Managing Administrative Settings

This chapter includes the following sections:

Administrative Settings for Cisco UCS Central

Cisco UCS Central, supports configuring policies and user authentication natively from the **Administration** tab in the GUI, similar to the tasks defined for UCS domains from the **Operations Management** tab. Most of the features are common across the two tabs, the difference being in the user role and server support.

The **Administration** tab allows you to perform administration tasks in the following areas:

- General Settings
- Users and Authentication

Users and Authentication

Cisco UCS Central supports creating local and remote users to access the system. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each of these users must have a unique username and password. For more information, see User Management.

Cisco UCS Central uses LDAP for native authentication, but excludes RADIUS and TACACS+ authentication in this release. However, RADIUS, TACACS+ and LDAP authentication are supported in locally managed Cisco UCS domains. For more information, see Managing Administrative Settings, on page 1.

Creating Locally Authenticated Users

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Local Users**.
Step 4 In the **Actions** area, click **Create Locally Authenticated Users** and complete all the fields.
Step 5 Click the **Roles/Locales** tab so assign the type of role or locale, and click the **SSH** tab to assign the type of security key.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating Remote Users

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Remote Users**.
Step 4 In the **Actions** area, click **Create Remote Users** and complete all the fields.
Step 5 Click the **Roles/Locales** tab so assign the type of role or locale, and click the **SSH** tab to assign the type of security key.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating User Roles

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Roles**.
Step 4 In the **Actions** area, click **Create Role** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Creating User Locales

Before You Begin

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Locales**.
Step 4 In the **Actions** area, click **Create Locales** and complete all the fields.
Step 5 Click **Assign/Unassign Organization**, and/or **Assign/Unassign Domain Group**, to assign or unassign organizations and/or domain groups to the locale selected from Cisco UCS Central.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating an Authentication Domain

Cisco UCS Central uses LDAP for native authentication, but excludes RADIUS and TACACS+ authentication in this release. However, RADIUS, TACACS+ and LDAP remote authentication are supported for Cisco UCS domains, from the Cisco UCS Central Domain Group root.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Authentication Domains**.
Step 4 In the **Actions** area, click **Create Authentication Domain** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Creating an LDAP Provider

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Providers**.
Step 5 In the **Actions** area, click **Create LDAP Provider** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating an LDAP Provider Group

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Provider Groups**.
Step 5 In the **Actions** area, click **Create LDAP Provider Group** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating an LDAP Group Map

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Group Maps**.
Step 5 In the **Actions** area, click **Create LDAP Group Map** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

Deleting an LDAP Provider

Before You Begin

You need to create an LDAP provider.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **LDAP Providers**.
Step 5 In the **Actions** area, right-click the LDAP provider you wish to remove and click **Delete LDAP Provider**.
Step 6 Click **Save**.

Deleting an LDAP Provider Group

Before You Begin

You need to create an LDAP provider group.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Provider Groups**.
Step 5 In the **Actions** area, right-click the provider group you wish to remove and click **Delete LDAP Provider Group**.
Step 6 Click **Save**.

Deleting an LDAP Group Map

Before You Begin

You need to create an LDAP group map.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Group Maps**.
Step 5 In the **Actions** area, right-click the LDAP map you wish to remove and click **Delete LDAP Group Map**.
Step 6 Click **Save**.

General Settings

You can configure policies from the Cisco UCS Central GUI. These administrative policies are defined at the organization level and can manage anything in the infrastructure, from date and time, SNMP traps, to backup and export policies.

Creating an SNMP Trap

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **SNMP**.
Step 4 In the **Properties** area, select the **enabled** radio button.
By default the Admin State is disabled. You need to manually change it to enabled.
Step 5 In the **Actions** area, click **Create SNMP Trap** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

What to Do Next

Create an SNMP user.

Creating an SNMP User

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **SNMP**.
Step 4 In the **Actions** area, click **Create SNMP User** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Configuring an HTTPS Certificate

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **HTTPS**.
Step 4 In the **Actions** area, select a third party key ring from the **Key Ring** drop down list.
Step 5 Click **Save**.

Configuring an NTP Server

Cisco UCS Central supports global date and time policies based on international time zones and a defined NTP server.

Before You Begin

To configure an NTP server for Cisco UCS Central, you must first create a date and time policy.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **Date/Time** and select a time zone from the **Time Zone** drop down list.
Step 4 In the **Actions** area, click **Add NTP Server**.
Step 5 Click **OK**.
Step 6 Click **Save**.

Configuring a DNS Server

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **DNS**.
Step 4 In the **Actions** area, click **Add DNS Server** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Configuring Fault Policy

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **Fault Policy**.
Step 4 In the **Actions** area, complete all the fields.
Step 5 Click **Save**.

What to Do Next

Configuring Export Policy

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **TFTP Core Export Policy**.
Step 4 In the **Actions** area, complete all the fields.
Step 5 Click **Save**.

IPv6 Configuration

You can enable IPv6 on Cisco UCS Central in the standalone and High Availability (HA) modes. Cisco UCS Central configured on a single virtual machine is a standalone setup. A standalone setup is not part of any cluster. A UCS Central HA setup comprises two virtual machines, also known as primary node and secondary node respectively.

These virtual machines form an HA cluster, which is accessed through a common IP address. This IP address is known as a cluster IP address or a virtual IP address. You can assign an IPv6 address to the virtual IP Address (VIP) in addition to the IPv4 address.

Configuring IPv6 in Standalone Mode

Procedure

Step 1 On the menu bar, click **Administration**
Step 2 In the Navigation pane, select General.

By default the **General** tab would display tabs in the work pane

Step 3 Under the **Management Interface** tab, in the Node A area, click the **IPv6** tab, and complete all the required fields.

Step 4 Click **Save**.

Configuring IPv6 in HA mode

Procedure

Step 1 On the menu bar, click **Administration**

Step 2 In the Navigation pane, select General.
By default the **General** tab would display tabs in the work pane.

Step 3 Under the **Management Interface** tab, in the Node A and Node B area, click the **IPv6** tab, and complete all the required fields.

Step 4 Click **Save**.

Step 5 In the main area above the Nodes, add the Virtual IPv6 address information.

Step 6 Click **Save**.

Key Rings

Cisco UCS Central allows creation of key rings as a third party certificate for stronger authentication. HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices.

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 2048 bits to 4096 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Central provides a default key ring with an initial 2048-bit key pair, and allows you to create additional key rings.

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

Note Cisco UCS Central uses the same Third Party Certificate for both UCS Central to UCS Manager communication as well as for communication between UCS Central and the users' web browsers. UCS Central does not support using different certificates for the two types of communication at this time. Currently Third Party Certificates are only supported with Cisco UCS Manager, Release 2.2 (2c) and later.

Note When you create a key ring and certificate request, Cisco UCS Central generates the certificate request with a certificate signing capability. This certificate request after getting signed from a CA server should have one of the key usages defined as 'certificate signing'. If you use Microsoft Windows as an Internal Enterprise Certification Authority Server, you need to use the **Subordinate Certification Authority** template to generate the certificate. However, if you use a standalone CA server, you are not required to select the Certificate Template.

Creating a Key Ring

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Certificates**.
Step 4 In the **Actions** area, click **Create Key Ring** and complete all the fields.
Step 5 In the **Certificate Request Actions** area, click **Create** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating a Trusted Point

Cisco UCS Central allows you to create a trusted point containing the certificate of the root certificate authority (CA) and a subordinate CA in a bundled format. The root CA must contain a primary and self-signed certificate.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Certificates**.
Step 4 In the **Actions** area, click **Create Trusted Point** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Deleting a Key Ring

Before You Begin

Ensure that the HTTPS is not using the key ring.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Certificates**.
Step 4 In the **KeyRings Actions** area, right-click the key ring you want to delete and choose**Delete**.
Step 5 Click **Yes** in the confirmation dialog box.
The key ring is deleted from Cisco UCS Central.

Deleting a Trusted Point

Before You Begin

Ensure that the trusted point is not in use.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Certificates**.
Step 4 In the **KeyRings Actions** area, right-click the trusted point you want to delete and choose**Delete**.
Step 5 Click **Yes** in the confirmation dialog box.
The trusted point is deleted from Cisco UCS Central.

Importing a CA Certificate into a Browser

When you try to run the Cisco UCS Central application on your Internet browser for the first time, you might receive an error, which says that the website is untrusted or that the website's certificate is from an untrusted source or issuer. In such cases, you are required to import the root CA and subordinate CA (if any) certificate into your browser. Different browsers support this function. Complete the following procedures to import the certificates.

Mozilla Firefox

Procedure

Step 1 In the **Menu** bar, click**Tools** > **Options Advanced** > **Certificates**.
Step 2 Click **View Certificates**.
Step 3 Click **Authorities**.
Step 4 Click **Import**
Step 5 Select the CA certificate stored in your computer and open it.

The **Downloading Certificate** pop-up window opens.

Step 6 Select the checkbox **Trust this CA to identify Websites**.

Step 7 Click **OK**.

Microsoft Internet Explorer

Procedure

Step 1 In the **Menu** bar, click**Tools** > **Internet Options Content** > **Certificates**.

Step 2 Click **Trusted Root Certification Authorities**.

Step 3 Click **Import**
The **Certificate Import Wizard** pop-up window opens.

Step 4 Follow instructions in the Wizard until you select the CA certificate stored in your computer.

Step 5 Click **Finish**.

Google Chrome

Procedure

Step 1 On the right hand side of the **URL address** bar, select **Settings** .

Step 2 Under the HTTPS/SSL section, click **Manage Certificates**.

Step 3 Click **Trusted Root Certification Authorities**.

Step 4 Click **Import**
The **Certificate Import Wizard** pop-up window opens.

Step 5 Follow instructions in the Wizard until you select the CA certificate stored in your computer.

Step 6 Click **Finish**.

Administrative Settings for Cisco UCS Domains

Remote Access Policies

Cisco UCS Central supports global remote access policies defining the interfaces monitoring policy, displaying SSH configuration status, and providing policy settings for HTTP, Telnet, web session limits and CIM XML.

Configuring HTTP

Configuring an HTTP Remote Access Policy

Before You Begin

Before configuring an HTTP remote access 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, click **Operational Policies**.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **HTTP** 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.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- Telnet
- Web Session Limits
- CIM XML
- Interfaces Monitoring Policy
- SSH Configuration

Deleting an HTTP Remote Access Policy

An HTTP remote access policy is deleted from a domain group under the domain group root. HTTP remote access policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **HTTP** 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 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **Save**.

Configuring Telnet

Configuring a Telnet Remote Access Policy

Before You Begin

Before configuring a Telnet remote access 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, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **Telnet** 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.
Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP

- Web Session Limits
- CIM XML
- Interfaces Monitoring Policy
- SSH Configuration

Deleting a Telnet Remote Access Policy

A Telnet remote access policy is deleted from a domain group under the domain group root. Telnet remote access policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **Telnet** 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 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **Save**.

Configuring Web Session Limits

Configuring a Web Session Limits

Before You Begin

Before configuring a web session limits remote access 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, click **Operational Policies**.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Web Session Limits** 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.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- CIM XML
- Interfaces Monitoring Policy

Deleting a Web Session Limits

A web session limits remote access policy is deleted from a domain group under the domain group root. Web session limits remote access policies under the domain groups root cannot be deleted.

Procedure

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

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

Step 3 Expand the node for a domain group containing the policy to delete.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Web Session Limits** 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 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

Configuring CIM XML

Configuring a CIM XML Remote Access Policy

Before You Begin

Before configuring a CIM XML remote access 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, click **Operational Policies**.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **CIM XML** 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.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- Web Session Limits
- Interfaces Monitoring Policy

Deleting a CIM XML Remote Access Policy

A CIM XML remote access policy is deleted from a domain group under the domain group root. CIM XML remote access policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **CIM XML** 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 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **Save**.

Configuring Interfaces Monitoring

Configuring an Interfaces Monitoring Remote Access Policy

Before You Begin

Before configuring an interfaces monitoring remote access 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, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **Interfaces Monitoring** tab.
Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
a) In the **Monitoring Mechanism** area, select **Mii Status** to select Media Independent Interface Monitoring.
b) In the **Monitoring Mechanism** area, select **Ping ARP Targets** to select ARP Target Monitoring.
c) In the **Monitoring Mechanism** area, select **Ping Gateway** to select Gateway Ping Monitoring.
Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- Web Session Limits
- CIM XML

Deleting an Interfaces Monitoring Remote Access Policy

A interfaces monitoring remote access policy is deleted from a domain group under the domain group root. Interfaces monitoring remote access policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **Interfaces Monitoring** 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 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **Save**.

Authentication Services

Cisco UCS Central uses LDAP for native authentication, and RADIUS and TACACS+ for remote authentication.

Guidelines and Recommendations for Remote Authentication Providers

If a system is configured for one of the supported remote authentication services, you must create a provider for that service to ensure that Cisco UCS Central can communicate with it. In addition, you need to be aware of the following guidelines that impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in Cisco UCS Central or in the remote authentication server. The temporary sessions for users who log in through remote authentication services can be viewed through Cisco UCS Central GUI or Cisco UCS Central CLI.

User Roles in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles those users require for working in Cisco UCS Central and that the names of those roles match the names used in Cisco UCS Central. Depending on the role policy, a user may not be allowed to log in or will be granted only read-only privileges.

Local and Remote User Authentication Support

Cisco UCS Central uses LDAP for remote authentication, but excludes RADIUS and TACACS+ authentication in this release. However, RADIUS, TACACS+ and LDAP authentication are supported in locally managed Cisco UCS domains.

User Attributes in Remote Authentication Providers

When a user logs in, Cisco UCS Central does the following:

1. Queries the remote authentication service.
2. Validates the user.
3. If the user is validated, checks for the roles and locales assigned to that user.

The following table contains a comparison of the user attribute requirements for the remote authentication providers supported by Cisco UCS Central.

Table 1: Comparison of User Attributes by Remote Authentication Provider

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	Optional. You can choose to do either of the following: • Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements. • Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair.	The Cisco LDAP implementation requires a unicode type attribute. If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1 A sample OID is provided in the following section.

Sample OID for LDAP User Attribute

The following is a sample OID for a custom CiscoAVPair attribute:

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
```

```
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

LDAP Providers

You can configure remote users, assign roles and locales from Cisco UCS Central the same way as you can create LDAP users from Cisco UCS Manager. You should always create the LDAP provider from Cisco UCS Central Domain Group root.

LDAP Provider Groups

You can define up to 28 LDAP provider groups and nest them up to as many levels as the Active Directory supports for nesting in Cisco UCS Central. When you assign a provider to a nested group, even if the provider is a member of a different LDAP group, they become authenticated member of the parent nested group. During authentication, all the providers within a provider group are tried in order. If all of the configured servers are unavailable or unreachable, Cisco UCS Central automatically falls back to the local authentication method using the local username and password.

Creating an LDAP Provider

Cisco UCS Central supports a maximum of 16 LDAP providers.

Before You Begin

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with Cisco UCS Central. This account should be given a non-expiring password.

- In the Cisco UCS Central, configure one of the following:
  - LDAP groups: LDAP groups contain user role and locale information.
  - Users with the attribute that holds the user role and locale information for Cisco UCS Central: You can choose whether to extend the LDAP schema for this attribute. If you do not want to extend the schema, use an existing LDAP attribute to hold the Cisco UCS Central user roles and locales. If you prefer to extend the schema, create a custom attribute, such as the CiscoAVPair attribute.

    The Cisco LDAP implementation requires a unicode type attribute.

    If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1
  - For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Central.

- If you want to use secure communications, create a trusted point containing the certificate of the root certificate authority (CA) of the LDAP server in Cisco UCS Central.

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, click **Operational Policies**.
Step 4 In the **Work** pane, click **Security**.
Step 5 In the **Work** pane, expand **LDAP** and click **Providers**.
Step 6 Click **Create LDAP Provider** and fill in required information in all fields.
Step 7 Click **OK**.

What to Do Next

For implementations involving a single LDAP database, select LDAP as the authentication service.

Note When you specify multiple databases for implementation, if you choose a specific user within the database, the server goes in the order of the specified LDAP databases before authenticating the user.

Configuring Default Settings for LDAP Providers

You can configure the default settings for all providers defined in Cisco UCS Central from this **Properties (LDAP)** dialog box. If an individual provider includes a setting for any of these properties, Cisco UCS uses that setting and ignores the default setting.

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, click **Operational Policies**.
Step 4 In the **Work** pane, click **Security**.
Step 5 In the **Work** pane, expand **LDAP** and click **Providers**.
Step 6 In the **Actions** area, click **Properties** and complete all fields.
Step 7 In the **Properties (LDAP)** dialog box, complete all fields on the **General** tab and click **OK**.

Deleting an LDAP Provider

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, click **Operational Policies**.
Step 4 In the **Work** pane, click **Security**.
Step 5 In the **Work** pane, expand **LDAP** > **Providers**.
Step 6 In the **Work** pane, click the LDAP provider you want to delete.
Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **LDAP Provider** you want to delete to access that option.
Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Changing the LDAP Group Rule for an LDAP Provider

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, click **Operational Policies**.
Step 4 In the **Work** pane, click **Security**.
Step 5 In the **Work** pane, expand **LDAP** > **Providers**.
Step 6 Right click on the LDAP Provider name to which you want to change the group rules for.
Step 7 In the **Properties (LDAP Provider name)** dialog box, in the **LDAP Group Rules** section, change the group rules.
Step 8 Click **OK**.

LDAP Group Maps

For organizations that already use LDAP groups to restrict access to LDAP databases, group membership information can be used by Cisco UCS domains to assign a role or locale to an LDAP user during login. This eliminates the need to define role or locale information in the LDAP user object when Cisco UCS Central is deployed.

Cisco UCS Central uses LDAP group rule to determine LDAP groups when assigning user roles and locales to a remote user. When a user logs in, Cisco UCS Central retrieves information about the user's role and locale

from the LDAP group map. If the role and locale criteria match the information in the policy, Cisco UCS Central provides access to the user.

Role and locale definitions are configured locally in Cisco UCS Central and do not update automatically based on changes to an LDAP directory. If you delete or rename LDAP groups in the LDAP directory, make sure to update the changes in Cisco UCS Central.

You can configure an LDAP group map to include any of the following combinations of roles and locales:

- Roles only
- Locales only
- Both roles and locales

Example: If you want to configure authentication for an LDAP group representing a group of server administrators at a specific location, you can include user roles such as server-profile and server-equipment to the LDAP group. If you want to restrict access to server administrators at a specific location, you can specify locales with specific site names.

Note Cisco UCS Central includes many out-of-the-box user roles but does not include any locales. So you have to create a custom locale to map an LDAP provider group to a locale.

Nested LDAP Groups

You can search LDAP groups that are nested within another group defined in an LDAP group map. With this new capability, you do not always need to create subgroups in a group map in Cisco UCS Central.

Note

- Nested LDAP search support is supported only for Microsoft Active Directory servers. The supported versions are Microsoft Windows 2003 SP3, Microsoft Windows 2008 R2, and Microsoft Windows 2012.
- When you create nested LDAP group in MS-AD, if you use special characters in the name, make sure to configure the characters with \\(, \\). The following is an example for creating a nested LDAP group using Cisco UCS Central CLI:

```
create ldap-group CN=test1\\(\\),CN=Users,DC=ucsm,DC=qasam-lab,DC=in
```

Using the LDAP nesting feature, you can add an LDAP group as a member of another group and nest groups to consolidate member accounts and reduce the replication of traffic.

By default, user rights are inherited when you nest an LDAP group within another group. For example, if you make Group_1 a member of Group_2, the users in Group_1 will have the same permissions as the members of Group_2. You can then search users that are members of Group_1 by choosing only Group_2 in the LDAP group map, instead of having to search Group_1 and Group_2 separately.

Creating an LDAP Group Map

Before You Begin

- Create an LDAP group in the LDAP server.

- Configure the distinguished name for the LDAP group in the LDAP server.
- Create locales in Cisco UCS Central (optional).
- Create custom roles in Cisco UCS Central (optional).

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, click **Operational Policies**.
Step 4 In the **Work** pane, click **Security**.
Step 5 In the **Work** pane, expand **LDAP** and click **Group Maps**.
Step 6 In the **Actions** area, click **Create LDAP Group Map** and complete all fields and click **OK**.

What to Do Next

Set the LDAP group rule.

Deleting an LDAP Group Map

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, click **Operational Policies**.
Step 4 In the **Work** pane, click **Security**.
Step 5 In the **Work** pane, expand **LDAP** > **Group Maps**.
Step 6 In the **Work** pane, click the group map you want to delete.
Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **Group Map** you want to delete to access that option.
Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring RADIUS Providers

Configuring Properties for RADIUS Providers

The properties that you configure in this task are the default settings for all provider connections of this type defined in Cisco UCS Central. If an individual provider includes a setting for any of these properties, Cisco UCS Central uses that setting and ignores the default setting.

Note RADIUS native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central under the Domain Group root and domain groups. RADIUS may be used to create global policies for Cisco UCS domains.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

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

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **RADIUS** to access that option.

a) In the **Properties (RADIUS)** dialog box, complete all fields on the **General** tab.
b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Create a RADIUS provider.

Creating a RADIUS Provider

Cisco UCS Central supports a maximum of 16 RADIUS providers. RADIUS native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central under the Domain Group root and domain groups. RADIUS may be used to create global policies for Cisco UCS domains.

Before You Begin

Perform the following configuration in the RADIUS server:

- Configure users with the attribute that holds the user role and locale information for Cisco UCS Central. You can choose whether to extend the RADIUS schema for this attribute. If you do not want to extend the schema, use an existing RADIUS attribute to hold the Cisco UCS user roles and locales. If you prefer to extend the schema, create a custom attribute, such as the cisco-avpair attribute.

  The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001.

  The following syntax example shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute: `shell:roles="admin,aaa" shell:locales="L1,abc"`. Use a comma "," as the delimiter to separate multiple values.

- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Central.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Actions** area, click **Create RADIUS Provider** and complete all fields.
You can also right-click **Providers** to access that option.

a) In the **Create RADIUS Provider** dialog box, complete all fields on the **General** tab.
b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

- For implementations involving a single RADIUS database, select RADIUS as the primary authentication service.
- For implementations involving multiple RADIUS databases, configure a RADIUS provider group.

Deleting a RADIUS Provider

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Work** pane, click the **RADIUS Provider** you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **RADIUS Provider** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring TACACS+ Providers

Configuring Properties for TACACS+ Providers

The properties that you configure in this task are the default settings for all provider connections of this type defined in Cisco UCS Central. If an individual provider includes a setting for any of these properties, Cisco UCS Central uses that setting and ignores the default setting.

Note TACACS+ native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central. TACACS+ may be used to create global policies for Cisco UCS domains.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, click **TACACS+**.

Step 6 In the **Actions** area, click **Properties**.
You can also right-click **TACACS+** to access that option.

a) In the **Properties (TACACS+)** dialog box, complete all fields on the **General** tab.
b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Create an TACACS+ provider.

Creating a TACACS+ Provider

Cisco UCS Central supports a maximum of 16 TACACS+ providers. TACACS+ native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central. TACACS+ may be used to create global policies for Cisco UCS domains.

Before You Begin

Perform the following configuration in the TACACS+ server:

- Create the cisco-av-pair attribute. You cannot use an existing TACACS+ attribute.

  The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider.

  The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc".` Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing

authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values.

- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Central.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** and click **Providers**.

Step 6 In the **Actions** area, click **Create TACACS+ Provider** and complete all fields.
You can also right-click **Providers** to access that option.

a) In the **Create TACACS+ Provider** dialog box, complete all fields on the **General** tab.
b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

- For implementations involving a single TACACS+ database, select TACACS+ as the primary authentication service.
- For implementations involving multiple TACACS+ databases, configure a TACACS+ provider group.

Deleting a TACACS+ Provider

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** > **Providers**.

Step 6 In the **Work** pane, click the TACACS+ provider you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **TACACS+ Provider** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring Multiple Authentication Systems

Multiple Authentication Systems

You can configure Cisco UCS to use multiple authentication systems by configuring the following features:

- Provider groups
- Authentication domains

Once provider groups and authentication domains have been configured in Cisco UCS Central GUI, the following syntax can be used to log in to the system using Cisco UCS Central CLI: **ucs-** *auth-domain*

When multiple authentication domains and native authentication are configured with a remote authentication service, use one of the following syntax examples to log in with SSH or Putty:

From a Linux terminal:

- **ssh ucs-***auth-domain**username*@*Cisco UCS domain-ip-address*

  ```
  ssh ucs-example\\jsmith@192.0.20.11
  ```

- **ssh -l ucs-***auth-domain**username* {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*}

  ```
  ssh -l ucs-example\\jsmith 192.0.20.11
  ```

- **ssh** {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*} **-l ucs-***auth-domain**username*

  ```
  ssh 192.0.20.11 -l ucs-example\\jsmith
  ```

From a Putty client:

- Login as: **ucs-***auth-domain**username*

  ```
  Login as: ucs-example\\jsmith
  ```

From a SSH client:

- Host Name: *Cisco UCS domain-ip-address*

  User Name: **ucs-***auth-domain**username*

  ```
  Host Name: 192.0.20.11
  ```

  ```
  User Name: ucs-example\\jsmith
  ```

Provider Groups

A provider group is a set of providers that will be used by Cisco UCS during the authentication process. Cisco UCS Central allows you to create a maximum of 16 provider groups, with a maximum of eight providers allowed per group.

During authentication, all the providers within a provider group are tried in order. If all of the configured servers are unavailable or unreachable, Cisco UCS Central automatically falls back to the local authentication method using the local username and password.

Creating an LDAP Provider Group

Creating an LDAP provider group allows you to authenticate using multiple LDAP databases.

Note Authenticating with a single LDAP database does not require you to set up an LDAP provider group.

Before You Begin

Create one or more LDAP providers.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Provider Groups**.

Step 6 In the **Actions** area, click **Create LDAP Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create LDAP Provider Group** dialog box, complete all fields on the **General** tab.
b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

For implementations involving a single LDAP database, select LDAP as the authentication service.

Deleting an LDAP Provider Group

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Provider Groups**.

Step 6 In the **Work** pane, click the LDAP provider group you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **LDAP Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a RADIUS Provider Group

Creating a RADIUS provider group allows you to authenticate using multiple RADIUS databases.

Note Authenticating with a single RADIUS database does not require you to set up a RADIUS provider group.

Before You Begin

Create one or more RADIUS providers.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Actions** area, click **Create RADIUS Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create RADIUS Provider** dialog box, complete all fields on the **General** tab.
b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting a RADIUS Provider Group

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** > **Provider Groups**.

Step 6 In the **Work** pane, click the RADIUS provider group you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **RADIUS Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a TACACS+ Provider Group

Creating a TACACS+ provider group allows you to authenticate using multiple TACACS+ databases.

Note Authenticating with a single TACACS+ database does not require you to set up a TACACS+ provider group.

Before You Begin

Create one or more TACACS+ providers.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** and click **Provider Groups**.

Step 6 In the **Actions** area, click **Create TACACS+ Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create TACACS+ Provider Group** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	The name of the TACACS+ provider group.
Available Providers list box	The available TACACS+ providers that you can add to the TACACS+ group. You can use Shift+Click and Ctrl+Click to select multiple providers.
>> button	Adds all available providers to the group regardless of what providers are selected in the **Available Providers** list box.
> button	Adds the providers selected in the **Available Providers** list box to the group.
< button	Removes the providers selected in the **Assigned Providers** list box from the group.
<< button	Removes all providers from the group regardless of what providers are selected in the **Assigned Providers** list box.

Name	Description
Assigned Providers list box	The TACACS+ providers that are included in the TACACS+ group. Cisco UCS searches the providers in the order that they appear in the table. To change the provider priority, select a provider and use the arrow buttons above the list to move the provider to the desired position.

b) Click **OK**.

Step 7 Click **Save**.

Deleting a TACACS+ Provider Group

You cannot delete a provider group if it is being used by an authentication configuration.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** > **Provider Groups**.

Step 6 In the **Work** pane, click the **TACACS+ Provider Group** you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **TACACS+ Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Authentication Domains

Authentication domains are used by Cisco UCS Domain to leverage multiple authentication systems. Each authentication domain is specified and configured during login. If no authentication domain is specified, the default authentication service configuration is used.

You can create up to eight authentication domains. Each authentication domain is associated with a provider group and realm in Cisco UCS Domain. If no provider group is specified, all servers within the realm are used.

Note Effective with this release, authentication domains for LDAP are supported for Cisco UCS Central. However, the authentication domains are supported for managed Cisco UCS domains from the Cisco UCS Central Domain Group root.

Creating an Authentication Domain

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Authentication Domains**.

Step 6 In the **Actions** area, click **Create Authentication Domain** and complete all fields.
You can also right-click **Authentication Domains** to access that option.

a) In the **Create Authentication** dialog box, complete all fields on the **General** tab.
b) Click **OK**.

Step 7 Click **Save**.

Selecting a Primary Authentication Service

Selecting the Console Authentication Service

Before You Begin

If the system uses a remote authentication service, create a provider for that authentication service. If the system uses only local authentication through Cisco UCS, you do not need to create a provider first.

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Properties** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete all **Default Authentication** fields on the **General** tab.
b) In the **Properties (Native Authentication)** dialog box, complete all **Console Authentication** fields on the **General** tab.
c) In the **Properties (Native Authentication)** dialog box, complete **Remote Users Policy** field on the **General** tab.
d) Click **OK**.

Step 7 Click **Save**.

Selecting the Default Authentication Service

Before You Begin

If the system uses a remote authentication service, create a provider for that authentication service. If the system uses only local authentication through Cisco UCS, you do not need to create a provider first.

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, click **Operational Policies**.
Step 4 In the **Work** pane, click **Security**.
Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.
Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Native Authentication** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete all **Default Authentication** fields on the **General** tab.
b) Click **OK**.

Step 7 Click **Save**.

Role Policy for Remote Users

By default, if user roles are not configured in Cisco UCS Central read-only access is granted to all users logging in to Cisco UCS Central from a remote server using the LDAP protocol (excluding RADIUS and TACACS+ authentication in this release).

Note RADIUS, TACACS+ and LDAP authentication are supported in locally managed Cisco UCS domains.

You can configure the role policy for remote users in the following ways:

- **assign-default-role**

Does not restrict user access to Cisco UCS Central based on user roles. Read-only access is granted to all users unless other user roles have been defined in Cisco UCS Central.

This is the default behavior.

- **no-login**

  Restricts user access to Cisco UCS Central based on user roles. If user roles have not been assigned for the remote authentication system, access is denied.

For security reasons, it might be desirable to restrict access to those users matching an established user role in Cisco UCS Central.

Configuring the Role Policy for Remote Users

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, click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Native Authentication** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete **Remote Users Policy** field on the **General** tab.

b) Click **OK**.

Step 7 Click **Save**.

Configuring DNS Servers

Managing DNS Policies

Cisco UCS Central supports global DNS policies defining the DNS server and domain name. Registered Cisco UCS domains choosing to define DNS management globally within that domain's policy resolution control will defer DNS management to its registration with Cisco UCS Central.

Configuring a DNS Policy

Before You Begin

Before configuring a DNS policy in a domain group under the Domain Group root, 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, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DNS**.
Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
Step 7 Click **Save**.

Deleting a DNS Policy

Deleting a DNS policy will remove all DNS server settings within that 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, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DNS**.
Step 6 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 7 Click **Save**.

Configuring a DNS Server for a DNS Policy

Before You Begin

Configure a DNS 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, click **Operational Policies**.
Step 4 In the **Work** pane, click **DNS**.
Step 5 In the **Actions** area, click **Add DNS Server** and complete all fields.

a) In the **Add DNS Server** dialog box, complete all fields.
b) Click **OK**.

Step 6 Click **Save**.

Deleting a DNS Server from a DNS 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, click **Operational Policies**.
Step 4 In the **Work** pane, click **DNS**.
Step 5 In the **Actions** area, select the DNS server to delete and click **Delete**.
You can also right-click the DNS server to access that option.
Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 7 Click **Save**.

Managing Power Policies

Cisco UCS Central supports global equipment policies defining the global power allocation policy (based on policy driven chassis group cap or manual blade level cap methods), power policy (based on grid, n+1 or non-redundant methods). Registered Cisco UCS domains choosing to define power management and power supply units globally within that client's policy resolution control will defer power management and power supply units to its registration with Cisco UCS Central.

Configuring a Global Power Allocation Equipment Policy

Before You Begin

Before configuring a global power allocation equipment 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, 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 **Global Power Allocation Policy** tab.
Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
Step 8 Click **Save**.

Deleting a Global Power Allocation Equipment 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, 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 **Global Power Allocation 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**.

Configuring a Power Equipment Policy

Before You Begin

Before configuring a power equipment 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, 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 **Power Policy** tab.
Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
Step 8 Click **Save**.

Deleting a Power Equipment 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, 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 **Power 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**.

Managing Time Zones

Managing Time Zones

Cisco UCS Central supports global date and time policies based on international time zones and defined NTP server. Registered Cisco UCS Manager clients choosing to define date and time globally within that client's policy resolution control will defer the configuration for date and time to its registration with Cisco UCS Central.

Configuring a Date and Time Policy

Before You Begin

Before configuring a date and time 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, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DateTime**.
Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
Step 7 Click **Save**.

Deleting a Date and Time Policy

A date and time policy is deleted from a domain group under the domain group root. Date and time policies under the domain groups root cannot be deleted.

Deleting a date and time policy will remove all NTP server settings within that 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 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DateTime**.
Step 6 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 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 8 Click **Save**.

Configuring an NTP Server for a Date and Time Policy

Before You Begin

To configure an NTP server for a domain group under the domain group root, a date and time policy must first have been created.

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, click **Operational Policies**.
Step 4 In the **Work** pane, click **DateTime**.
Step 5 In the **Actions** area, click **Add NTP Server** and complete all fields and click **OK**.
Step 6 Click **Save**.

Configuring Properties for an NTP Server

An existing NTP server's properties may be updated before saving an NTP server instance. To change the name of an NTP server that is saved, it must be deleted and recreated.

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, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **DateTime**.
Step 6 In the **Actions** area, select the NTP server to configure, click **Properties** and complete all fields.
You can also right-click the NTP server to access that option. The **Properties (NTP Provider)** dialog accessed by clicking **Properties** in the in the **Actions** area cannot be edited if the NTP server has been saved. To change the server name of an NTP server that was saved, delete and recreate the NTP server.

a) In the **Properties (NTP Provider)** dialog box, complete all fields.

Name	Description
NTP Server field	The IP address or hostname of the NTP server you want to use. **Note** If you use a hostname rather than an IPv4 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.

b) Click **OK**.

Step 7 Click **Save**.

Deleting an NTP Server from a Date and Time 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, click **Operational Policies**.

Step 4 In the **Work** pane, click **DateTime**.

Step 5 In the **Actions** area, select the NTP server to delete and click **Delete**.
You can also right-click the NTP server to access that option. An NTP server that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

SNMP Policies

Cisco UCS Central supports global SNMP policies enabling or disabling, defining SNMP traps and SNMP users (with regular and privacy passwords, authentication types of md5 or sha, and encryption types DES and AES-128). Registered Cisco UCS domains choosing to define SNMP policies globally within that client's policy resolution control will defer all SNMP policies to its registration with Cisco UCS Central.

The SNMP Agent functionality provides the ability to remotely monitor the Cisco UCS Central. You can also change the Cisco UCS Central host IP, and then restart the SNMP agent on the new IP. SNMP is run on both the active and standby Cisco UCS Central servers and the configuration is persisted on both. Cisco UCS Central offers read-only access to only the operating system managed information base (MIB).Through the Cisco UCS Central CLI you can configure the community strings for SNMP v1, v2c, and create and delete the SNMPv3 users.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS Central, the managed device, that maintains the data for Cisco UCS Central and reports the data, as needed, to the SNMP manager. Cisco UCS

Central includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Central.

- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS Central supports only the OS MIBs.

Cisco UCS Central supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. The following RFCs define the SNMP:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco UCS Central generates SNMP notifications as traps. Traps are less reliable because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco UCS Central cannot determine if the trap was received.

SNMP Security Features

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

SNMP Security Models and Levels

The following table describes the combinations of SNMP security models and levels supported in Cisco UCS Central.

Table 2: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.

Model	Level	Authentication	Encryption	What Happens
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMP Support in Cisco UCS Central

Support for MIBs

Cisco UCS Central supports read-only access to OS MIBs. No set operations are available for the MIBs. The following MIBs are supported by Cisco UCS Central:

- SNMP MIB-2 System
- HOST-RESOURCES-MIB
    - hrSystem
    - hrStorage
    - hrDevice
    - hrSWRun
    - hrSWRunPerf
- UCD-SNMP-MIB
    - Memory

    - dskTable
    - systemStats
    - fileTable
- SNMP MIB-2 Interfaces
    - ifTable
- IP-MIB
- SNMP-FRAMEWORK-MIB
    - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

Note Cisco UCS Central does not provide support for IPV6 andCisco UCS Central MIBs.

Authentication Protocols for SNMPv3 Users

Cisco UCS Central supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

AES Privacy Protocol for SNMPv3 Users

Cisco UCS Central uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826. If AES is disabled but privacy password is set, then DES is used for encryption.

If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Central uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Configuring an SNMP Policy

Before You Begin

Before configuring a SNMP policy under a domain group, ensure that a SNMP policy is first created. Policies under the Domain Groups root which were already created by the system and are 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**, or the **Domain Group** name where you want to create the policy.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

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

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

Step 6 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 **Actions** area, click **Enabled** to choose the **Admin State**.
If **Enabled**, Cisco UCS Central uses SNMP to monitor the Cisco UCS Central system. Cisco UCS uses SNMP in all Cisco UCS domains included in the domain group if the groups themselves are not configured with SNMP.

The default state is **Disabled** with no fields displayed. Leaving the default state disables the SNMP policy

b) Enter the community or the username in the **Community/Username** field.
You can use the default SNMP v1 or v2c community name or SNMP v3 username Cisco UCS includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is public.

c) Enter the system contact person information in the **System Contact** field.
The **System Contact** person is responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.

d) Enter the system location in the **System Location** field.
The **System Location** defines the location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

Step 7 Click **Save**.

What to Do Next

Create SNMP traps and SNMP users.

Creating an SNMP Trap

Procedure

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

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

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Traps** area, click **Create SNMP Trap** and complete all applicable fields in the **Create SNMP Trap** dialog box.

a) Enter the SNMP host IP in the **IP Address** field.
Cisco UCS sends the trap to the defined IP address.

b) Enter the community or the username in the **Community/Username** field.
You can use the default SNMP v1 or v2c community name or SNMP v3 username Cisco UCS includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is public.

c) Enter the port number in the **Port** field.
Cisco UCS uses the defined port to communicate with the SNMP host for the trap. Enter an integer between 1 and 65535. The default port is 162.

d) Click **v1**, **v2c**, or **v3** to choose the SNMP **Version**.

e) Click **trap** to choose the SNMP trap**Type**.

f) Click **auth**, **no auth**, or **priv** to define the **v3Privilege**.

g) Click **OK**.

Step 6 Click **Save**.

Creating an SNMP User

Procedure

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

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

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Users** area, click **Create SNMP User** and complete all applicable fields in the **Create SNMP User** dialog.

a) Enter the SNMP username in the **Name** field.
Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen).

Note You cannot create an SNMP username that is identical to locally authenticated username.

b) Click **md5** or **sha** to chose the authorization type.
c) Check the **AES-128** checkbox.
If checked, this user uses AES-128 encryption.
d) Enter the user password in the **Password** field.
e) Re-enter the user password in the **Confirm Password** field.
f) Enter the privacy password for this user in the **Privacy Password** field.
g) Re-enter the privacy password for this user in the **Confirm Privacy Password** field.
h) Click **OK**.

Step 6 Click **Save**.

Deleting an SNMP Policy

A SNMP policy is deleted from a domain group under the domain group root. SNMP policies under the domain groups root cannot be deleted.

Deleting an SNMP policy will remove all SNMP trap and SNMP User settings within that 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, click **Operational Policies**.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **SNMP**.
Step 6 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 7 Click **Save**.

Deleting an SNMP Trap

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 In the **Navigation** pane, click **Operational Policies**.
Step 4 In the **Work** pane, click **SNMP**.
Step 5 In the **SNMP Traps** area, select the SNMP trap to delete and click **Delete**.
You can also right-click the SNMP trap to access that option.

Step 6 Click **Save**.

Deleting an SNMP User

Procedure

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

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

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Users** area, select the SNMP user to delete and click **Delete**.
You can also right-click the SNMP user to access that option.

Step 6 Click **Save**.

System Event Log

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

The system event log (SEL) 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.

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, 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, fill in the required fields.
b) In the **Backup Configuration** area, fill in the required fields.

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, 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**.