# Managing the System Event Log

This chapter includes the following sections:

## System Event Log Policy

Cisco UCS Central supports a global system event log (SEL) policy.

## System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

The SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

You can use the SEL policy to backup the SEL to a remote server, and optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually backup or clear the SEL.

The backup file is automatically generated. The filename format is sel-*SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp*; for example, sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.

**Tip** For more information about the SEL, including how to view the SEL for each server and configure the SEL policy, see the Cisco UCS Manager configuration guides, which are accessible through the Cisco UCS B-Series Servers Documentation Roadmap.

# Configuring a SEL Policy

### Before You Begin

Before configuring a SEL policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

### Procedure

**Step 1**  On the menu bar, click **Operations Management**.

**Step 2**  In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

**Step 3**  Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

**Step 4**  In the **Navigation** pane, click **Operational Policies**.

**Step 5**  In the **Work** pane, click **Equipment**.

**Step 6**  In the **Work** pane, click the **SEL Policy** tab.

**Step 7**  In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

a)  In the **General** area, complete the following:

| Name | Description |
|---|---|
| **Name** field | The name of the Server Event Log (SEL) policy must be "sel". |
| **Type** field | The type of this policy must be "SEL". |
| **Description** field | The user-defined description of the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote). |

b)  In the **Backup Configuration** area, complete the following:

| Name | Description |
|------|-------------|
| **Protocol** field | The remote server communication protocol. This can be one of the following:<br><br>&bull; **FTP**<br><br>&bull; **TFTP**<br><br>&bull; **SCP**<br><br>&bull; **SFTP** |
| **Hostname** field | The hostname or IP address of the remote server. This can be a server, storage array, local drive, or any read/write media that Cisco UCS Central can access through the network.<br><br>The name of the backup file is generated by Cisco UCS. The name is in the following format:<br>`sel-`*`system-name-`*`ch`*`chassis-id-`*`serv`*`blade-id-blade-serial`*<br>`-`*`timestamp`*<br><br>**Note**    If you use a hostname rather than an IP address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central. |
| **Remote Path** field | The absolute path to the file on the remote server.<br><br>If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator. |
| **Backup Interval** drop-down list | The time to wait between automatic backups. If you select **Never**, Cisco UCS does not perform any automatic SEL data backups.<br><br>**Note**    If you want the system to create automatic backups, make sure you check the **Timer** check box in the **Action** option box. |
| **Format** field | The format to use for the backup file. This can be one of the following:<br><br>&bull; **ASCII**<br><br>&bull; **Binary** |
| **Clear on Backup** check box | If checked, Cisco UCS clears all system event logs after the backup. |
| **User** field | The username Cisco UCS Central should use to log in to the remote server. This field does not apply if the protocol is TFTP. |

| Name | Description |
|---|---|
| **Password** field | The password for the remote server username. This field does not apply if the protocol is TFTP. |
| **Action** option box | For each box that is checked, Cisco UCS creates a SEL backup when that event is encountered:<br><br>• **Log Full**—The log reaches the maximum size allowed.<br><br>• **On Change of Association**—The association between a server and its service profile changes.<br><br>• **On Clear**—The user manually clears a system event log.<br><br>• **Timer**—The time interval specified in the **Backup Interval** drop-down list is reached. |

**Step 8**   Click **Save**.

# Deleting a SEL Policy

### Procedure

**Step 1**   On the menu bar, click **Operations Management**.

**Step 2**   In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

**Step 3**   Under the **Domain Groups root** node, do one of the following choices:

• To configure the policy in the domain group root, click **Operational Policies**.

• To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

**Step 4**   In the **Navigation** pane, click **Operational Policies**.

**Step 5**   In the **Work** pane, click **Equipment**.

**Step 6**   In the **Work** pane, click the **SEL Policy** tab.

**Step 7**   In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

**Step 8**   Click **Save**.