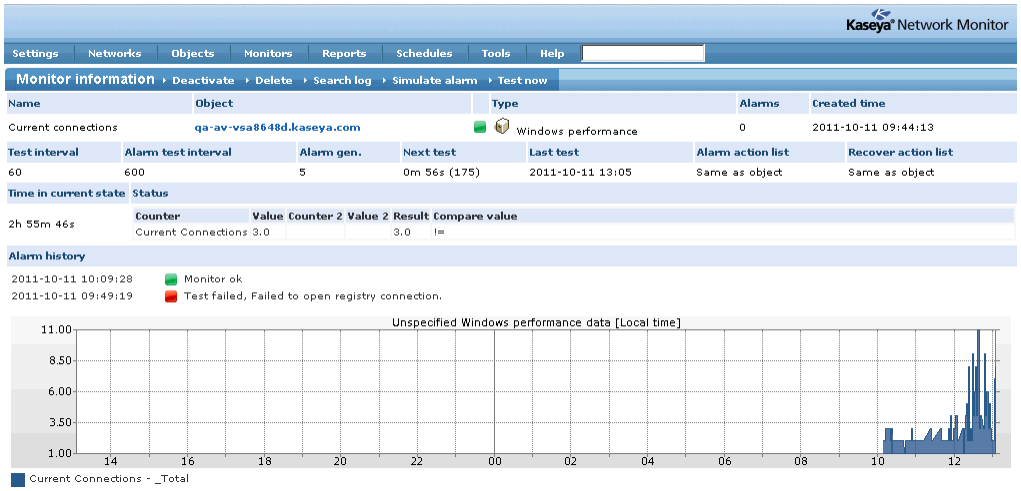

Once you save the credential you can view the data returned by `MS IIS` monitors.

6. On the same **Object list** page click the name of the object you just added.



- The **Name**, **Address** and **Network** displays in the **Object information** section at the top of the page.
- A list of the monitors assigned to this object displays in the **Monitor list** section in the middle of this page. They are now all active.
- Most of these monitors were assigned using the `MS IIS` object template. You can see the complete list of monitors based on the object template, by clicking the phrase **Show more entries** at the bottom of the **Alarm history** column. They are grouped together to the right of `MS IIS` in the **Based on template** column.

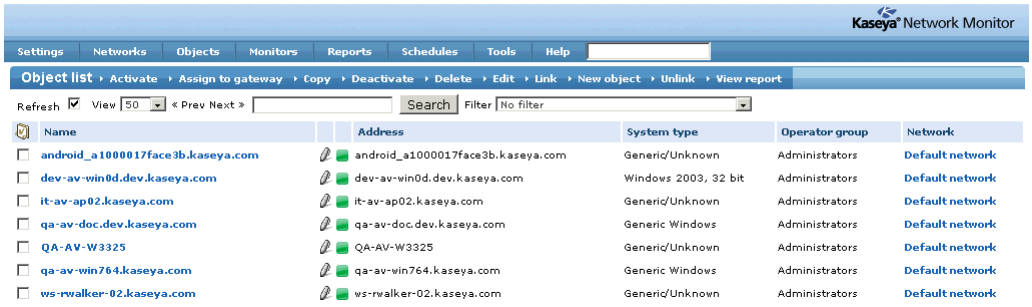
7. Click the phrase `Current connections` in the **Name** column of the **Monitor list**, for a monitor with a green status icon.
   - The **Monitor information** page displays.
   - *If you just added the object, the monitor may not have returned any data yet.*




# Viewing Reports

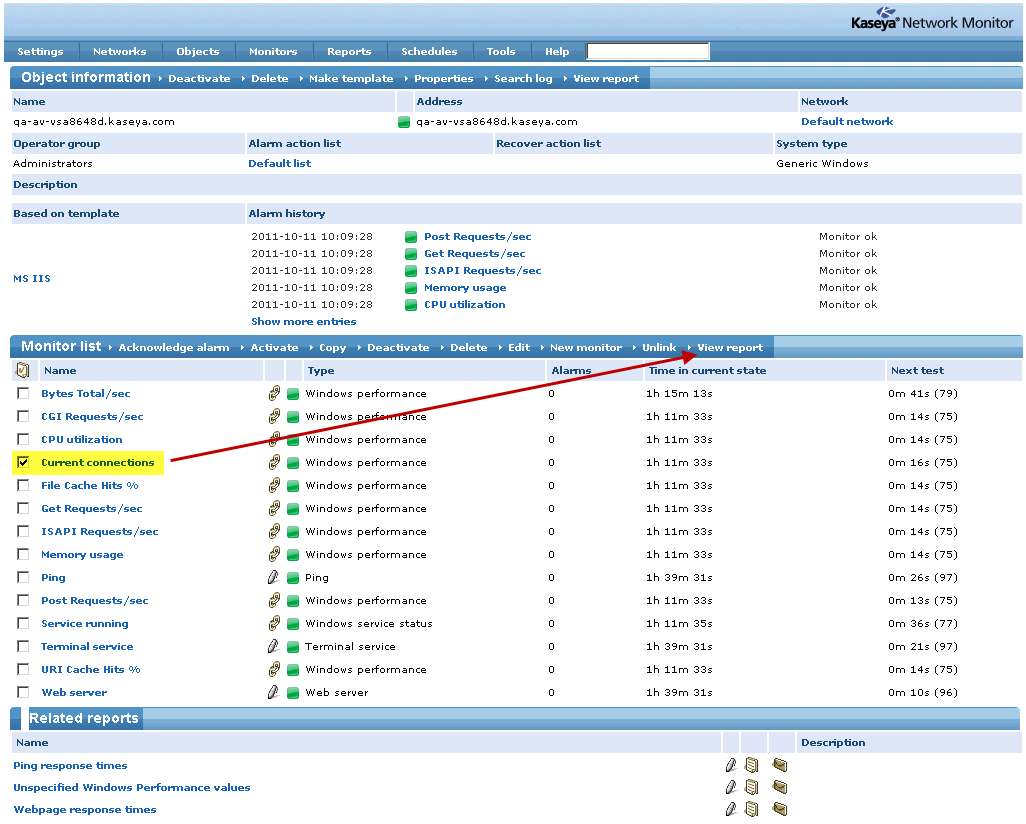
In this procedure you view a report of the data returned by the `Current connections` monitor.

1. Select Objects > List. The objects you've added display.




2. Click the name of the object you just added to be monitored. The **Object information** page displays.

3. Check the checkbox next to the phrase `Current connections`. *Just add this one monitor the first time you run this report.* Then click the **View report** option in the **Monitor list** section menu.



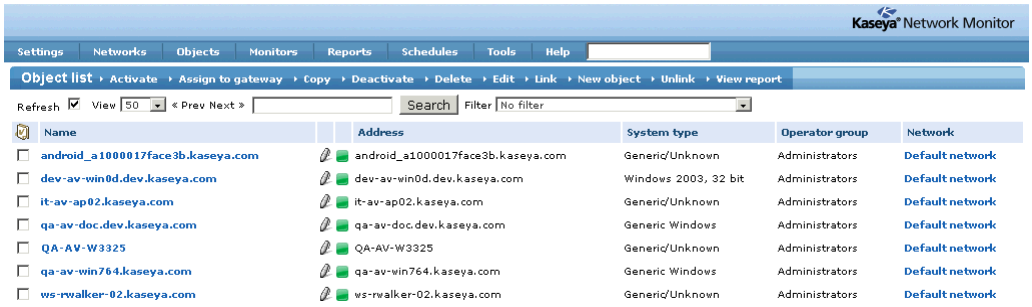

4. The **Create quick report** page displays. *Accept all of the defaults.*


5. Click the **View Report** button at the bottom of the page.
   - A `Webpage response times` report displays.
6. Run the report again using *multiple monitors* this time.
   - A quick report is designed to quickly generate a report to compare data *from different types of monitors at the the same time*.
   - Use the **split monitors** or **group monitors** options in the **Create quick report** page to overlay data from multiple monitors onto one chart or display each monitor on its own chart.

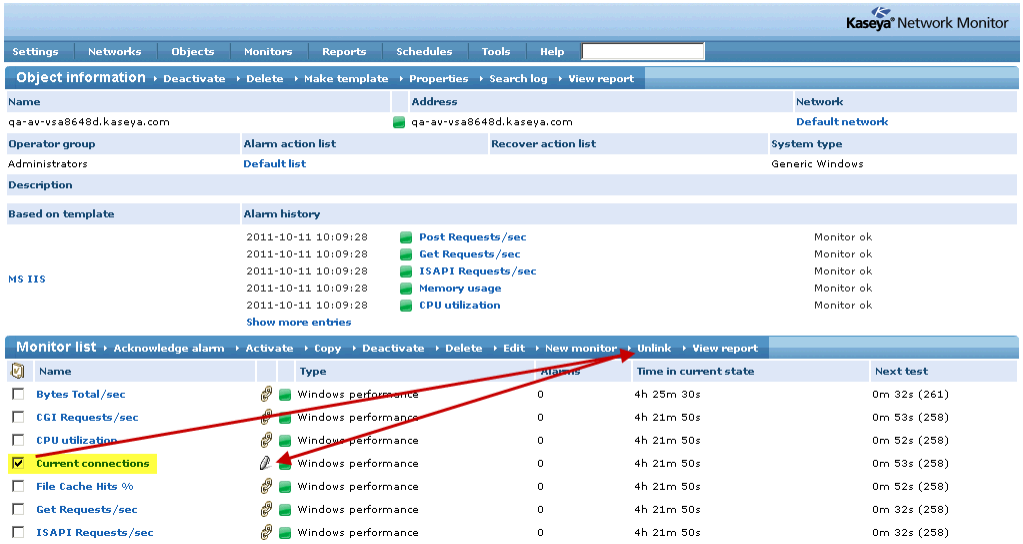
# Configuring Alarms

In this section you edit the default alarm settings for a monitor, to force an alarm to be created immediately.

1. Select Objects > List. The objects you've added display.

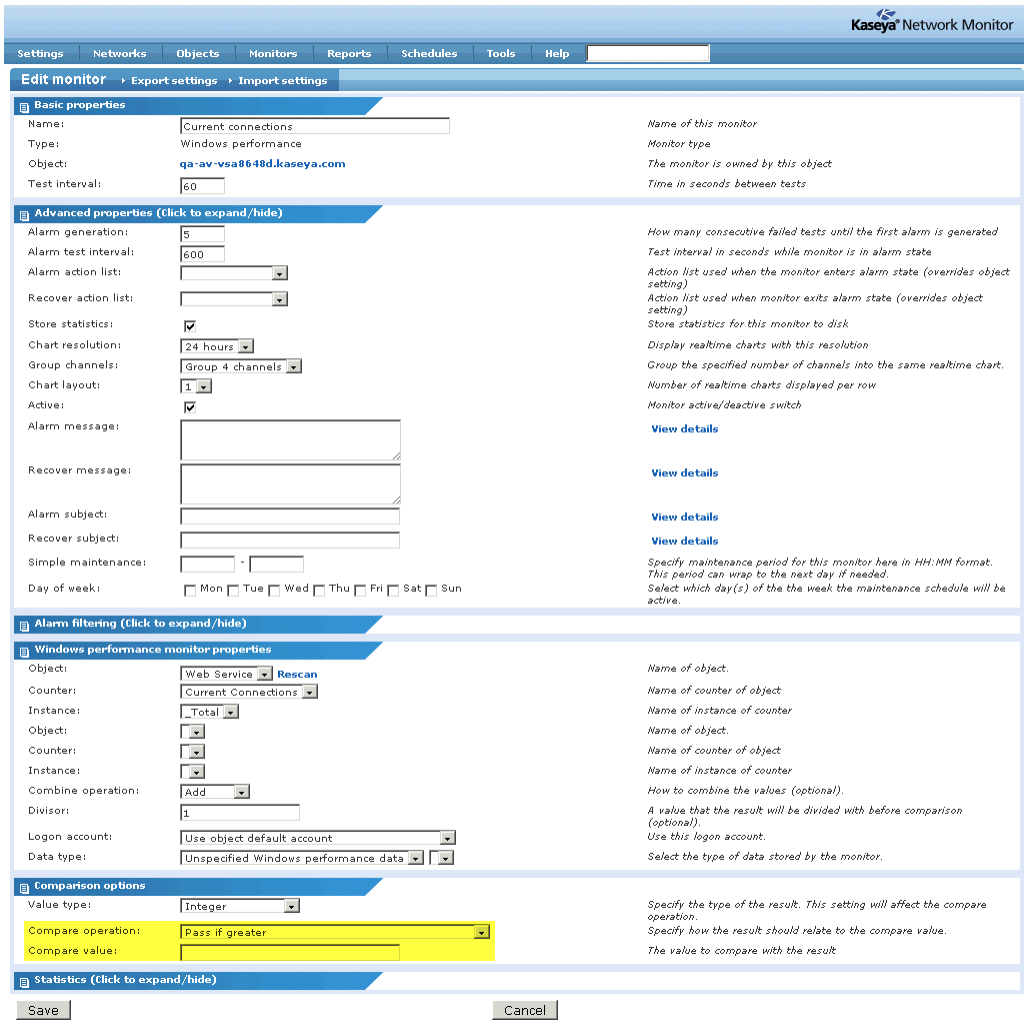



2. Click the name of the object you just added to be monitored. The **Object information** page displays.
   - By default all the monitors configured in the `MS IIS` object template only trigger an alarm if they fail to return any data. This procedure discusses how to add an alarm threshold to a monitor.
   - First, *you will need to unlink the monitor from its object template.* That's because the properties of linked monitors are always determined by the properties assigned the object template. Linking enables you to configure a single monitor in an object template and have the change reflected in all the monitors linked to that object template.
   - Because this is a "first time" configuration demonstration, changing the configuration of a standard object template is not recommended. *The rest of this document assumes the monitor is unlinked from the object template.*
3. Check the checkbox next to the phrase `Current connections`. Then click the **Unlink** option. After you select this option the chainlink icon for `Current connections` changes to a pencil icon.




4. Click `Current connections` to display the **Monitor information** page.
5. Identify the typical value for the **current connection counter** for this object by looking at the chart.
   - *If you just added the new monitor, the monitor may not have returned any data yet.*
6. Click **Properties** in the **Monitor information** section menu.

- The **Edit monitor** page displays.



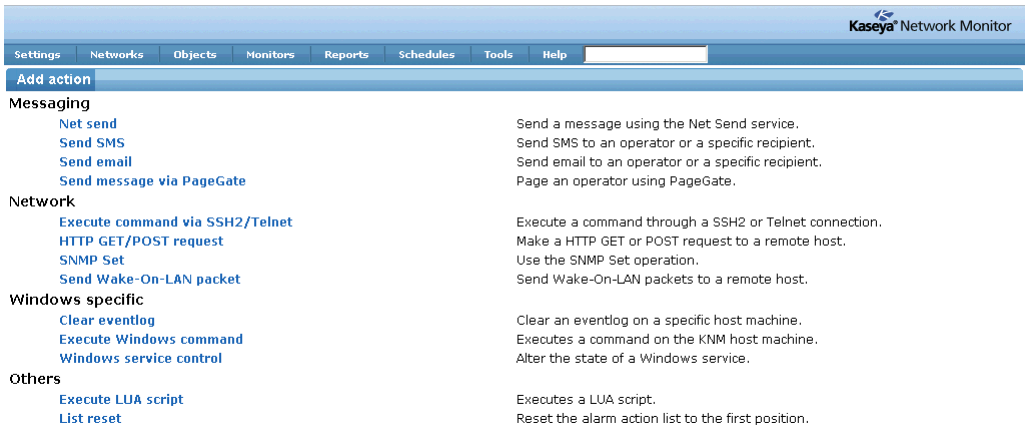

7. In the **Comparison options > Compare operation** field, select `Pass if greater`.
8. In the **Comparison options > Compare value**, enter a value *less* than the typical **current connection counter** you identified in step 5 above.
9. Expand the **Advanced properties** section by clicking **Click to expand/hide**, if it is not already expanded.
   - The **Alarm generation** value specifies the minimum number of *consecutive* "tests" that must fail to generate an alarm.
   - The **Test interval** value in the **Basic Properties** section shows how much time must elapse between tests *before the first alarm is generated*.
   - The **Alarm test interval** value in the **Advance properties** section 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.
10. Leave the **Alarm action list** field blank so that it defaults to the alarm action list specified for the object.
11. Click **Save** to save your changes to this monitor.
    - The **Monitor Information** page displays.
    - Now that a threshold exists for this monitor, it should show as a red line on the chart.

- The first time the monitor fails a test it will display a warning icon.
- The icon will change to an alarm icon when it enters its first alarm state.
- The monitor will remain in its alarm state until any *one* of the following occurs:
  - ✓ The test no longer fails, at least once, in continuing series of consecutive tests.
  - ✓ The alarm is acknowledged by an operator (**Network Monitor** administrator). An acknowledged alarm means an operator knows about it and is acting to correct it.
  - ✓ The monitor properties page is edited.

# Configuring Alarm Action Lists

In this procedure you create a new alarm action list. An alarm action list determines the automated response to an alarm count, either by object or by monitor. Then you link it to the new monitor you created in an earlier procedure.

1. Select Settings > **Alarm lists**.
   - The **Action list info** page displays.
2. Click **New action list**.
   - The **Edit action list** page displays.
3. Enter the following parameters.
   - **Name**
   - **Description**
   - **Operator Group** - Leave this field blank, so that it can be assigned to any object or monitor.
4. Click **Save** to save your changes.
   - The **Action lists** page displays.
5. Click the name of your new action list in the **Name** column.
   - The **Action list info** page displays for your new action list.
6. Click **Add action** in the **Actions** section of this page.
   - The **Add action** page displays.




7. Click the **Send email** option.
   - The **Edit action** page display for **Send email**.
8. Enter a value of 2 in the **Alarm number** field.
   - This is the *alarm count* number. An alarm count value of 2 means this action will occur in response to a *second alarm*, if the alarm action list you are editing is associated with a monitor or object.

- You can associate different actions with different alarm counts using this field.

9. Click the **Specific recipient** radio option and enter in your email address.
   - This ensures your new action list will only send email to you, rather than any other recipients.
   - Alternatively, you could send email to all operators on duty, an operator group assigned to the object, the operator group manager, or a different operator group.
10. Expand the **Test Action Configuration** section of this page.
    - Select the object you added earlier and the `Current connections` monitor.
11. Click **Test Action**.
    - Check your email inbox for the test email that was sent to you.
12. Re-display the **Monitor Information** page for `Current connections`.

You can re-display this page by clicking Objects > List > <objectname> > Monitor List > `Current connections`.

1. Click **Properties** at the top of the page.
   - The **Edit monitor** page displays.
2. Expand the **Advanced properties** section by clicking **Click to expand/hide**, if it is not already expanded.
3. In the **Alarm action list** field, select the name of the new alarm action list you just created.
   - Selecting this value overrides the default alarm action list specified for the object.
4. Click **Save** to save your changes to this monitor.
   - The **Monitor Information** page displays.
5. The email notification action you created will be triggered the next time an alarm count of `2` occurs for this monitor. *The alarm count is reset to zero any time you edit the properties of a monitor.*

# Index