



## Alerts

### SANtricity software

NetApp  
March 17, 2026

# Table of Contents

- Alerts ..... 1
  - Learn about alerts in SANtricity System Manager ..... 1
    - What are alerts? ..... 1
    - How do I configure alerts? ..... 1
    - Related information ..... 1
- Concepts ..... 1
  - How alerts work in SANtricity System Manager ..... 1
  - Learn about alerts terminology in SANtricity software ..... 2
- Manage email alerts ..... 3
  - Configure mail server and alert recipients in SANtricity System Manager ..... 3
  - Edit email addresses for alerts in SANtricity System Manager ..... 4
  - Add email addresses for alerts in SANtricity System Manager ..... 5
  - Delete mail server or email addresses for alerts in SANtricity System Manager ..... 5
  - Edit mail server for alerts in SANtricity System Manager ..... 6
- Manage SNMP alerts ..... 6
  - Configure SNMP alerts in SANtricity System Manager ..... 6
  - Add trap destinations for SNMP alerts in SANtricity System Manager ..... 8
  - Configure SNMP MIB variables in SANtricity System Manager ..... 9
  - Edit communities for SNMPv2c traps in SANtricity System Manager ..... 10
  - Edit user settings for SNMPv3 traps in SANtricity System Manager ..... 10
  - Add communities for SNMPv2c traps in SANtricity System Manager ..... 11
  - Add users for SNMPv3 traps in SANtricity System Manager ..... 11
  - Remove communities for SNMPv2c traps in SANtricity System Manager ..... 12
  - Remove users for SNMPv3 traps in SANtricity System Manager ..... 12
  - Delete trap destinations in SANtricity System Manager ..... 13
- Manage syslog alerts ..... 13
  - Configure syslog server for alerts in SANtricity System Manager ..... 13
  - Edit syslog servers for alerts in SANtricity System Manager ..... 14
  - Add syslog servers for alerts in SANtricity System Manager ..... 14
  - Delete syslog servers for alerts in SANtricity System Manager ..... 15
- Storage system alerts FAQ for SANtricity System Manager ..... 15
  - What if alerts are disabled? ..... 15
  - How do I configure SNMP or syslog alerts? ..... 15
  - Why are timestamps inconsistent between the array and alerts? ..... 16

# Alerts

## Learn about alerts in SANtricity System Manager

You can configure SANtricity System Manager to send storage array alerts by email, SNMP traps, and syslog messages.

### What are alerts?

*Alerts* notify administrators about important events that occur on the storage array. Events can include such issues as a battery failure, a component moving from Optimal to Offline, or redundancy errors in the controller. All Critical events are considered "alertable," along with some Warning and Informational events.

Learn more:

- [How alerts work](#)
- [Alerts terminology](#)

### How do I configure alerts?

You can configure alerts to be sent as a message to one or more email addresses, as an SNMP trap to an SNMP server, or as a message to a syslog server. Alert configuration is available from **Settings > Alerts**.

Learn more:

- [Configure mail server and recipients for alerts](#)
- [Configure syslog server for alerts](#)
- [Configure SNMP alerts](#)

### Related information

Learn more about concepts related to alerts:

- [Event log overview](#)
- [Inconsistent time stamps](#)

## Concepts

### How alerts work in SANtricity System Manager

Alerts notify administrators about important events that occur on the storage array. Alerts can be sent through email, SNMP traps, and syslog.

The alerts process works as follows:

1. An administrator configures one or more of the following alerting methods in System Manager:
  - **Email** — Messages are sent to email addresses.
  - **SNMP** — SNMP traps are sent to an SNMP server.

- **Syslog** — Messages are sent to a syslog server.
2. When the storage array's event monitor detects an issue, it writes information about that issue to the event log (available from **Support > Event Log**). For example, issues can include such events as a battery failure, a component moving from Optimal to Offline, or redundancy errors in the controller.
  3. If the event monitor determines that the event is "alertable," it then sends a notification using the configured alerting methods (email, SNMP, and/or syslog). All Critical events are considered "alertable," along with some Warning and Informational events.

## Alerts configuration

You can configure alerts from the Initial Setup wizard (for email alerts only) or from the Alerts page. To access the Alerts page, go to **Settings > Alerts** from the left panel.

## Alerts information

Alerts can include the following types of information:

- Name of the storage array.
- Event error type related to an event log entry.
- Date and time when the event occurred.
- Brief description of the event.



Syslog alerts follow the RFC 5424 messaging standard.

## Learn about alerts terminology in SANtricity software

Learn how the alerts terms apply to your storage array.

Component	Description
Event monitor	The event monitor resides on the storage array and runs as a background task. When the event monitor detects anomalies on the storage array, it writes information about the issues to the event log. Issues can include such events as a battery failure, a component moving from Optimal to Offline, or redundancy errors in the controller. If the event monitor determines that the event is "alertable," it then sends a notification using the configured alerting methods (email, SNMP, and/or syslog). All Critical events are considered "alertable," along with some Warning and Informational events.
Mail server	The mail server is used for sending and receiving email alerts. The server uses Simple Mail Transfer Protocol (SMTP).
SNMP	Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for managing and sharing information between devices on IP networks.
SNMP trap	An SNMP trap is a notification sent to an SNMP server. The trap contains information about significant issues with the storage array.

Component	Description
SNMP trap destination	An SNMP trap destination is an IPv4 or IPv6 address of the server running an SNMP service.
Community name	A community name is a string that acts like a password for the network server(s) in a SNMP environment.
MIB file	The management information base (MIB) file defines the data being monitored and managed in the storage array. It must be copied and compiled on the server with the SNMP service application. This MIB file is available with the System Manager software on the Support site.
MIB variables	Management Information Base (MIB) variables can return values such as the storage array name, array location, and a contact person in response to SNMP GetRequests.
Syslog	Syslog is a protocol used by network devices for sending event messages to a logging server.
UDP	User Datagram Protocol (UDP) is a transport layer protocol that specifies a source and destination port number in their packet headers.

## Manage email alerts

### Configure mail server and alert recipients in SANtricity System Manager

To configure email alerts, you must specify a mail server address and the email addresses of the alert recipients. Up to 20 email addresses are allowed.

#### Before you begin

- The address of the mail server must be available. The address can be an IPv4 or IPv6 address, or a fully qualified domain name.



To use a fully qualified domain name, you must configure a DNS server on both controllers. You can configure a DNS server from the Hardware page.

- Email address to be used as the alert sender must be available. This is the address that appears in the "From" field of the alert message. A sender address is required in the SMTP protocol; without it, an error results.
- Email address(es) of the alert recipient(s) must be available. The recipient is typically an address for a network administrator or storage administrator. You can enter up to 20 email addresses.

#### About this task

This task describes how to configure the mail server, enter email addresses for the sender and recipients, and test all the email addresses entered from the Alerts page.



Email alerts can also be configured from the Initial Setup wizard.

## Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **Email** tab.

If an email server is not yet configured, the Email tab displays "Configure Mail Server."

3. Select **Configure Mail Server**.

The Configure Mail Server dialog box opens.

4. Enter the mail server information, and then click **Save**.

- **Mail server address** — Enter a fully qualified domain name, IPv4 address, or IPv6 address of the mail server.



To use a fully qualified domain name, you must configure a DNS server on both controllers. You can configure a DNS server from the Hardware page.

- **Email sender address** — Enter a valid email address to be used as the sender of the email. This address appears in the "From" field of the email message.
- **Encryption** — If you want to encrypt messages, select either **SMTPS** or **STARTTLS** for the encryption type, and then select the port number for encrypted messages. Otherwise, select **None**.
- **User name and password** — If needed, enter a user name and password for authentication with the outgoing sender and the mail server.
- **Include contact information in email** — To include the sender's contact information with the alert message, select this option, and then enter a name and phone number.

After you click **Save**, the email addresses appear in the Email tab of the Alerts page.

5. Select **Add Emails**.

The Add Emails dialog box opens.

6. Enter one or more email addresses for the alert recipients, and then click **Add**.

The email addresses appear on the Alerts page.

7. If you want to make sure the email addresses are valid, click **Test All Emails** to send test messages to the recipients.

## Results

After you configure email alerts, the event monitor sends email messages to the specified recipients whenever an alertable event occurs.

## Edit email addresses for alerts in SANtricity System Manager

You can change the email addresses of the recipients who receive email alerts.

### Before you begin

The email address you intend to edit must be defined in the Email tab of the Alerts page.

## Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **Email** tab.
3. From the **Email Address** table, select the address you want to change, and then click the **Edit** (pencil) icon on the far right.

The row becomes an editable field.

4. Enter a new address, and then click the **Save** (checkmark) icon.



If you want to cancel changes, select the **Cancel** (X) icon.

## Results

The Email tab of the Alerts page displays the updated email addresses.

## Add email addresses for alerts in SANtricity System Manager

You can add up to 20 recipients for email alerts.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **Email** tab.
3. Select **Add Emails**.

The Add Emails dialog box opens.

4. In the empty field, enter a new email address. If you want to add more than one address, select **Add another email** to open another field.
5. Click **Add**.

## Results

The Email tab of the Alerts page displays the new email addresses.

## Delete mail server or email addresses for alerts in SANtricity System Manager

You can remove the previously defined mail server so that alerts are no longer sent to the email addresses, or you can remove individual email addresses.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **Email** tab.
3. From the table, do one of the following:
  - To remove a mail server so that alerts are no longer sent to the email addresses, select the row for the mail server.
  - To remove an email address so that alerts are no longer sent to this address, select the row for the email address you want to delete. The **Delete** button in the upper right of the table becomes available for selection.

4. Click **Delete**, and confirm the operation.

## Edit mail server for alerts in SANtricity System Manager

You can change the mail server address and email sender address used for email alerts.

### Before you begin

The address of the mail server you are changing must be available. The address can be an IPv4 or IPv6 address, or a fully qualified domain name.



To use a fully qualified domain name, you must configure a DNS server on both controllers. You can configure a DNS server from the Hardware page.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **Email** tab.
3. Select **Configure Mail Server**.

The Configure Mail Server dialog box opens.

4. Edit the mail server address, sender information, and contact information.
  - **Mail server address** — Edit the fully qualified domain name, IPv4 address, or IPv6 address of the mail server.



To use a fully qualified domain name, you must configure a DNS server on both controllers. You can configure a DNS server from the Hardware page.

- **Email sender address** — Edit the email address to be used as the sender of the email. This address appears in the "From" field of the email message.
  - **Include contact information in email** — To edit the sender's contact information, select this option, and then edit the name and phone number.
5. Click **Save**.

## Manage SNMP alerts

### Configure SNMP alerts in SANtricity System Manager

To configure Simple Network Management Protocol (SNMP) alerts, you must identify at least one server where the storage array's event monitor can send SNMP traps. The configuration requires a community name or user name, and an IP address for the server.

### Before you begin

- A network server must be configured with an SNMP service application. You need the network address of this server (either an IPv4 or an IPv6 address), so the event monitor can send trap messages to that address. You can use more than one server (up to 10 servers are allowed).
- The management information base (MIB) file has been copied and compiled on the server with the SNMP service application. This MIB file defines the data being monitored and managed.

If you do not have the MIB file, you can obtain it from the NetApp Support site:

- Go to [NetApp Support](#).
- Click the **Downloads** tab, and then select **Downloads**.
- Click **E-Series SANtricity OS Controller Software**.
- Select **Download Latest Release**.
- Log in.
- Accept the Caution statement and license agreement.
- Scroll down until you see the MIB file for your controller type, and then click the link to download the file.

### About this task

This task describes how to identify the SNMP server for trap destinations, and then test your configuration.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.

On first-time setup, the SNMP tab displays "Configure Communities/Users."

3. Select **Configure Communities/Users**.

The Select SNMP version dialog box opens.

4. Select the SNMP version for the alerts, either **SNMPv2c** or **SNMPv3**.

Depending on your selection, the Configure Communities dialog box or the Configure SNMPv3 Users dialog box opens.

5. Follow the appropriate instructions for SNMPv2c (communities) or SNMPv3 (users):
  - **SNMPv2c (communities)** — In the Configure Communities dialog, enter one or more community strings for the network servers. A community name is a string that identifies a known set of management stations, and is typically created by a network administrator. It consists of only printable ASCII characters. You can add up to 256 communities. When you are done, click **Save**.
  - **SNMPv3 (users)** — In the Configure SNMPv3 Users dialog, click **Add**, and then enter the following information:
    - **User name** — Enter a name to identify the user, which can be up to 31 characters long.
    - **Engine ID** — Select the Engine ID, which is used to generate authentication and encryption keys for messages, and must be unique on the administrative domain. In most cases, you should select **Local**. If you have a non-standard configuration, select **Custom**; another field appears where you must enter the authoritative engine ID as a hexadecimal string, with an even number of characters between 10 and 32 characters long.
    - **Authentication credentials** — Select an authentication protocol, which ensures the identity of users. Next, enter an authentication password, which is required when the authentication protocol is set or changed. The password must be between 8 and 128 characters long.
    - **Privacy credentials** — Select a privacy protocol, which is used to encrypt the contents of messages. Next, enter a privacy password, which is required when the privacy protocol is set or changed. The password must be between 8 and 128 characters long. When you are done, click **Add**, and then click **Close**.

6. From the Alerts page with the SNMP tab selected, click **Add Trap Destinations**.

The Add Trap Destinations dialog box opens.

7. Enter one or more trap destinations, select their associated community names or user names, and then click **Add**.
- **Trap Destination** — Enter an IPv4 or IPv6 address of the server running an SNMP service.
  - **Community name or User name** — From the drop-down, select the community name (SNMPv2c) or user name (SNMPv3) for this trap destination. (If you defined only one, the name already appears in this field.)
  - **Send Authentication Failure Trap** — Select this option (the checkbox) if you want to alert the trap destination whenever an SNMP request is rejected because of an unrecognized community name or user name. After you click **Add**, the trap destinations and associated names appear in the **SNMP** tab of the **Alerts** page.
8. To make sure a trap is valid, select a trap destination from the table, and then click **Test Trap Destination** to send a test trap to the configured address.

## Results

The event monitor sends SNMP traps to the server(s) whenever an alertable event occurs.

## Add trap destinations for SNMP alerts in SANtricity System Manager

You can add up to 10 servers for sending SNMP traps.

### Before you begin

- The network server you want to add must be configured with an SNMP service application. You need the network address of this server (either an IPv4 or an IPv6 address), so the event monitor can send trap messages to that address. You can use more than one server (up to 10 servers are allowed).
- The management information base (MIB) file has been copied and compiled on the server with the SNMP service application. This MIB file defines the data being monitored and managed.

If you do not have the MIB file, you can obtain it from the NetApp Support site:

- Go to [NetApp Support](#).
- Click **Downloads**, and then select **Downloads**.
- Click **E-Series SANtricity OS Controller Software**.
- Select **Download Latest Release**.
- Log in.
- Accept the Caution statement and license agreement.
- Scroll down until you see the MIB file for your controller type, and then click the link to download the file.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.

The currently defined trap destinations appear in the table.

### 3. Select **Add Trap Destinations**.

The Add Trap Destinations dialog box opens.

4. Enter one or more trap destinations, select their associated community names or user names, and then click **Add**.
  - **Trap Destination** — Enter an IPv4 or IPv6 address of the server running an SNMP service.
  - **Community name or User name** — From the drop-down, select the community name (SNMPv2c) or user name (SNMPv3) for this trap destination. (If you defined only one, the name already appears in this field.)
  - **Send Authentication Failure Trap** — Select this option (the checkbox) if you want to alert the trap destination whenever an SNMP request is rejected because of an unrecognized community name or user name. After you click **Add**, the trap destinations and associated community names or user names appear in the table.
5. To make sure a trap is valid, select a trap destination from the table, and then click **Test Trap Destination** to send a test trap to the configured address.

### Results

The event monitor sends SNMP traps to the server(s) whenever an alertable event occurs.

## Configure SNMP MIB variables in SANtricity System Manager

For SNMP alerts, you can optionally configure Management Information Base (MIB) variables that appear in SNMP traps. These variables can return the storage array name, array location, and a contact person.

### Before you begin

The MIB file must be copied and compiled on the server with the SNMP service application.

If you do not have a MIB file, you can obtain it as follows:

- Go to [NetApp Support](#).
- Click **Downloads**, and then select **Downloads**.
- Click **E-Series SANtricity OS Controller Software**.
- Select **Download Latest Release**.
- Log in.
- Accept the Caution statement and license agreement.
- Scroll down until you see the MIB file for your controller type, and then click the link to download the file.

### About this task

This task describes how to define MIB variables for SNMP traps. These variables can return the following values in response to SNMP GetRequests:

- `sysName` (name for the storage array)
- `sysLocation` (location of the storage array)
- `sysContact` (name of an administrator)

## Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.
3. Select **Configure SNMP MIB Variables**.

The Configure SNMP MIB Variables dialog box opens.

4. Enter one or more of the following values, and then click **Save**.
  - **Name** — The value for the MIB variable `sysName`. For example, enter a name for the storage array.
  - **Location** — The value for the MIB variable `sysLocation`. For example, enter a location of the storage array.
  - **Contact** — The value for the MIB variable `sysContact`. For example, enter an administrator responsible for the storage array.

## Results

These values appear in SNMP trap messages for storage array alerts.

## Edit communities for SNMPv2c traps in SANtricity System Manager

You can edit community names for SNMPv2c traps.

### Before you begin

A community name must be created.

## Steps

1. From the left panel, select **Setting > Alerts**.
2. Select the **SNMP** tab.

The trap destinations and community names appear in the table.

3. Select **Configure Communities**.
4. Enter the new community name, and then click **Save**. Community names can consist of only printable ASCII characters.

## Results

The SNMP tab of the Alerts page displays the updated community name.

## Edit user settings for SNMPv3 traps in SANtricity System Manager

You can edit user definitions for SNMPv3 traps.

### Before you begin

A user must be created for the SNMPv3 trap.

## Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.

The trap destinations and user names appear in the table.

3. To edit a user definition, select the user in the table and then click **Configure Users**.
4. In the dialog, click **View/Edit Settings**.
5. Edit the following information:
  - **User name** — Change the name that identifies the user, which can be up to 31 characters long.
  - **Engine ID** — Select the Engine ID, which is used to generate authentication and encryption keys for messages, and must be unique on the administrative domain. In most cases, you should select **Local**. If you have a non-standard configuration, select **Custom**; another field appears where you must enter the authoritative engine ID as a hexadecimal string, with an even number of characters between 10 and 32 characters long.
  - **Authentication credentials** — Select an authentication protocol, which ensures the identity of users. Next, enter an authentication password, which is required when the authentication protocol is set or changed. The password must be between 8 and 128 characters long.
  - **Privacy credentials** — Select a privacy protocol, which is used to encrypt the contents of messages. Next, enter a privacy password, which is required when the privacy protocol is set or changed. The password must be between 8 and 128 characters long.

## Results

The SNMP tab of the Alerts page displays the updated settings.

## Add communities for SNMPv2c traps in SANtricity System Manager

You can add up to 256 community names for SNMPv2c traps.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.

The trap destinations and community names appear in the table.

3. Select **Configure Communities**.

The Configure Communities dialog box opens.

4. Select **Add another community**.
5. Enter the new community name, and then click **Save**.

## Results

The new community name appears in the SNMP tab of the Alerts page.

## Add users for SNMPv3 traps in SANtricity System Manager

You can add up to 256 users for SNMPv3 traps.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.

The trap destinations and user names appear in the table.

3. Select **Configure Users**.

The Configure SNMPv3 Users dialog box opens.

4. Select **Add**.

5. Enter the following information, and then click **Add**.

- **User name** — Enter a name to identify the user, which can be up to 31 characters long.
- **Engine ID** — Select the Engine ID, which is used to generate authentication and encryption keys for messages, and must be unique on the administrative domain. In most cases, you should select **Local**. If you have a non-standard configuration, select **Custom**; another field appears where you must enter the authoritative engine ID as a hexadecimal string, with an even number of characters between 10 and 32 characters long.
- **Authentication credentials** — Select an authentication protocol, which ensures the identity of users. Next, enter an authentication password, which is required when the authentication protocol is set or changed. The password must be between 8 and 128 characters long.
- **Privacy credentials** — Select a privacy protocol, which is used to encrypt the contents of messages. Next, enter a privacy password, which is required when the privacy protocol is set or changed. The password must be between 8 and 128 characters long.

## Remove communities for SNMPv2c traps in SANtricity System Manager

You can remove a community name for SNMPv2c traps.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.

The trap destinations and community names appear on the **Alerts** page.

3. Select **Configure Communities**.

The Configure Communities dialog box opens.

4. Select the community name you want to delete, and then click the **Remove (X)** icon on the far right.

If trap destinations are associated with this community name, the Confirm Remove Community dialog box shows the affected trap destination addresses.

5. Confirm the operation, and then click **Remove**.

### Results

The community name and its associated trap destination are removed from the Alerts page.

## Remove users for SNMPv3 traps in SANtricity System Manager

You can remove a user for SNMPv3 traps.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.

The trap destinations and user names appear on the Alerts page.

3. Select **Configure Users**.

The Configure SNMPv3 Users dialog box opens.

4. Select the user name you want to delete, and then click **Delete**.
5. Confirm the operation, and then click **Delete**.

## Results

The user name and its associated trap destination are removed from the Alerts page.

## Delete trap destinations in SANtricity System Manager

You can delete a trap destination address so that the storage array's event monitor no longer sends SNMP traps to that address.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **SNMP** tab.

The trap destination addresses appear in the table.

3. Select a trap destination, and then click **Delete** in the upper right of the page.
4. Confirm the operation, and then click **Delete**.

The destination address no longer appears on the Alerts page.

## Results

The deleted trap destination no longer receives SNMP traps from the storage array's event monitor.

## Manage syslog alerts

### Configure syslog server for alerts in SANtricity System Manager

To configure syslog alerts, you must enter a syslog server address and a UDP port. Up to five syslog servers are allowed.

#### Before you begin

- The syslog server address must be available. This address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- UDP port number of the syslog server must be available. This port is typically 514.

#### About this task

This task describes how to enter the address and port for the syslog server, and then test the address you entered.

## Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **Syslog** tab.

If a syslog server is not yet defined, the Alerts page displays "Add Syslog Servers."

3. Click **Add Syslog Servers**.

The Add Syslog Server dialog box opens.

4. Enter information for one or more syslog servers (maximum of five), and then click **Add**.
  - **Server Address** — Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.
  - **UDP Port** — Typically, the UDP port for syslog is 514. The table displays the configured syslog servers.
5. To send a test alert to the server addresses, select **Test All Syslog Servers**.

## Results

The event monitor sends alerts to the syslog server whenever an alertable event occurs. To further configure syslog settings for audit logs, see [Configure syslog server for audit logs](#).



If multiple syslog servers are configured, all configured syslog servers will receive an audit log.

## Edit syslog servers for alerts in SANtricity System Manager

You can edit the server address used for receiving syslog alerts.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **Syslog** tab.
3. From the table, select a syslog server address, and then click the **Edit** (pencil) icon from on the far right.

The row becomes an editable field.

4. Edit the server address and UDP port number, and then click the **Save** (checkmark) icon.

### Results

The updated server address appears in the table.

## Add syslog servers for alerts in SANtricity System Manager

You can add a maximum of five servers for syslog alerts.

### Before you begin

- The syslog server address must be available. This address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- The UDP port number of the syslog server must be available. This port is typically 514.

### Steps

1. From the left panel, select **Settings > Alerts**.

2. Select the **Syslog** tab.
3. Select **Add Syslog Servers**.

The Add Syslog Server dialog box opens.

4. Select **Add another syslog server**.
5. Enter information for the syslog server, and then click **Add**.
  - **Syslog Server Address** — Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.
  - **UDP Port** — Typically, the UDP port for syslog is 514.



You can configure up to five syslog servers.

## Results

The syslog server addresses appear in the table.

## Delete syslog servers for alerts in SANtricity System Manager

You can delete a syslog server so it no longer receives alerts.

### Steps

1. From the left panel, select **Settings > Alerts**.
2. Select the **Syslog** tab.
3. Select a syslog server address, and then click **Remove** from the top right.

The Confirm Delete Syslog Server dialog box opens.

4. Confirm the operation, and then click **Delete**.

## Results

The server you removed no longer receives alerts from the event monitor.

## Storage system alerts FAQ for SANtricity System Manager

This FAQ can help if you're just looking for a quick answer to a question.

### What if alerts are disabled?

If you want administrators to receive notifications about important events that occur in the storage array, you must configure an alerting method.

For storage arrays managed with SANtricity System Manager, you configure alerts from the Alerts page. Alert notifications can be sent through email, SNMP traps, or syslog messages. In addition, email alerts can be configured from the Initial Setup Wizard.

### How do I configure SNMP or syslog alerts?

In addition to email alerts, you can configure alerts to be sent by Simple Network Management Protocol (SNMP) traps or by syslog messages.

To configure SNMP or syslog alerts, go to **Settings > Alerts**.

## **Why are timestamps inconsistent between the array and alerts?**

When the storage array sends alerts, it does not correct for the time zone of the target server or host that receives the alerts. Instead, the storage array uses the local time (GMT) to create the timestamp used for the alert record. As a result, you might see inconsistencies between the timestamps for the storage array and the server or host receiving an alert.

Because the storage array does not correct for time zone when sending alerts, the timestamp on the alerts is GMT-relative, which has a time-zone offset of zero. To calculate a timestamp appropriate to your local time zone, you should determine your hour offset from GMT, and then add or subtract that value from the timestamps.

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.