Configuring Syslog in Cisco UCS Manager

This chapter contains the following sections:

Syslog Configuration

You can configure syslog in Cisco UCS Manager using both Cisco UCS Manager GUI and the Cisco UCS Manager CLI.

Configuring the Syslog Using Cisco UCS Manager GUI

SUMMARY STEPS

1. In the **Navigation** pane, click the **Admin** tab.
2. On the **Admin** tab, expand **All** > **Faults, Events, and Audit Log**.
3. Click **Syslog**.
4. In the **Work** pane, click the **Syslog** tab.
5. In the **Local Destinations** area, complete the following fields:
6. In the **Remote Destinations** area, complete the following fields to configure up to three external logs that can store messages generated by the Cisco UCS components:
7. In the **Local Sources** area, complete the following fields:
8. Click **Save Changes**.

DETAILED STEPS

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Faults, Events, and Audit Log**.

Step 3 Click **Syslog**.

Step 4 In the **Work** pane, click the **Syslog** tab.

Step 5 In the **Local Destinations** area, complete the following fields:

Name	Description
Console Section	
Admin State field	Whether Cisco UCS displays Syslog messages on the console. This can be one of the following: • **Enabled—**Syslog messages are displayed on the console as well as added to the log. • **Disabled—**Syslog messages are added to the log but not displayed on the console.
Level field	If this option is **enabled**, select the lowest message level that you want displayed. Cisco UCS displays that level and above on the console. This can be one of the following: • **Emergencies** • **Alerts** • **Critical**
Monitor Section	
Admin State field	Whether Cisco UCS displays Syslog messages on the monitor. This can be one of the following: • **Enabled—**Syslog messages are displayed on the monitor as well as added to the log. • **Disabled—**Syslog messages are added to the log but not displayed on the monitor. If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.

Name	Description
Level drop-down list	If this option is **enabled**, select the lowest message level that you want displayed. The system displays that level and above on the monitor. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
File Section	
Admin State field	Whether Cisco UCS stores messages in a system log file on the fabric interconnect. This can be one of the following: • **Enabled—**Messages are saved in the log file. • **Disabled—**Messages are not saved. If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	Select the lowest message level that you want the system to store. Cisco UCS stores that level and above in a file on the fabric interconnect. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**

Name	Description
Name field	The name of the file in which the messages are logged. This name can be up to 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period). The default is messages.
Size field	The maximum size, in bytes, the file can be before Cisco UCS Manager begins to write over the oldest messages with the newest ones. Enter an integer between 4096 and 4194304.

Step 6 In the **Remote Destinations** area, complete the following fields to configure up to three external logs that can store messages generated by the Cisco UCS components:

Name	Description
Admin State field	This can be one of the following: • **Enabled** • **Disabled** If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Hostname field	The hostname or IP address on which the remote log file resides. **Note** If you use a hostname rather than an IPv4 or IPv6 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.

Name	Description
Facility drop-down list	This is the remote server where the syslog files are sent. You can configure specific log files to reach specific destinations. This can be one of the following: • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

Step 7 In the **Local Sources** area, complete the following fields:

Name	Description
Faults Admin State field	If this field is **Enabled**, Cisco UCS logs all system faults.
Audits Admin State field	If this field is **Enabled**, Cisco UCS logs all audit log events.
Events Admin State field	If this field is **Enabled**, Cisco UCS logs all system events.

Step 8 Click **Save Changes**.

Configuring the Syslog Using the Cisco UCS Manager CLI

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # {**enable** | **disable**} **syslog console**	Enables or disables the sending of syslogs to the console.
Step 3	UCS-A /monitoring # **set syslog console level** {**emergencies** | **alerts** | **critical**}	(Optional) Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the

	Command or Action	Purpose
		console. The level options are listed in order of decreasing urgency.The default level is Critical.
Step 4	UCS-A /monitoring # {**enable** | **disable**} **syslog monitor**	Enables or disables the monitoring of syslog information by the operating system.
Step 5	UCS-A /monitoring # **set syslog monitor level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	(Optional) Select the lowest message level that you want displayed. If the monitor state is enabled, the system displays that level and above. The level options are listed in order of decreasing urgency.The default level is Critical. **Note** Messages at levels below Critical are displayed on the terminal monitor only if you have entered the **terminal monitor** command.
Step 6	UCS-A /monitoring # {**enable** | **disable**} **syslog file**	Enables or disables the writing of syslog information to a syslog file.
Step 7	UCS-A /monitoring # **set syslog file name** *filename*	The name of the file in which the messages are logged. Up to 16 characters are allowed in the file name.
Step 8	UCS-A /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	(Optional) Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog file. The level options are listed in order of decreasing urgency.The default level is Critical.
Step 9	UCS-A /monitoring # **set syslog file size** *filesize*	(Optional) The maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones. The range is 4096 to 4194304 bytes.
Step 10	UCS-A /monitoring # {**enable** | **disable**} **syslog remote-destination** {**server-1** | **server-2** | **server-3**}	Enables or disables the sending of syslog messages to up to three external syslog servers.
Step 11	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **level**{**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	(Optional) Select the lowest message level that you want stored to the external log. If the remote-destination is enabled, the system sends that level and above to the external server. The level options are listed in order of decreasing urgency.The default level is Critical.
Step 12	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **hostname** *hostname*	The hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname.
Step 13	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**}	(Optional) The facility level contained in the syslog messages sent to the specified remote syslog server.

	Command or Action	Purpose
Step 14	UCS-A /monitoring # {**enable** | **disable**} **syslog source** {**audits** | **events** | **faults**}	This can be one of the following: • **audits—**Enables or disables the logging of all audit log events. • **events—**Enables or disables the logging of all system events. • **faults—**Enables or disables the logging of all system faults.
Step 15	UCS-A /monitoring # **commit-buffer**	Commits the transaction.

This example shows how to enable the storage of syslog messages in a local file and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # disable syslog console
UCS-A /monitoring* # disable syslog monitor
UCS-A /monitoring* # enable syslog file
UCS-A /monitoring* # set syslog file name SysMsgsUCSA
UCS-A /monitoring* # set syslog file level notifications
UCS-A /monitoring* # set syslog file size 4194304
UCS-A /monitoring* # disable syslog remote-destination server-1
UCS-A /monitoring* # disable syslog remote-destination server-2
UCS-A /monitoring* # disable syslog remote-destination server-3
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```