Kaseya 2

Syslog 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.

Syslog Monitor

This quick start guide demonstrates how to configure *syslog monitoring* 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.

The syslog monitor constantly reviews the syslog messages sent to **Network Monitor** by a syslog host. Based on the type of syslog message and the message text, the system monitor can trigger an alarm and send an email notification. More than one syslog monitor can be added to each object to receive different combinations of messages. Before you create a monitor of this type, you need to start the internal syslog server. If another syslog service is executing on the system hosting **Network Monitor** the result is unpredictable.

> **Note: A host device or machine must be configured to direct syslog messages remotely to the system hosting your instance of Network Monitor. Network Monitor** detects UDP syslog messages that are either broadcast to the entire subnet or directed specifically to the **Network Monitor** syslog server using port 514. Configuration of each machine and device is unique and outside the scope of this documentation.

How This Quick Start Guide is Organized

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

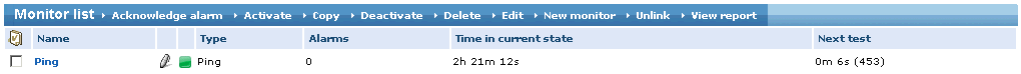
- Any state other than deactivated is an activated state.
- An activated monitor tests its object.
- Deactivating any or all monitors of an object does not deactivate the object.
- Deactivating any or all objects of a network does not deactivate their parent network.
- Deactivating an object deactivates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

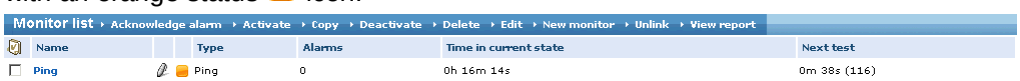
Monitor status progression

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.



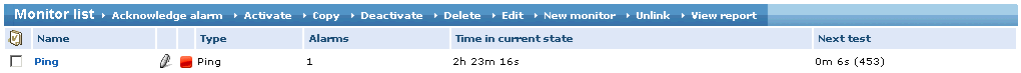
A monitor during normal operation is displayed with a green status icon.

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.

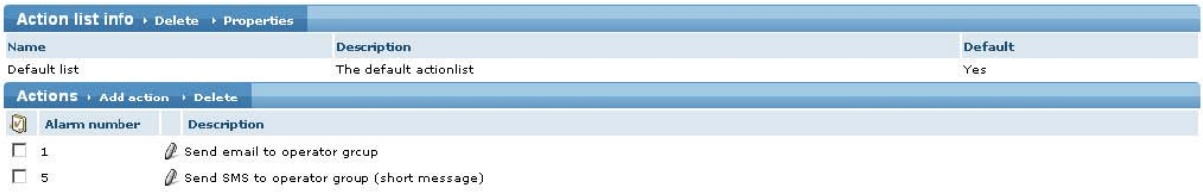


A monitor in alarm state is displayed with a red status icon.

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.

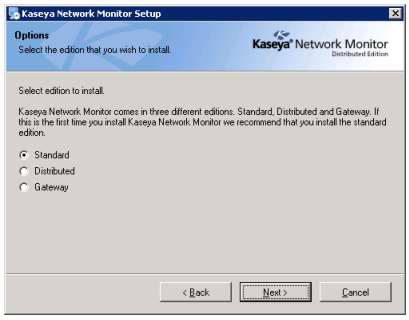
When completed you are ready to install **Network Monitor**. After installing **Network Monitor** and connecting to the web interface for the first time, consult the topic **Running the Startup Guide** *(page 6)*.

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.

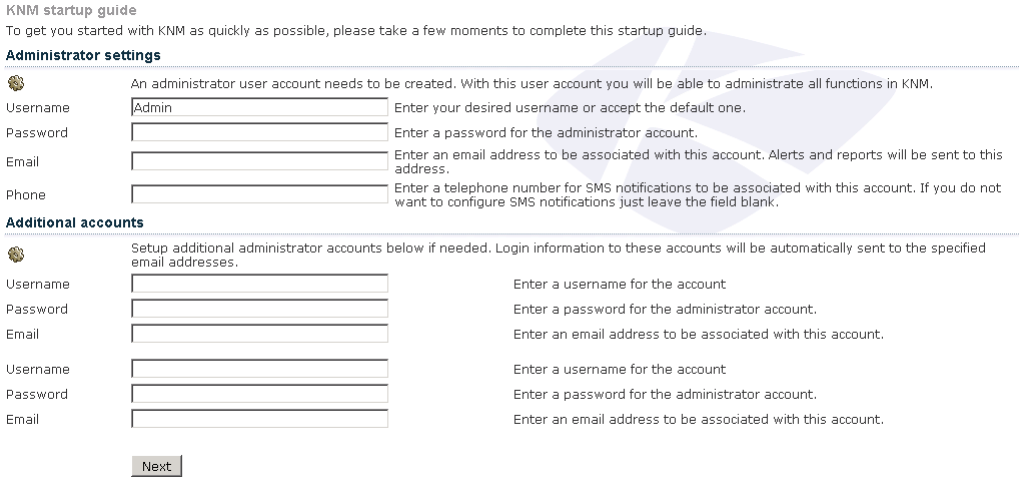
Running the Startup Guide

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

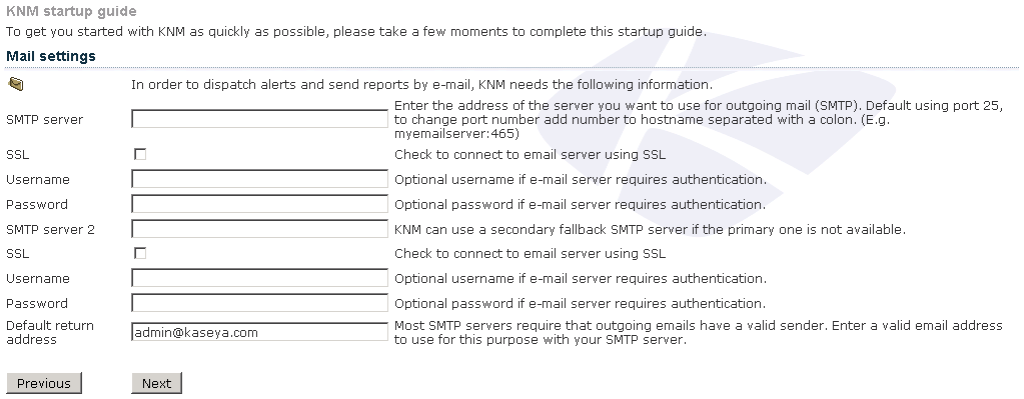
> **Note:** A person logging into the **Network Monitor** server is referred to as an *operator*. Each operator can only have one logon *session* open at one time.

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**.

Mail settings



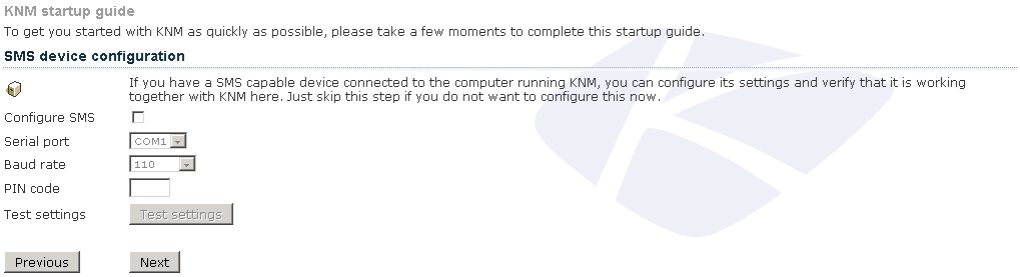
To send email notifications and reports you need to configure the email server settings. Two email servers can be configured: a primary server and a secondary backup server used in case the primary server is unreachable.

- **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

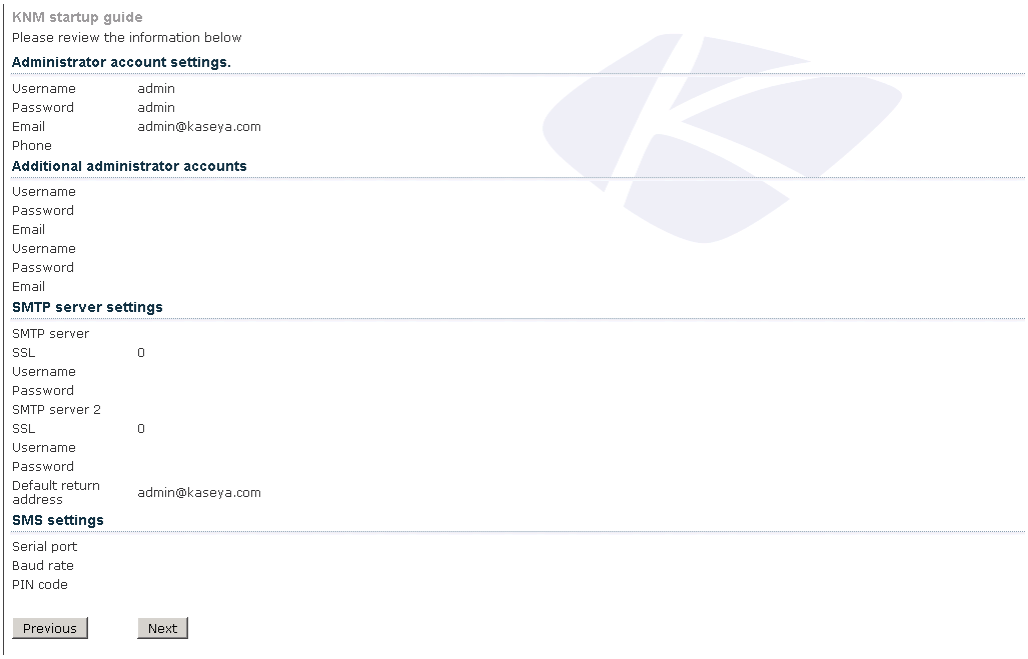
If you did not enter a phone number on the first step in the startup guide you can enter it in the My settings page, without the phone number. **Network Monitor** is unable to send the operator an SMS notification. You are able to access the **My settings** page when you logon after the startup guide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

The following procedures provide a step-by-step, "first time" demonstration of how to configure a *Syslog 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.

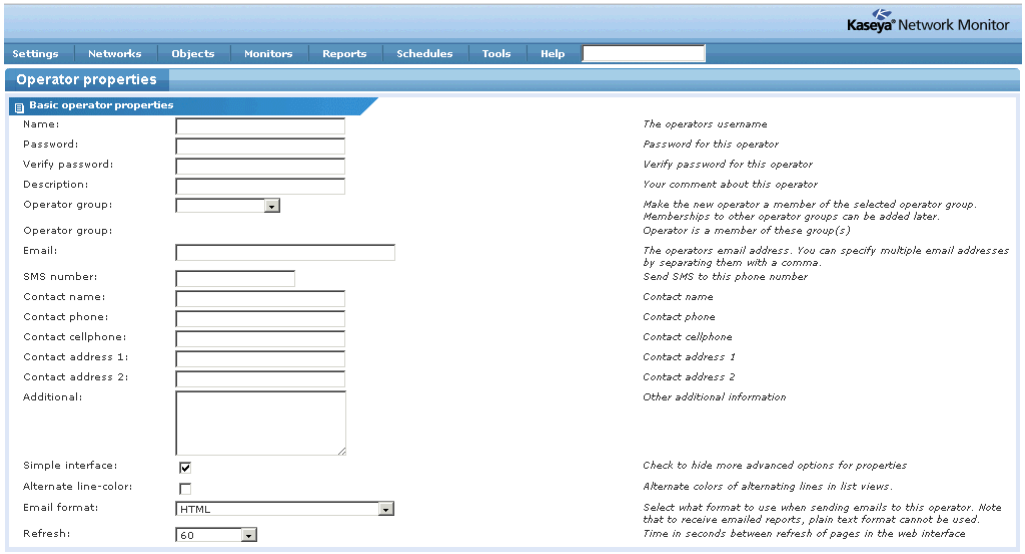
Each operator can be a member of one or more *operator groups* and must be a member of at least one. Each object in **Network Monitor** always belongs to one operator group. In this way, an operator group in **Network Monitor** can be thought of as being in charge of an object. Normally, alerts for a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



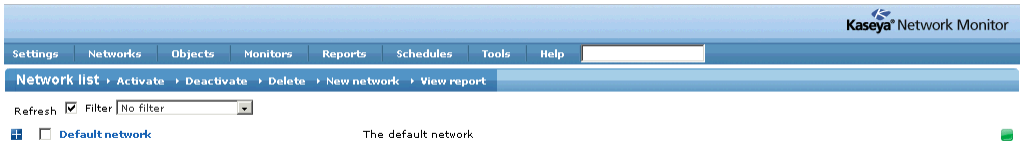
3. Enter values for the following fields.
   - **Name**
   - **Password**
   - **Verify password**
   - **Operator group** - Select `Administrators`. You can select a different operator group later.
   - **Email** - Enter your email address.
4. Click **System administrator** button. This will auto-populate 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.

Preparing Network Monitor for Syslog Monitoring

The following preparatory steps should be performed before selecting a particular object for syslog monitoring using **Network Monitor**.

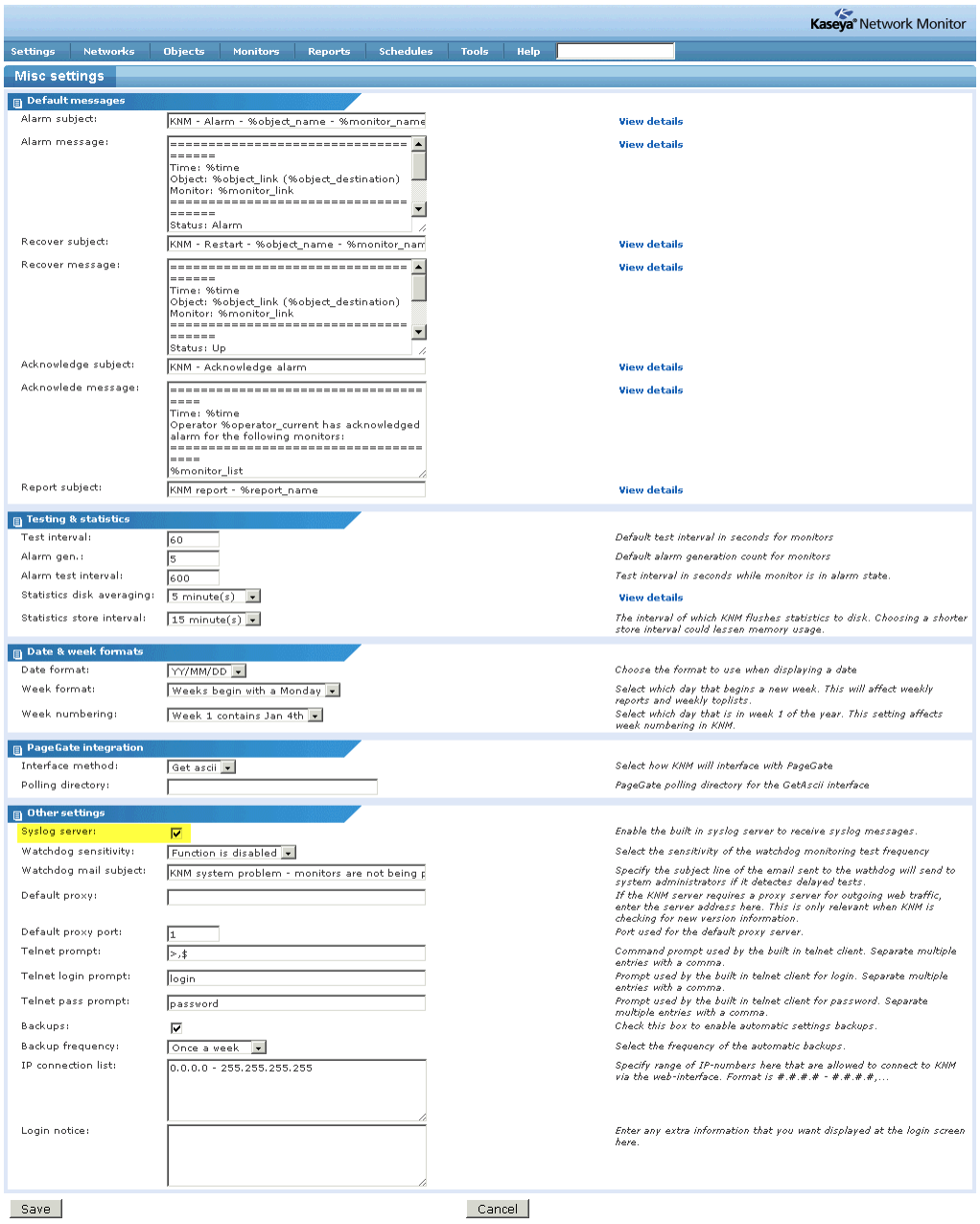
1. **A host device or machine must be configured to direct syslog messages remotely to the system hosting your instance of Network Monitor. Network Monitor** detects UDP syslog messages that are either broadcast to the entire subnet or directed specifically to the **Network Monitor** syslog server using port 514. Configuration of each machine and device is unique and outside the scope of this documentation.
2. Enable the syslog server in **Network Monitor**. This step is detailed below.
3. Confirm syslog messages are being *received* by **Network Monitor**. This step is detailed below.

Note: On the Settings > Program settings > **Log settings** page are syslog options for creating **Network Monitor** syslog messages and *sending* them to an syslog server. You do not need to enable these options. They only apply if you want to create syslog messages for the **Network Monitor** server itself.

Enabling the Syslog Server in Network Monitor

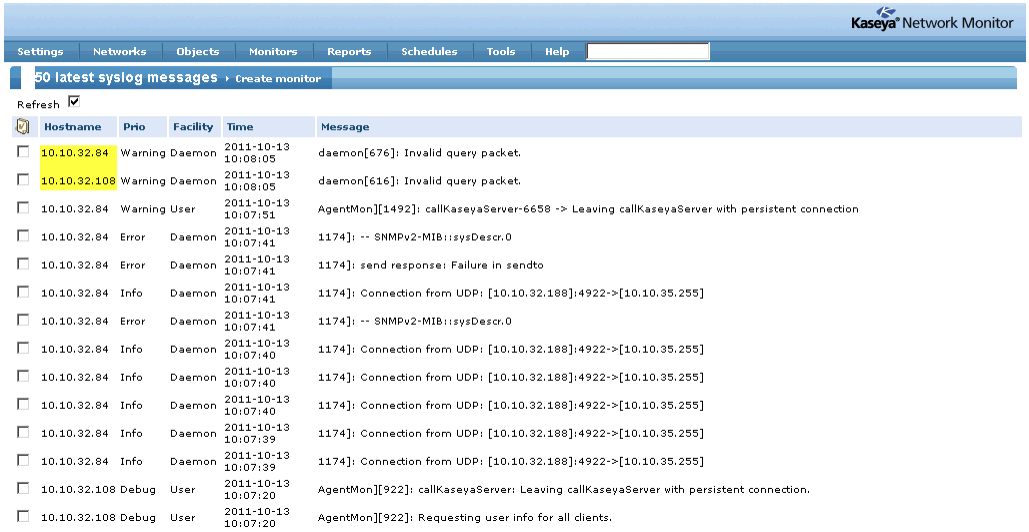
1. Select Settings > Program settings > **Misc settings**.

2. Check the **Syslog server** checkbox and click the **Save** button.



Confirm Syslog Messages are Being Received by Network Monitor

1. Select Tools > SNMP / Syslog > **Syslog messages**. The **50 latest yslog messages** received by **Network Monitor** display on this page.



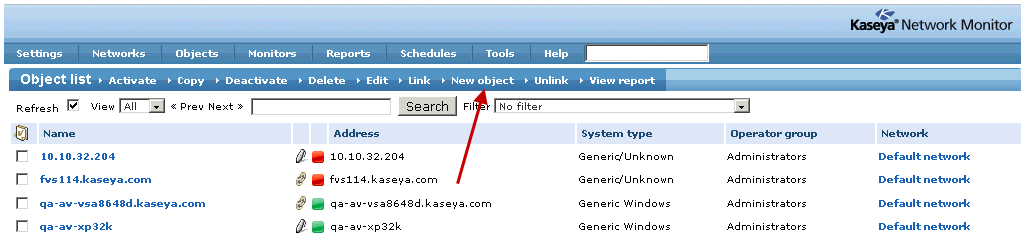
- In the image above you can see an example of two different IP addresses directing syslog messages to **Network Monitor**.
- *No objects or monitors are yet configured.* This page simply confirms that syslog messages being sent by devices and machines are being received by the syslog server you just enabled in **Network Monitor**.

> **Note:** If you're not seeing syslog messages display here for a computer or device you want to monitor, you'll have to return to the computer or device and configure it to direct syslog messages remotely to your instance of **Network Monitor**. *Do not continue performing the instructions in this quick start guide until syslog messages display on this page as expected.*

Adding Objects Manually

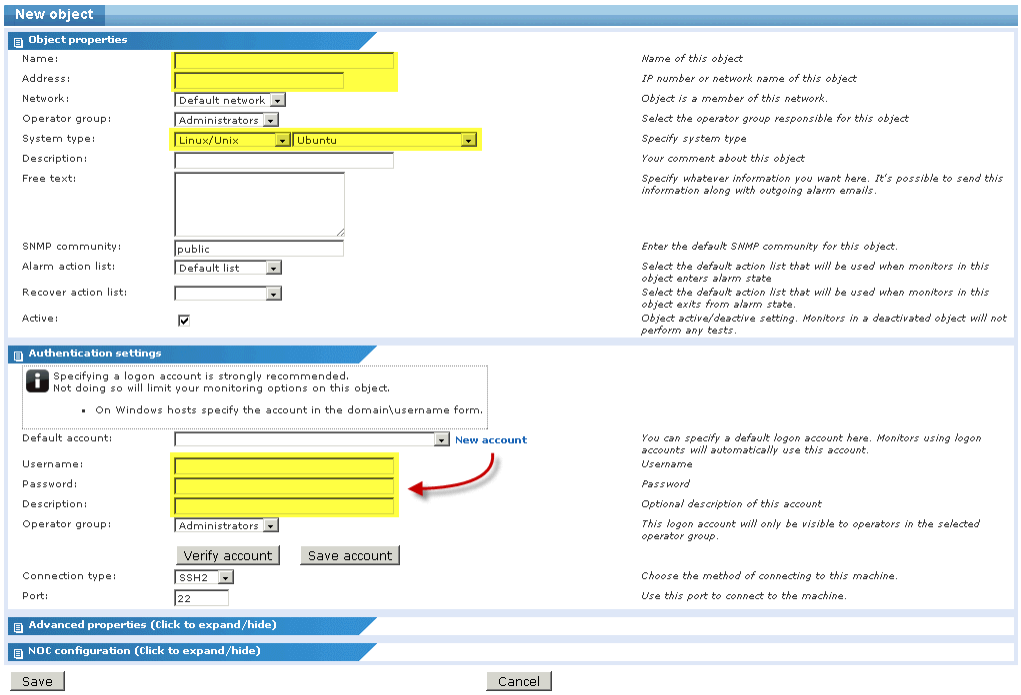
Since you've already used Tools > SNMP / Syslog > **Syslog messages** to identify the IP address of a computer or device that is sending **Network Monitor** syslog messages, you don't have to use **Network discovery**. Instead, this procedure describes how to add the object manually.

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



2. Enter the **Name** of the object. This does not have to be the same as the host name of the computer or device, but it often is the same.
3. Enter the IP **Address** of the computer or device.

4. Select the **System type** that best describes the computer or device you have selected and configured to send syslog messages remotely to your instance if **Network Monitor**. In this example Linux/Ubuntu is shown as selected, but it is only an example.



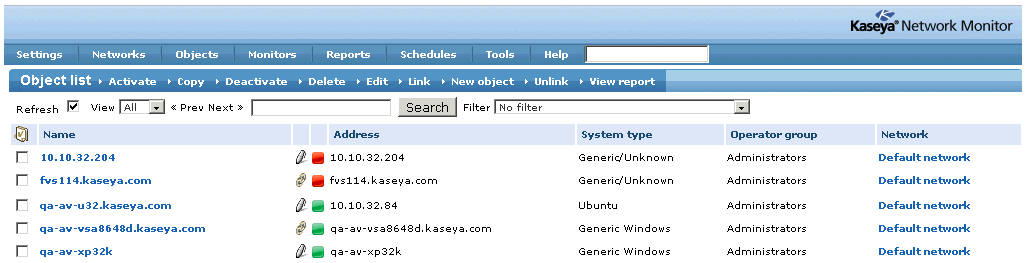
   - Accept the `Default network` **Network**.
   - Accept the default **Operator Group** (**Network Monitor** user group) to assign the object.
   - Accept the default **Alarm action list** to assign the object. An alarm action list determines the actions that occur in response to an alarm condition.
   - *Leave the* **Recover action list** *blank for now.*
   - A logon credential is not necessarily required for syslog monitoring, but even if is not, entering one, if possible, is strongly recommended. You may wish to add additional monitors that do require a credential later on for this same object.
5. Enter **Authentication settings** if possible. 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.
6. Click **Save** to complete the configuration of the object.

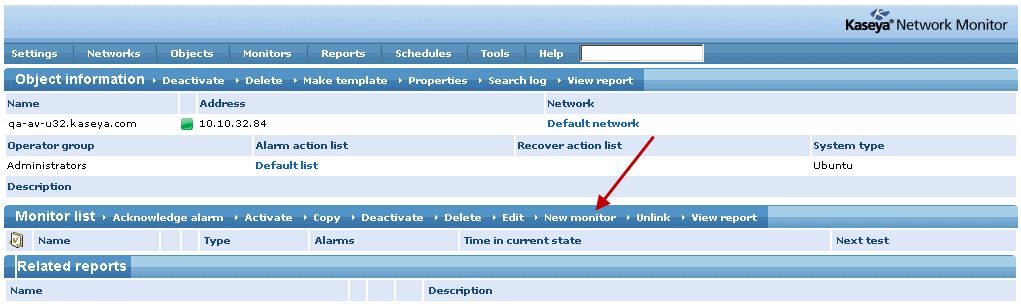
Adding a Syslog Monitor

In this procedure you assign a `Syslog` monitor to the new object you just added.

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

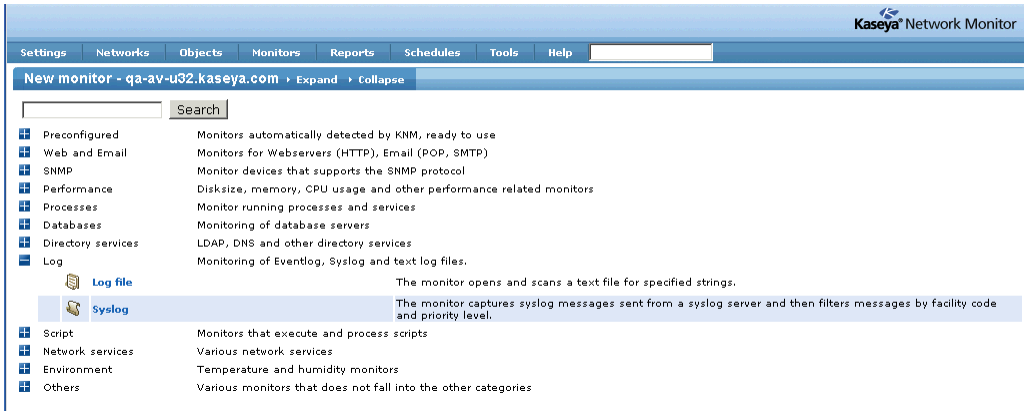


2. Click the name of the object you just added.



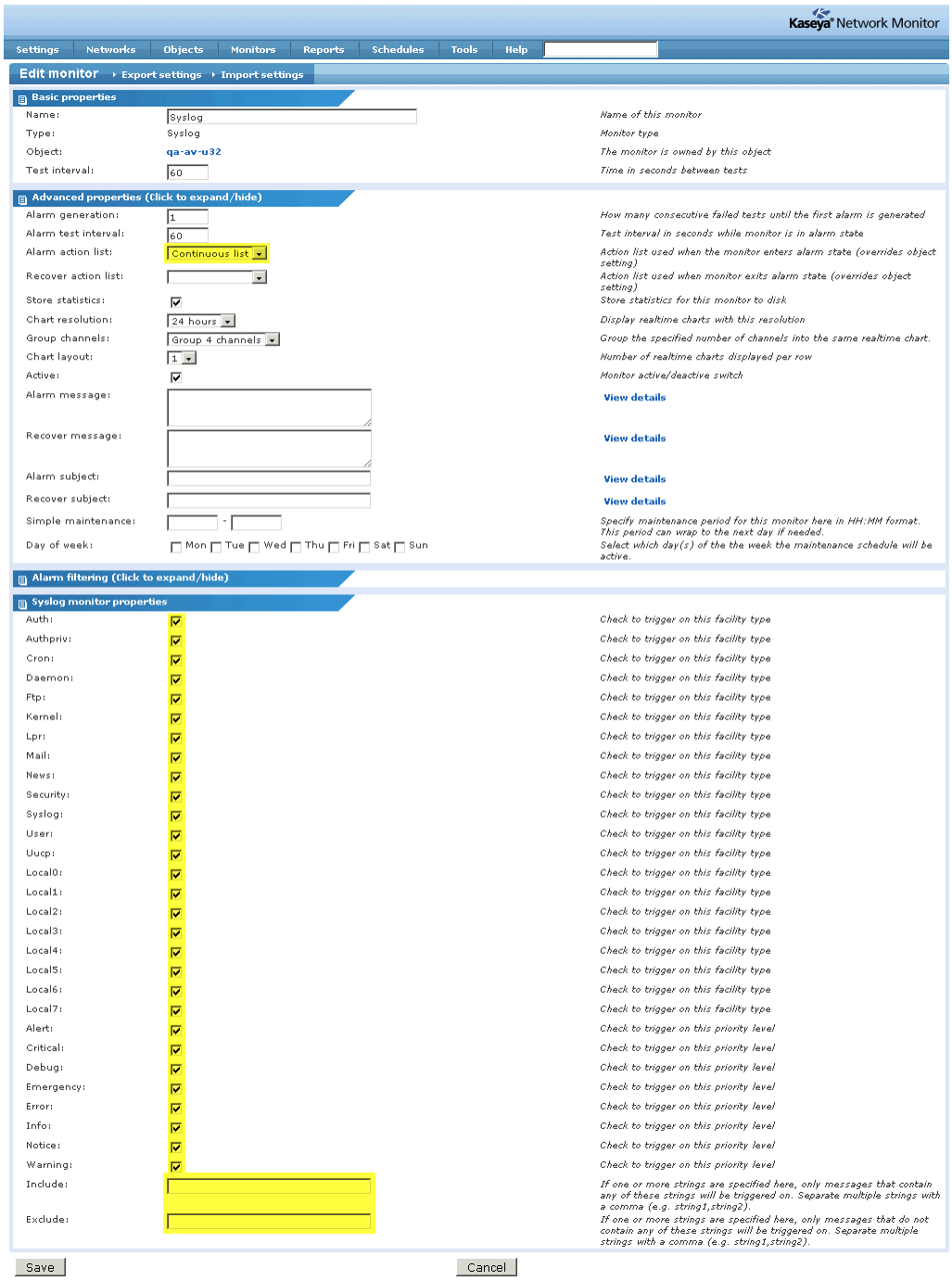
   - The **Name**, **Address** and **Network** displays in the **Object information** section at the top of the page.
   - This object was added manually so there are no monitors yet assigned to the object.

3. Click the **New monitor** option in the **Monitor list** section menu.
4. Select the Log > **Syslog** monitor in the monitor tree.



   - The **Edit Monitor** page displays automatically.

5. Set options in the **Syslog monitor** properties section of the **Edit monitor** page.



- **A syslog message only displays in the Status column if it triggers an alarm.** Select `Continuous list` in the **Alarm action list** drop-down list. This ensures that the alarm state for the syslog monitor is always reset back to a green status *Ok* state, after each syslog message triggers an alarm. Without the reset, each new syslog message that matched the criteria you set would be ignored, for as long as the monitor was in the red status *Alarm* state.
- All syslog messages are classified by *facility* and *priority*. You must check at least one *facility* and at least one *priority* to trigger any alarm at all, and it will only be for the combination you select. Check them all to trigger an alarm for every combination.

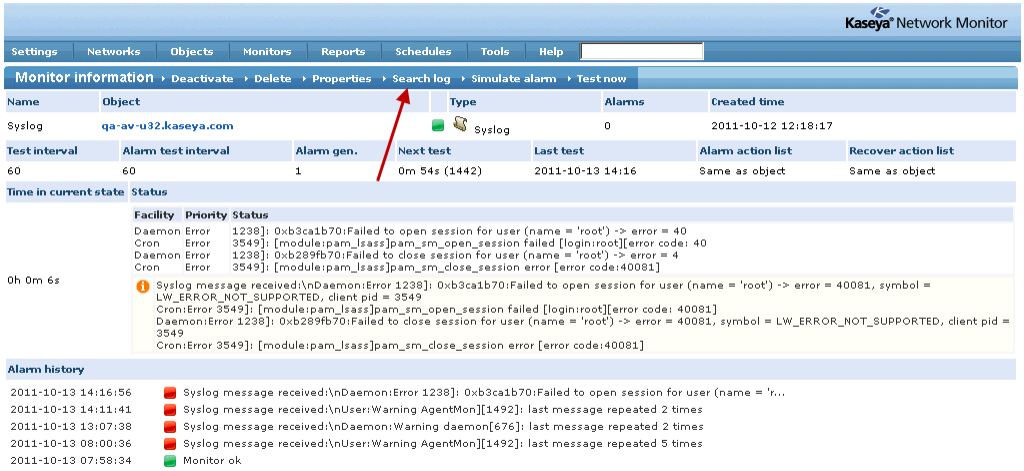
- You can filter the alarms triggered further by entering text strings in the **Include** and **Exclude** fields. This is the text that appears in the body of syslog message.
- You can also create multiple syslog monitors for the same object and set them to match different criteria.

6. Click **Save** to save your selections.
   - The **Monitor information** page displays.
   - *If you just added the monitor, the monitor may not have returned any matching data yet.*

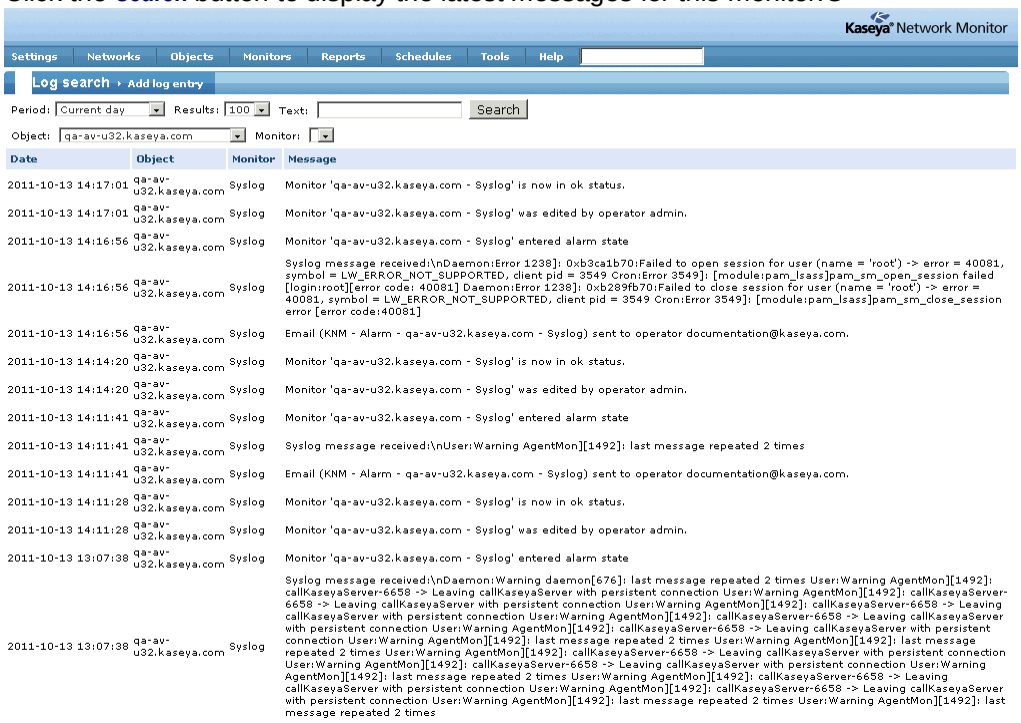
Viewing the Syslog Monitor Log

The `Syslog` monitor only provides you the latest syslog messages you have received. Use this procedure to view the entire history of syslog messages that match the conditions you specified for a single object.

1. Re-display the **Monitor information** page for `Syslog`, if it is not already displayed.
   - You can re-display this page by clicking Objects > List > <objectname> > Monitor List > `Syslog`.
2. Click the **Search log** option on the **Monitor information** section menu, for the `Syslog` monitor you just configured.



3. Click the **Search** button to display the latest messages for this monitor.O



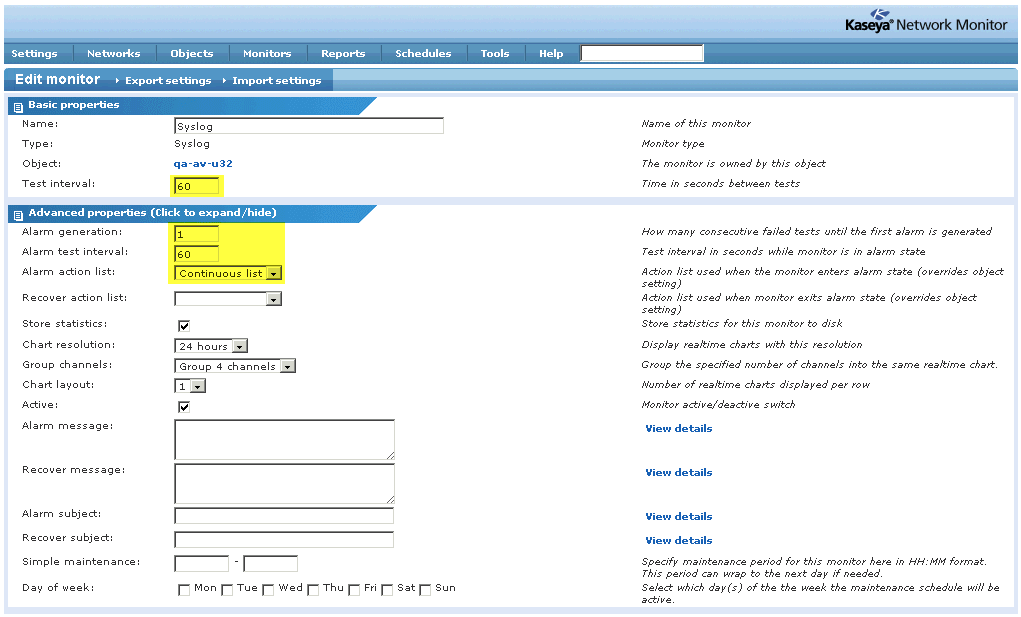
- The **Log search** page shows log entries any time a monitor enters a different alarm state as well as the syslog message itself.
- You can immediately display log entries for other *monitors*—or all monitors for the selected object—by selecting a different item in the **Monitor** drop-down list at the top of the page and clicking **Search** again.
- You can immediately display log entries for other *objects*—or all objects—by selecting a different item in the **Object** drop-down list at the top of the page and clicking **Search** again.

Viewing Alarm Configuration

In this section you view the default alarm settings for a `Syslog` monitor. You'll see that the monitor is configured to trigger an alarm immediately, the first time an alarm condition is encountered. In contrast, other types of monitors perform repeated tests before triggering an alarm.

1. Re-display the **Monitor Information** page for `Syslog`, if it is not already displayed.
   - You can re-display this page by clicking Objects > List > <objectname> > Monitor List > `Syslog`.
2. Click **Properties** in the **Monitor information** section menu.

- The **Edit monitor** page displays.



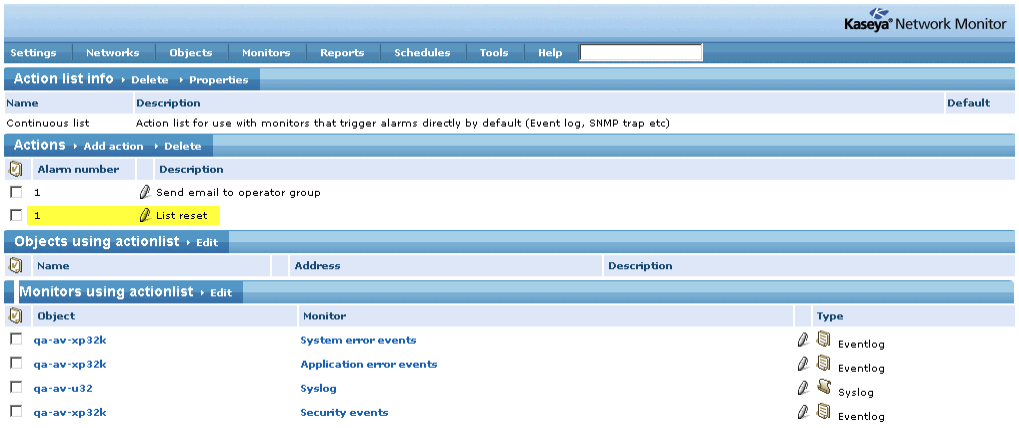
3. Expand the **Advanced properties** section by clicking **Click to expand/hide**, if it is not already expanded.
   - The **Alarm generation** value specifies the minimum number of *consecutive* "tests" that must fail to generate an alarm. In this case the value is 1, meaning it only takes one occurrence to trigger an alarm. In contrast, other monitors often have this value set to 5, meaning it takes five occurrences before an alarm is triggered.
   - 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*. In this case, the setting is irrelevant because there is only one test before the alarm is generated. In other monitors this interval is usually much longer then the **Test interval**, to give you time to respond to the original alarm.
4. Ensure the **Alarm action list** is set to `Continuous list`, which was selected when **Adding a Syslog Monitor** *(page 15)*.
5. Click **Save** if you made any changes to this monitor.
   - The **Monitor Information** page displays.
   - The first time the monitor fails a test it will display an alarm icon.
   - The `Continuous list` action list ensures that the alarm is immediately reset back to a green status *Ok* state.

Viewing Alarm Action Lists

In this procedure you view the `Continuous list` alarm action list to see how it is constructed. You already selected it for your syslog monitor when **Adding a Syslog Monitor** *(page 15)*. An alarm action list determines the automated response to an alarm count.

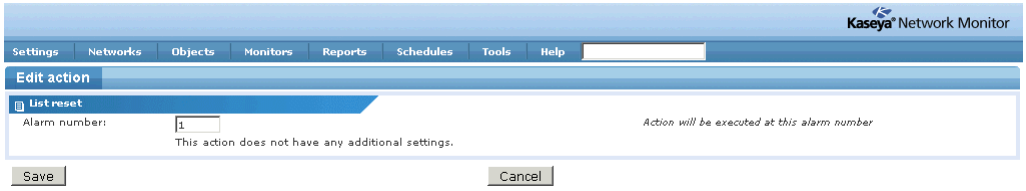
1. Select Settings > **Alarm lists**. The **Action lists** page displays.

2. Click the `Continuous list` action list. The **Action list info** page displays.



   - The last action in the `Continuous list` action list is `List reset`.

3. Click the pencil icon next to `List reset`, as though you were going to edit this action.



   - You can see there is only one value you can change. It tells you that a monitor will be reset back to a green status *Ok* state when a monitor's alarm state reaches the value specified.

Warning: Don't change this value! It affects other monitors that use it in **Network Monitor**.

   - Since 1 is always the first value of any monitor's alarm state, the monitor will be reset as soon as the alarm is triggered.
   - The `Continuous list` is typically used with a monitor that triggers an alarm each time it occurs, instead of undergoing repeated tests. Examples include event logs, SNMP traps and syslog messages.
   - Without the reset, each new event that matched the alarm criteria you set would be ignored, for as long as the monitor was in the red status *Alarm* state.

4. Click **Cancel** to close this window.

Index