

Configuring Communication Services

This chapter includes the following sections:

- Configuring HTTP, page 1
- Configuring SSH, page 3
- Configuring IPMI, page 4
- Configuring SNMP, page 6

Configuring HTTP

Before You Begin

You must log in as a user with admin privileges to perform this task.

GUI Configuration Guide for Cisco UCS E-Series Server Modules Integrated Management Controller, Release 1.0

- **Step 1** In the Navigation pane, click the Admin tab.
- Step 2 On the Admin tab, click Communications Services.
- Step 3 In the Communications Services pane, click the Communication Services tab.

Figure 1: Communication Services Tab

	Log Out
Overall Server Status — C 🔄 🕹 🧮 😟 0	
Communications Services	
Server Admin Communication Services SMMP	
User Management (HTTP Properties (IPMI over LAN Properties	
Network HTTP/S Enabled: S Enabled: S	
Certificati Management HTTP Port: 80 Privilege Level Limit: admin	
CIMC Log HTTPS Port: 443 Encryption Key: 000000000000000000000000000000000000	
Event Managament Session Timeout 10000 seconds	
Utilities Active Sessions: 3	
/ SSH Properties	
SSH Enabled: 🗹	
SSH Port: 22	
SSH Timeout: 1900 seconds	
Max Sessions: 4	
Active Sessions: 1	
	-
	V
Save Changes	Reset Values

Step 4 In the **HTTP Properties** area, update the following properties:

Name	Description
HTTP/S Enabled check box	Whether HTTP and HTTPS are enabled on the CIMC.
HTTP Port field	The port to use for HTTP communication. The default is 80.
HTTPS Port field	The port to use for HTTPS communication. The default is 443
Session Timeout field	The number of seconds to wait between HTTP requests before the CIMC times out and terminates the session.
	Enter an integer between 60 and 10,800. The default is 1800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the CIMC.
	This value may not be changed.

GUI Configuration Guide for Cisco UCS E-Series Server Modules Integrated Management Controller, Release

Name	Description
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the CIMC.

Step 5 Click Save Changes.

Configuring SSH

Before You Begin

You must log in as a user with admin privileges to configure SSH.

Procedure

- **Step 1** In the Navigation pane, click the Admin tab.
- Step 2 On the Admin tab, click Communications Services.
- Step 3 In the Communications Services pane, click the Communication Services tab.

Figure 2: Communication Services Tab

cisco Cisco Integ	rated Management Controller	CIMC Hostname: Logged in as:	ucse_user admin@10.21.169.25 Log Out
Crisco Cisco Integ	Acted Management Controller Communication Services Communication Services HTTP forctiss HTTP Properties HTTPs Port: Session Timeaut: Session Timeaut: SSH Properties SSH Properties SSH Properties SSH Properties SSH Properties SSH Properties Active Sessions: Active Sessions:	Logged in as:	admin @ 10.2.1.169.25 Log Out
		Save Ch	anges Reset Values

Step 4 In the **SSH Properties** area, update the following properties:

GUI Configuration Guide for Cisco UCS E-Series Server Modules Integrated Management Controller, Release 1.0

Name	Description
SSH Enabled check box	Whether SSH is enabled on the CIMC.
SSH Port field	The port to use for secure shell access. The default is 22.
SSH Timeout field	The number of seconds to wait before the system considers an SSH request to have timed out. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent SSH sessions allowed on the CIMC. This value may not be changed.
Active Sessions field	The number of SSH sessions currently running on the CIMC.

Step 5 Click Save Changes.

Configuring IPMI

IPMI Over LAN

Intelligent Platform Management Interface (IPMI) defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called a Baseboard Management Controller (BMC) and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating system obtain information about system health and control system hardware. For example, IPMI enables the monitoring of sensors, such as temperature, fan speeds and voltages, for proactive problem detection. If the server temperature rises above specified levels, the server operating system can direct the BMC to increase fan speed or reduce processor speed to address the problem.

Configuring IPMI over LAN

Configure IPMI over LAN when you want to manage the CIMC with IPMI messages.

Before You Begin

You must log in as a user with admin privileges to perform this task.

GUI Configuration Guide for Cisco UCS E-Series Server Modules Integrated Management Controller, Release

- **Step 1** In the Navigation pane, click the Admin tab.
- Step 2 On the Admin tab, click Communications Services.
- Step 3 In the Communications Services pane, click the Communication Services tab.

Figure 3: Communication Services Tab

cisco Cisco Integ	rated Management Controller	CIMC Hostname: Logged in as:	ucse_user admin@10.21.169.25 Log Out
Overall Server Status	C 3 4 🗰 0 0		
Waiting BIOS POST	Communications Services		
Server Admin	Communication Services SNMP		
User Management	(HTTP Properties		
Network	HTTP/S Enabled:		
Certificate Management	HTTP Port: 80 Privilege Level Limit: admin		
CIMC Log	HTTPS Port: 443	00	
Event Management	Session Timeout: 10800 seconds		
Utilities	Max Sessions: 4		
	SSH Properties		
	SSH Port: 22		
	SSH Timeout: 1800 seconds		
	Max Sessions: 4		
	Active Sessions: 1		
		Save Cha	nges Reset Values

Step 4 In the **IPMI over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	Whether IPMI access is allowed on this server.

Name	Description
Privilege Level Limit drop-down list	The highest privilege level that can be assigned to an IPMI session on this server. This can be one of the following:
	• read-only —IPMI users can view information but cannot make any changes. If you select this option, IPMI users with the "Administrator", "Operator", or "User" user roles can only create read-only IPMI sessions, regardless of their other IPMI privileges.
	• user —IPMI users can perform some functions but cannot perform administrative tasks. If you select this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server.
	• admin—IPMI users can perform all available actions. If you select this option, IPMI users with the "Administrator" user role can create admin, user, and read-only sessions on this server.
Encryption Key field	The IPMI encryption key to use for IPMI communications.

Step 5 Click Save Changes.

Configuring SNMP

SNMP

The Cisco UCS E-Series Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps.

Configuring SNMP Properties

Before You Begin

You must log in as a user with admin privileges to perform this task.

- **Step 1** In the Navigation pane, click the Admin tab.
- Step 2 On the Admin tab, click Communications Services.
- Step 3 In the Communications Services pane, click the SNMP tab.

Figure 4: SNMP Tab

sco Cisco Integ	irated Manageme	nt Controller			CIMC Host Logged	name: ucse_user in as: admin@10.21.169. Log (
verall Server Status	C 3. 3. 🔳 0.	0				
Good	Communications Se	rvices				
Server Admin	Communication Services 🧲	SNMP				
ser Management	SNMP Properties		 Trap Sett	ings		
twork	SNMP Enabled:		To configu	ire a trap dest	ination, select the target below	
ommunications Services	SNMP Port:	161	Commor	n Trap Destir	ation Settings]
ertificate Management	Access Community String	cimepublic	Trap C	ommunity Stri	ng: public	
MC Log	System Contact:	who@where		SNMP Versi	op: 1/2	
mware Management	Custom Landian	Lucia and		_	O Taxa O Inform	
lities	System Location:	unknown]	19	pe: @ trap O Inform	
			Trap De	stinations —]
			ID	Enabled	Trap Destination IP Address	
			1		0.0.0.0	A
			2		0.0.0.0	
			3		0.0.0.0	
			4		0.0.0.0	
						¥
						Character (Desert Malvas

Step 4 In the **SNMP Properties** area, update the following properties:

Name	Description
SNMP Enabled check box	Whether this server sends SNMP traps to the designated host.
SNMP Port field	The port the server uses to communicate with the SNMP host. This value cannot be changed.
Access Community String field	The default SNMP v1 or v2c community name. Enter a string up to 18 characters.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string up to 254 characters, such as an email address or a name and telephone number.

Name	Description
System Location field	The location of the host on which the SNMP agent (server) runs.
	Enter a string up to 254 characters.

Step 5 Click Save Changes.

What to Do Next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings.

Configuring SNMP Trap Settings

Before You Begin

You must log in as a user with admin privileges to disable platform event alerts.

GUI Configuration Guide for Cisco UCS E-Series Server Modules Integrated Management Controller, Release

- **Step 1** In the Navigation pane, click the Admin tab.
- Step 2 On the Admin tab, click Communications Services.
- Step 3 In the Communications Services pane, click the SNMP tab.

Figure 5: SNMP Tab

sco Cisco Integ	rated Manageme	nt Controller			CIMC Hostnar Logged in	ne: ucse_user as: admin@10.21.169 Log
verall Server Status	C 😃 🛃 🔞	0				
Good	Communications Se	rvices				
erver Admin	Communication Services 🧲	SNMP				
er Management	SNMP Properties		 Trap Sett	ings —		
twork	SNMP Enabled:		To configu	ure a trap des	tination, select the target below	
mmunications Services	SNMP Port:	161	Commor	n Trap Destii	nation Settings	
rtificate Management	Access Community String	cimepublic	Trap C	ommunity Stri	ng: public	
MC Log	System Contact:	who@where		CNMD Versi	ani (11)	
ent Management				SIMPLE VEISI		
lities	System Location:	unknown		Ty	pe: () Trap () Inform	
			Trap De	stinations —		
			ID	Enabled	Trap Destination IP Address	
			1		0.0.0.0	^
			2		0.0.0	
			3		0.0.0	
			4		0.0.0.0	
						¥.
)
					Save	Changes Reset Values

- **Step 4** In the **Trap Community String** text box in the **Common Trap Destination Settings** area, enter the name of the SNMP community to which trap information should be sent.
- **Step 5** In the **Trap Destinations** area, click the row of the desired SNMP trap destination. The **Traps Details** dialog box opens.
- **Step 6** In the **Trap Details** dialog box, complete the following fields:

Name	Description
ID column	The trap destination ID. This value cannot be modified.
Enabled column	For each SNMP trap destination that you want to use, check the associated check box in this column.
Trap Destination IP Address column	The IP address to which SNMP trap information is sent.

Step 7 Click Save Changes.

Sending a Test SNMP Trap Message

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

- **Step 1** In the Navigation pane, click the Admin tab.
- Step 2 On the Admin tab, click Communications Services.
- Step 3 In the Communications Services pane, click the SNMP tab.

Figure 6: SNMP Tab

ated Manageme	nt Controller				Logged	in as: admin@10.21.169. Log C
C 🕹 🕹 🧱 🙆	0					
Communications Se	rvices					
Communication Services 🧲	SNMP					
SNMP Properties			ap Sett	ings		
SNMP Enabled:	P Enabled: To configure a trap destination				nation, select the target below	
SNMP Port:	161	C	Commor	Trap Destin	ation Settings	
Access Community String	cimepublic		Trap C	ommunity Strin	g: public	
System Contact:	whordwhere			CHIMD Versie		
				Siver versio		
System Location:	unknown	JIL	Type: Type: Trap O Inform			
(Trap Destinations						
			ID	Enabled	Trap Destination IP Address	
			1		0.0.0.0	A
			2		0.0.0.0	
			3		0.0.0	
			4		0.0.0.0	
						v
					1	
	Source of the second se	Ated Management Controller	Ated Management Controller	Ated Management Controller	Ated Management Controller	Atted Management Controller Logodi Image:

- **Step 4** In the **Trap Destinations** area, click the row of the desired SNMP trap destination. The **Traps Details** dialog box opens.
- Step 5 Click Send SNMP trap.

An SNMPv1 test trap message is sent to the trap destination.

Note The trap must be configured and enabled in order to send a test message.

GUI Configuration Guide for Cisco UCS E-Series Server Modules Integrated Management Controller, Release