Cisco UCS Central Authentication Guide, Release 2.0

First Published: 2017-05-16

Last Modified: 2018-07-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.

Text Type	Indication
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

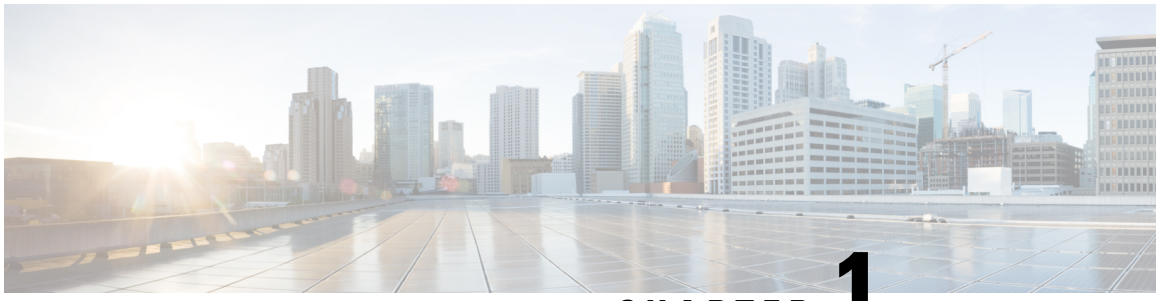
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.



CHAPTER 1

Overview

Overview

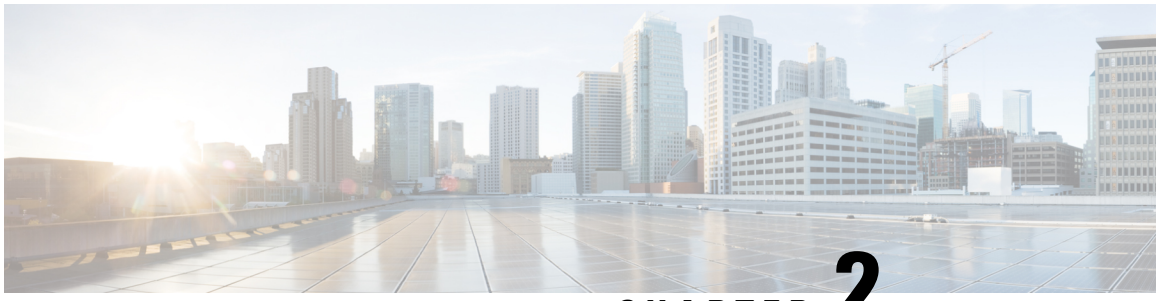
The Cisco UCS Central Authentication Guide provides guidelines and tasks related to managing and maintaining remote and locally authenticated user accounts.

Cisco UCS Central User Documentation Reference

The Cisco UCS Central following use case-based documents to understand and configure Cisco UCS Central:

Guide	Description
Cisco UCS Central Getting Started Guide	Provides a brief introduction to the Cisco UCS infrastructure, Cisco UCS Manager, and Cisco UCS Central. Includes an overview of the HTML5 UI, how to register Cisco UCS domains in Cisco UCS Central, and how to activate licenses.
Cisco UCS Central Administration Guide	Provides information on administrative tasks, such as user management, communication, firmware management, backup management, and Smart Call Home.
Cisco UCS Central Authentication Guide	Provides information on authentication tasks, such as passwords, users and roles, RBAC, TACACS+, RADIUS, LDAP, and SNMP.
Cisco UCS Central Server Management Guide	Provides information on server management, such as equipment policies, physical inventory, service profiles and templates, server pools, server boot, and server policies.

Guide	Description
Cisco UCS Central Storage Management Guide	Provides information on storage management, such as ports and port channels, VSAN and vHBA management, storage pools, storage policies, storage profiles, disk groups, and disk group configuration.
Cisco UCS Central Network Management Guide	Provides information on network management, such as ports and port channels, VLAN and vNIC management, network pools, and network policies.
Cisco UCS Central Operations Guide	Best practices for setting up, configuring, and managing domain groups for small, medium and large deployments.
Cisco UCS Central Troubleshooting Guide	Provides help for common issues in Cisco UCS Central.



CHAPTER 2

Users and Roles

Role-Based Access Control Overview

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and a locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, you can manage individual user privileges by assigning the appropriate roles and locales.

A user is granted write access to the required system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the engineering organization can update server configurations in the Engineering organization. They cannot, however, update server configurations in the Finance organization, unless the locales assigned to the user include the Finance organization.

Cisco UCS Central User Accounts

Access the system with user accounts. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each user account must have a unique username and password.

You can setup a user account with an SSH public key, in either of the two formats: OpenSSH or SECSH.

Admin Account

The Cisco UCS Central admin account is the default user account. You cannot modify or delete it. This account is the system administrator, or superuser account, and has full privileges. There is no default password assigned to the admin account. You must choose the password during the initial system setup.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

The local admin user can login for fail over, even when authentication is set to remote.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated through the Cisco UCS Central user database. Anyone with admin or aaa privileges can enable or disable it. Once you disable a local user account, the user cannot log in.

Note Cisco UCS Central does not delete configuration details for disabled local user accounts from the database. If you re-enable a disabled local user account, the account becomes active again with the existing configuration, including username and password.

Remotely Authenticated User Accounts

A remotely authenticated user account is any Cisco UCS Central user account that is authenticated through LDAP. Cisco UCS domains support LDAP, RADIUS and TACACS+.

If a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

Expiration of User Accounts

You can configure user accounts to expire at a predefined time. When the user account reaches the expiration time, the account disables.

By default, user accounts do not expire.

Note After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account to expire with the farthest expiration date available.

Guidelines for Creating Usernames

The username is also used as the login ID for Cisco UCS Central. When you assign login IDs to Cisco UCS Central user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)
- The login ID must be unique within Cisco UCS Central.

- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Reserved Words: Locally Authenticated User Accounts

You cannot use the following words when creating a local user account in Cisco UCS.

- root
- bin
- daemon
- adm
- lp
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man

- sys
- samdme
- debug

User Roles

User roles contain one or more privileges that define the operations that are allowed for a user. You can assign one or more roles to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role 2 has server-related privileges, users with Role1 and Role 2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Any user roles configured after the first 48 are accepted, but they are inactive with faults raised. Each domain group in Cisco UCS Central can also contain 48 user roles, including the user roles that are inherited from the parent domain group. When user roles are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 roles are active. Any user roles after the first 48 are inactive with faults raised.

All roles include read access to all configuration settings in the Cisco UCS domain. Users with read-only roles cannot modify the system state.

You can create, modify or remove existing privileges, and delete roles. When you modify a role, the new privileges apply to all users with that role. Privilege assignment is not restricted to the privileges defined for the default roles. Meaning, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have a different set of privileges. However, you can create a Server and Storage Administrator role that combines the privileges of both roles.

Note If you delete a role after it was assigned to users, it is also deleted from those user accounts.

Modify the user profiles on AAA servers (RADIUS or TACACS+) to add the roles corresponding to the privileges granted to that user. The attribute stores the role information. The AAA servers return this attribute with the request and parse it to obtain the roles. LDAP servers return the roles in the user profile attributes.

Default User Roles

The system contains the following default user roles:

AAA Administrator

Read-and-write access to users, roles, and AAA configuration. Read access to the remaining system.

Administrator

Complete read-and-write access to the entire system. Assigns this role to the default administrator account by default. You cannot change it.

Facility Manager

Read-and-write access to power management operations through the power management privilege. Read access to the remaining system.

Network Administrator

Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the remaining system.

Operations

Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the remaining system.

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Server Compute

Read and write access to most aspects of service profiles. However, the user cannot create, modify or delete vNICs or vHBAs.

Server Equipment Administrator

Read-and-write access to physical server-related operations. Read access to the remaining system.

Server Profile Administrator

Read-and-write access to logical server-related operations. Read access to the remaining system.

Server Security Administrator

Read-and-write access to server security-related operations. Read access to the remaining system.

Storage Administrator

Read-and-write access to storage operations. Read access to the remaining system.

Reserved Words: User Roles

You cannot use the following words when creating custom roles in Cisco UCS.

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

Privileges

Privileges give users, assigned to user roles, access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Tip Detailed information about these privileges and the tasks that they enable users to perform is available in *Privileges in Cisco UCS* available at the following URL: http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html.

Table 1: System Defined Roles

Role	Privileges	Role to Configure in LDAP/RADIUS/TACACS Server
AAA Administrator	aaa	aaa
Administrator	admin	admin
Facility Manager	facility-manager	power-mgmt
KVM Administrator	kvm	kvm
Network	pod-qos,pod-config,pod-policy,ext-lan-qos,pod-security,	network
Operations	fault, operations	fault, operations
Read-Only	read-only	read-only
Server-Compute Administrator		server-compute
Server-Equipment Administrator	server-policy,server-equipment,server-maintenance	server-equipment
Server Profile Administrator		server-profile
Server Security Administrator	server-security,service-profile-security,service-profile-security-policy	server-security
Statistics Administrator	stats	stats-management
Storage Administrator		storage

Table 2: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
domain-group-management	Domain Group Management	Domain Group Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator

Privilege	Description	Default Role Assignment
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
kvm	Launch KVM	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator
service-profile-compute	Service profile compute	Server Compute Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile endpoint access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator

Privilege	Description	Default Role Assignment
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Security Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator
stats	Statistics Management	Statistics Administrator

Managing UCS Central Roles

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Roles** and press **Enter**.

This launches the **UCS Central Roles Manage** dialog box.

Step 2 In **Roles**, click **Add** to create a new role, or select an existing role.

Step 3 In the **Network** tab, click **Add** to update and add privileges.

Step 4 Select relevant privileges for the role.

Step 5 Click **Apply** to apply the new privileges.

Step 6 Update the **Storage**, **Server**, and **Operations** privileges for the role, in the same manner.

Step 7 Click **Save**.

Managing UCS Central Local Users

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Local Users** and press **Enter**.

This launches the **UCS Central Local Users Manage** dialog box.

Step 2 In **Local Users**, click **Add** to create a new local user, or select an existing one.

Step 3 In the **Basic** tab, complete the necessary information for the user.

Step 4 In the **Roles** tab, add or remove the roles assigned to the user.

a) Click **Add** to display the roles.
b) Select a role or roles.
c) Click **Apply** to apply the new privileges.

Step 5 In the **Locales** tab, add or remove the locales assigned to the user.

a) Click **Add** to display the roles.
b) Select a role or roles.
c) Click **Apply** to apply the new privileges.

Step 6 In the **SSH** tab, select the **Authentication Type**.

Step 7 Click **Save**.

Managing UCS Central Remote Users

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Remote Users** and press **Enter**.

This launches the **UCS Central Remote Users Manage** dialog box.

Step 2 In **Remote Users**, review the remote LDAP users, roles, and locales.

Note This section is read-only.

Step 3 Click **Cancel** to close the window, or **Save** to save any changes made in other sections.

User Locales

You can assign a user to one or more locales. Each locale defines one or more organizations (domains) to which a user can access. Access is usually limited to the organizations specified in the locale. An exception is a locale without any organizations. It provides unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Any user locales configured after the first 48 are accepted, but are inactive with faults raised. Each domain group in Cisco UCS Central can contain 48 user locales, including the user locales that are inherited from the parent domain group. When user locales are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 locales are active. Any user locales after the first 48 are inactive with faults raised.

Users with admin or aaaadmin, aaa, or domain-group-management privileges can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization, a user assigned to that locale can only assign the Engineering organization to other users.

Note You cannot assign a locale to users with the admin privilege.

Note You cannot assign a locale to users with one or more of the following privileges:

- aaa
- admin
- fault
- operations

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations below it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization. However, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

User Organizations

A user can create one or more organizations. Each organization defines sub-organizations, faults, events, UUID suffix pools and blocks of UUIDs.

Cisco UCS organizations are hierarchically managed by users. A user that is assigned at the root level organization has automatic access to all organizations and domain groups under it.

Managing UCS Central Locales

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Locales** and press **Enter**.

This launches the **UCS Central Locales Manage** dialog box.

Step 2 In **Locales**, click **Add** to add a new locale, or select an existing one.

Step 3 Assign **Organizations** and **Domain Groups** to the locale.

a) Click **Add** to display the organizations or domain groups.
b) Select the organizations or domain groups.
c) Click **Apply** to apply the new privileges.

Step 4 Click **Save**.

Managing Domain Group Users

Procedure

Step 1 Click the **Domain Group** icon and choose **root**.

Step 2 Click the **Settings** icon and choose **Users**.

Step 3 In **Roles**, select roles to associate them with the domain group. Uncheck roles to disassociate them from the domain group.

Step 4 In the **Network** tab, click **Add** to update and add privileges.

a) Click **Add** to display the organizations.
b) Select relevant privileges for the role.
c) Click **Apply** to apply the new privileges.

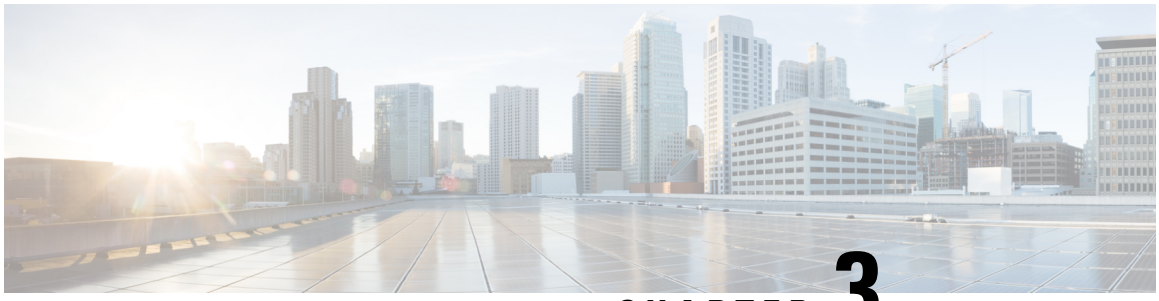
Step 5 Update the **Storage**, **Server**, and **Operations** privileges for the role, in the same manner.

Step 6 In **Locales**, select locales to associate them with the domain group. Uncheck roles to disassociate them from the domain group.

Step 7 Assign **Organizations** to the locale.

a) Click **Add** to display the organizations.
b) Select the organizations or domain groups.
c) Click **Apply** to apply the new privileges.

Step 8 Click **Save**.



CHAPTER 3

Authentication Services

Authentication Services

Cisco UCS Central supports the following methods for authenticating user logins:

- Local user authentication for user accounts that exist locally in Cisco UCS Central
- Remote user authentication for registered UCS domains with one of the following protocols:
  - LDAP
  - RADIUS
  - TACACS+

Guidelines for Creating Passwords

Each locally authenticated user account requires a password. Cisco recommends that each user have a strong password. A user with admin, aaa, or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on user passwords. If you enabled the password strength check, each user must use a strong password.

Cisco UCS Central rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters

- Digits
- Special characters

- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. Meaning, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

Password Profile for Locally Authenticated Users

The password profile contains the password history and the password change interval properties for all locally authenticated users of Cisco UCS Central. You cannot specify a different password profile for locally authenticated users.

Note You must have admin, aaa, or domain-group-management privileges to change the password profile properties. Except for the password history, these properties do not apply to users with these administrative privileges.

Password History Count

The password history count prevents locally authenticated users from reusing the same password. When you configure the password history count, Cisco UCS Central stores up to a maximum of 15 previously used passwords. The password history count stores the passwords in reverse chronological order with the most recent password first. This ensures that the user can only reuse the oldest password when the history count reaches its threshold.

A user can create and use the number of passwords configured in the password history count before reusing a password. For example, if you set the password history count to 8, a user cannot reuse the first password until the ninth password expires.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously used passwords at any time.

You can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

The password change interval restricts the number of password changes that a locally authenticated user can make within a specific number of hours. The following table describes the two interval configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	Does not allow changing passwords for locally authenticated user within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.	To prevent the user from changing passwords within 48 hours after a password change: • Set **Change during interval** to disable • Set **No change interval** to 48
Password changes allowed within change interval	Specifies the maximum number of times that a locally authenticated user password change can occur within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of two password changes within a 48-hour interval.	To allow a password change for a maximum of one time within 24 hours after a password change: • Set **Change during interval** to enable • Set **Change count** to 1 • Set **Change interval** to 24

Managing UCS Central Authentication

Procedure

Step 1 Click the **System Configuration** icon and choose **Authentication**.

This launches **Cisco UCS Central Authentication Manage** dialog box.

Step 2 In **LDAP**, supply the information requested in these tabs.

a) On the **Basic** tab, type values for the **Database Connection Timeout**, **Filter**, **Attribute**, and **Base DN**.

b) On the **Providers** tab, click + to add a provider, and complete the necessary information in the **Basic** and **Group Rules** tabs.

Select **Enabled** or **Disabled** in the SSL section. If you select **Enabled**, encryption is required for communications with the LDAP database. Enabling SSL LDAP uses STARTTLS which allows encrypted communication using port 389. If you check **Disabled**, authentication information will be sent as clear text.

c) On the **Groups** tab, click + to add a provider group, and optionally associate it with a provider.

- The maximum number of LDAP provider groups supported for Cisco UCS Central is 16.
- The maximum providers supported in Cisco UCS Central, for one provider group, is 8.

d) On the **Group Maps** tab, enter a **Provider Group Map DN**, and then optionally add **Roles** and **Locales**.

The maximum group map length cannot exceed more than 240 characters in Cisco UCS Central. For example:

```
maximum group-map length:
--------------------------------
CN=jeewan2,\
OU=1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-\
23-24-1,\
OU=1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-\
23-24-0,\
OU=ou-01-11-1,\
DC=ucsm,DC=qasam-lab,DC=in
```

Step 3 In **TACACS+**, complete the following sections as required:

a) On the **Basic** tab, type values for the **Database Connection Timeout** and **Retry Count**.

b) On the **Providers** tab, click + to add a provider, and complete the necessary configuration information.

You can use the up and down arrows to change the order of the providers.

c) On the **Groups** tab, click + to add a provider group, and optionally associate it with a provider.

Step 4 In **RADIUS**, complete the following sections as required:

a) On the **Basic** tab, type values for the **Database Connection Timeout** and **Retry Count**.

b) On the **Providers** tab, click + to add a provider, and complete the necessary configuration information.

You can use the up and down arrows to change the order of the providers.

c) On the **Groups** tab, click + to add a provider group, and optionally associate it with a provider.

Step 5 In **Authentication Domains**, configure, add, or delete Native or Console default domains.

The maximum number of Authentication Domains supported in Cisco UCS Central is 8.

Step 6 Click **Native (Default)**:

a) Select the **Default Behavior for Remote Users**.

- Assign read only access role
- Deny login

b) In **Web Session Refresh Period (Seconds)**, enter the maximum amount of time allowed between refresh requests for a user accessing a Cisco UCS domain.

If the session exceeds the time limit, Cisco UCS Central changes the web session to inactive, but it does not terminate the session.

Specify between 60 and 172800 seconds. The default is 600 seconds.

c) In **Web Session Timeout (Seconds)**, enter the maximum amount of time that can elapse after the last refresh request. If the web session exceeds time limit, Cisco UCS Central automatically terminates the web session.

Specify between 60 and 172800 seconds. The default is 7200 seconds.

d) Choose **Enable** or **Disable** for **Authentication**.

e) If you selected **Enabled**, select an **Authentication Realm**:

- **LDAP**—Define users on the LDAP server specified in Cisco UCS Central.
- **Local**—Define users locally in Cisco UCS Central or the Cisco UCS domain.

- **RADIUS**—Define users on the RADIUS server specified in Cisco UCS Central.
- **TACACS+**—Define users on the TACACS+ server specified in Cisco UCS Central.

f) If you selected **LDAP**, **RADIUS**, or **TACACS+**, you can select an associated provider group from the**Provider Group**.

Step 7 Click **Console (Default)**:

a) Choose to enable or disable **Authentication**.
b) If you selected **Enabled**, select an **Authentication Realm**.
c) If you selected **LDAP**, **RADIUS**, or **TACACS+**, you can select an associated provider group from the **Provider Group**.

Step 8 Click + to add a new authentication domain.

a) Enter the name of the authentication domain.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period). You cannot change this name once you save it.

For systems using LDAP, TACACS, and RADIUS, the authentication domain name counts toward the 32 character limit for locally created usernames. Because Cisco UCS reserves five characters for formatting, you are not allowed to have a combined total of more than 27 characters for the domain name and username.

b) Enter the **Web Session Refresh Period (Seconds)**.
c) Enter the **Web Session Timeout (Seconds)**.
d) If the **Authentication Realm** is set to **LDAP**, **RADIUS**, or **TACACS+**, select a **Provider Group**.

Step 9 Click **Save**.

After creating an authentication domain, you can edit the configuration or remove it.

Windows Passthrough Authentication

Cisco UCS Central release 2.0 uses Windows passthrough authentication for remote user logins to add a level of security to account logins. Windows passthrough authentication provides a streamlined method to sign into Cisco UCS Central without entering user credentials again, after you log on to a computer residing on a domain.

A check box present at the login prompt enables Windows passthrough authentication. However, you cannot click the check box initially to sign on using the Windows credentials. Cisco UCS Central prompts you to download an external plugin. After you download, install, and enable the plugin, you can sign on using the Windows passthrough authentication.

Windows passthrough authentication on Cisco UCS Central 2.0 has the following prerequisites:

- Your Windows client system must be connected to an Active Directory Domain and you must be logged in with Active Directory credentials
- Active Directory deployment must support Active Directory Federation Services
- Your environment must have a minimum .NET Framework Version 4.0.30319

Windows passthrough authentication has the following limitations:

- Cisco UCS Central supports Windows passthrough authentication only on Microsoft Internet Explorer version 11.
- You must download and install a Cisco plugin.
- Windows passthrough authentication is currently supported only when the authentication realm is set to LDAP and not RADIUS or TACAS+. The LDAP realm name has to match the domain name. For example, if an LDAP realm name is CISCO/username, the LDAP realm would be CISCO as well.

Managing Domain Group Authentication

Procedure

Step 1 Click the **Domain Group Navigation** icon and choose root.

This launches the **root Domain Group** page.

Step 2 Click the **Settings** icon and launch the **Authentication** page.

The **Root Manage** dialog opens.

Step 3 In **LDAP**, enter the following information:

a) On the **Basic** tab, type values for the **Database Connection Timeout**, **Filter**, **Attribute**, and **Base DN**.

b) In the **Providers** tab, click + to add a provider, and complete the necessary information in the **Basic** and **Group Rules** tabs.

Select **Enabled** or **Disabled** in the SSL section. If you select **Enabled**, encryption is required for communications with the LDAP database. Enabling LDAP uses STARTTLS which allows encrypted communication using port 389. If you check **Disabled**, authentication information will be sent as clear text.

c) In the **Groups** tab, click + to add a provider group, and optionally associate it with a provider.

- The maximum number of LDAP provider groups supported for Cisco UCS Central is 16.
- The maximum providers supported in Cisco UCS Central, for one provider group, is 8.

d) On the **Group Maps** tab, click + to enter a **Provider Group Map DN**, and then optionally add **Roles** and **Locales**.

The maximum group map length supported in Cisco UCS Central is 240.

```
maximum group-map length:
--------------------------------
CN=jeewan2,OU=1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-\
17-18-19-20-21-22-23-24-1,OU=1-2-3-4-5-6-7-8-9-10-11-\
12-13-14-15-16-17-18-19-20-21-22-23-24-0,OU=ou-01-11-1,\
DC=ucsm,DC=qasam-lab,DC=in
```

Step 4 In **TACACS+**, complete the following sections as required:

a) On the **Basic** tab, type values for the **Database Connection Timeout** and **Retry Count**.

b) On the **Providers** tab, click + to add a provider, and complete the necessary configuration information.

You can use the up and down arrows to change the order of the providers.

c) On the **Groups** tab, click + to add a provider group, and optionally associate it with a provider.

Step 5 In **RADIUS**, complete the following sections as required:

a) On the **Basic** tab, type values for the **Database Connection Timeout** and **Retry Count**.

b) On the **Providers** tab, click + to add a provider, and complete the necessary configuration information.

You can use the up and down arrows to change the order of the providers.

c) On the **Groups** tab, click + to add a provider group, and optionally associate it with a provider.

Step 6 In **Authentication Domains**, complete the following sections as required:

a) Click + to create an authentication policy for the domain group.

The policy overrides the settings inherited from its parent group. The maximum number of authentication domains supported in Cisco UCS Central is eight.

b) Enter the name of the authentication domain.

This name can be between 1 and 16 alphanumeric characters. For systems using LDAP, TACACS, and RADIUS, the authentication domain name is considered part of the username. It counts toward the 32 character limit for locally created usernames. Because Cisco UCS inserts 5 characters for formatting, authentication fails if the combined total of the domain name plus the username is more than 27 characters.

c) In **Web Session Refresh Period (Seconds)**, enter the maximum amount of time allowed between refresh requests for a user accessing a Cisco UCS domain included in the selected Cisco UCS Central domain group.

If this time limit is exceeded, Cisco UCS Central considers the web session to be inactive, but it does not terminate the session.

Specify an integer between 60 and 172800. The default is 600 seconds.

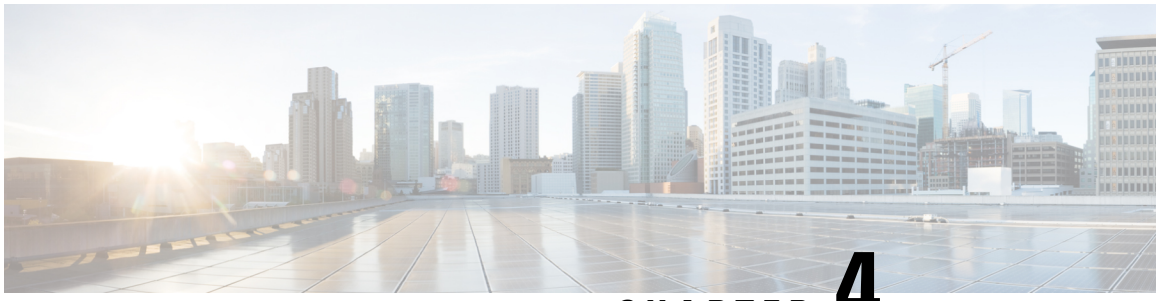
d) In **Web Session Timeout (Seconds)**, enter the maximum amount of time that can elapse before Cisco UCS Central ends the web session. If the web session exceeds the time limit, Cisco UCS Central automatically terminates the web session.

Specify an integer between 60 and 172800 seconds. The default is 7200 seconds.

e) Select the **Authentication Realm**:

- **LDAP**—Define users on the LDAP server specified in Cisco UCS Central.
- **Local**—Define users locally in Cisco UCS Central or the Cisco UCS domain.
- **RADIUS**—Define users on the RADIUS server specified in Cisco UCS Central.
- **TACACS+**—Define users on the TACACS+ server specified in Cisco UCS Central.

Step 7 Click **Save**.



CHAPTER 4

Remote Authentication

Guidelines and Recommendations for Remote Authentication Providers

If you configure a system 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, 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. You can view the temporary sessions for users who log in through remote authentication services 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, ensure that:

- Accounts include the roles those users require for working in Cisco UCS Central.
- Names of those roles match the names used in Cisco UCS Central.

Depending on the role policy, a user may not have permission to log in, or they may only have read-only privileges.

Local and Remote User Authentication Support

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

User Attributes in Remote Authentication Providers

When a user logs in, Cisco UCS Central:

1. Queries the remote authentication service.

2. Validates the user.
3. Checks for the roles and locales assigned to that user, (if user passed validation).

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

Table 3: Comparison of User Attributes by Remote Authentication Provider

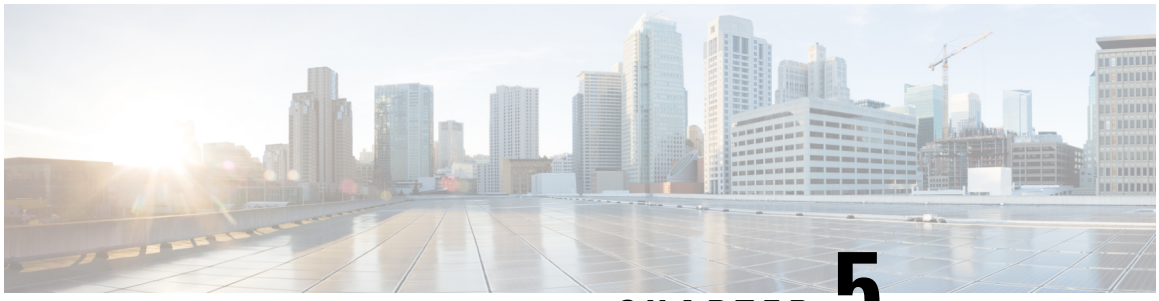
Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	Do one of the following: • Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements. • Extend the LDAP schema and create a custom attribute with a unique name, 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 The following section contains a sample OID (object identifier).
RADIUS	Optional	Do one of the following: • Do not extend the RADIUS schema and use an existing unused attribute that meets the requirements. • Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.	The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001. The following syntax example specifies 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.

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
TACACS+	Required	You must extend the schema and create a custom attribute with the name cisco-av-pair.	The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider. The following syntax example specifies 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.

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
```



CHAPTER 5

LDAP Authentication

LDAP Providers

Create and configure LDAP remote users, and assign roles and locales from Cisco UCS Central, in the same manner as Cisco UCS Manager. Always create the LDAP provider from the Cisco UCS Central domain group root.

LDAP Group Maps

You can define multiple LDAP group maps, and nest them up to as many levels as the Windows 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 an authenticated member of the parent nested group. During authentication, Cisco UCS Central tries all of the providers within a provider group in order. If Cisco UCS Central cannot reach all of the configured servers, it automatically falls back to the local authentication method using the local username and password.

The number of LDAP group maps you can define depends upon the version of Cisco UCS Manager. See Supported LDAP Group Maps, on page 28.

Provider Groups

A provider group is a set of providers that Cisco UCS uses 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 of 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.

LDAP Group Maps

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

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.

The number of LDAP group maps you can define depends upon the version of Cisco UCS Manager.

You can nest LDAP group maps up to as many levels as the Windows 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 an authenticated member of the parent nested group. During authentication, Cisco UCS Central tries all of the providers within a provider group in order. If Cisco UCS Central cannot reach all of the configured servers, it automatically falls back to the local authentication method using the local username and password.

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
- Roles and locales

For 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. You must create a custom locale to map an LDAP provider group to a locale.

Supported LDAP Group Maps

The number of supported LDAP group maps depends upon the version of Cisco UCS Manager:

Cisco UCS Manager Version	LDAP Group Maps Supported
Cisco UCS Manager Release 3.1(2) and later releases	160
Cisco UCS Manager Release 3.1(1)	128
Cisco UCS Manager Release 2.2(8) and later releases	160
Cisco UCS Manager Release 2.2(7) and previous releases	28

Nested LDAP Groups

You can nest LDAP groups as members of other groups to consolidate accounts and reduce replication.

By default, an LDAP group inherits user rights when nested 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.

You can search nested groups that are defined in LDAP group maps. Nesting groups eliminates the need to create subgroups.

Note Searching nested LDAP groups is supported for Microsoft Active Directory servers only. The supported versions are Microsoft Windows 2003 SP3, Microsoft Windows 2008 R2, and Microsoft Windows 2012.

If you include special characters in nested group names, make sure to escape them using the syntax shown in the following example.

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

Managing UCS Central LDAP Configuration

Procedure

Step 1 From the Actions bar, type **Managing UCS Central LDAP Configuration**.

This launches the **UCS Central LDAP Configuration Manage** dialog box.

Step 2 In **LDAP**, supply the information requested in these tabs.

a) On the **Basic** tab, type values for the **Database Connection Timeout**, **Filter**, **Attribute**, and **Base DN**.

b) On the **Providers** tab, click + to add a provider, and complete the necessary information in the **Basic** and **Group Rules** tabs.

Select **Enabled** or **Disabled** in the SSL section. If you select **Enabled**, encryption is required for communications with the LDAP database. When you enable SSL with LDAP configuration, the provider name must match the FQDN of the LDAP server certificate. If the provider name does not match the FQDN, authentication will fail. Enabling SSL LDAP uses STARTTLS which allows encrypted communication using port 389. If you check **Disabled**, authentication information will be sent as clear text.

c) On the **Groups** tab, click + to add a provider group, and optionally associate it with a provider.

d) On the **Group Maps** tab, enter a **Provider Group Map DN**. Optionally, add **Roles** and **Locales**.

Note Do not use special characters in the provider group map distinguished name.

Step 3 In **Authentication Domains**, configure, add, or delete Native or Console default domains.

Step 4 Click **Native (Default)** and take these steps.

a) Select the **Default Behavior for Remote Users**.

b) In **Web Session Refresh Period (Seconds)**, enter the maximum amount of time allowed between refresh requests.

If the web session exceeds the time limit, Cisco UCS Central considers the web session inactive, but it does not terminate the session.

Specify between 60 and 172800 seconds. The default is 600 seconds.

c) In **Web Session Timeout (Seconds)**, enter the maximum amount of time that can elapse after the last refresh request. If the web session exceeds the time limit, Cisco Cisco UCS Central considers the web session to have ended and automatically terminates the web session.

Specify between 60 and 172800 seconds. The default is 7200 seconds.

d) Choose **Enabled** or **Disabled** for **Authentication**.

e) If you selected **Enabled**, choose an **Authentication Realm**.

- **LDAP**—Define users on the LDAP server specified in Cisco UCS Central.
- **Local**—Define users locally in Cisco UCS Central or the Cisco UCS domain.
- **RADIUS**—Define users on the RADIUS server specified in Cisco UCS Central.
- **TACACS+**—Define users on the TACACS+ server specified in Cisco UCS Central.

f) If you selected **LDAP**, **RADIUS** or **TACACS**+, select an associated provider group from the **Provider Group** drop-down list.

Step 5 Click **Console (Default)**:

a) Choose **Enabled** or **Disabled** for **Authentication**.

b) If you selected **Enabled**, choose an **Authentication Realm**:

- **LDAP**—Define users on the LDAP server specified in Cisco UCS Central.
- **Local**—Define users locally in Cisco UCS Central or the Cisco UCS domain.
- **RADIUS**—Define users on the RADIUS server specified in Cisco UCS Central.
- **TACACS+**—Define users on the TACACS+ server specified in Cisco UCS Central.

c) If you selected **LDAP**, **RADIUS** or **TACACS**+, select an associated provider group from the **Provider Group** drop-down list.

Step 6 Click + to add a new authentication domain.

a) Enter the name of the authentication domain.

This name can be between 1 and 16 alphanumeric characters. Do not use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period). You cannot change this name once you save it.

For systems using LDAP, TACACS, and RADIUS, the authentication domain name is considered part of the user name. Therefore, it counts toward the 32 character limit for locally created user names. Because Cisco UCS reserves five characters for formatting, you cannot have a combined total of more than 27 characters for the domain name and user name.

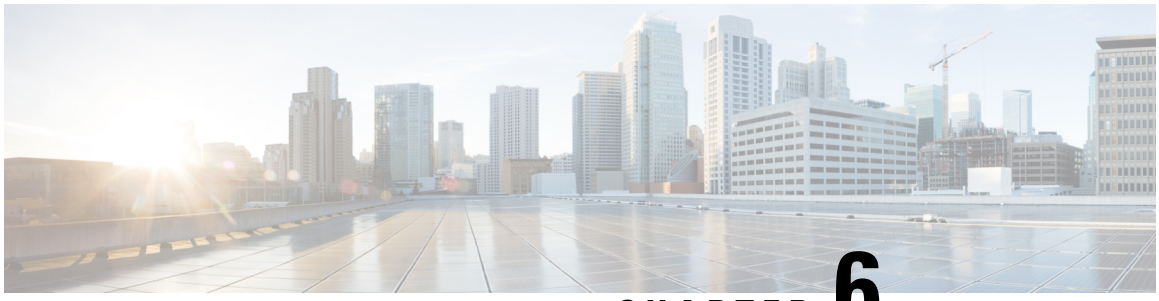
b) Enter the **Web Session Refresh Period (Seconds)**.

c) Enter the **Web Session Timeout (Seconds)**.

d) If you selected **LDAP**, **RADIUS** or **TACACS+**, select an associated provider group from the **Provider Group** drop-down list.

Step 7 Click **Save**.

After creating an authentication domain, you can edit the settings as necessary. You can also click the trash can to remove a selected authentication domain.



CHAPTER 6

SNMP Authentication

SNMP Policies

Cisco UCS Central supports:

- Global SNMP policies
- Defining SNMP traps and informs
- Defining SNMP users

You can define them 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 defer all SNMP policies to its registration with Cisco UCS Central.

The SNMP Agent functionality remotely monitors 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. The configuration persists 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:

SNMP Manager

System used to control and monitor the activities of network devices using SNMP.

SNMP Agent

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.

Managed Information Base (MIB)

Collection of managed objects in the SNMP agent. Cisco UCS Central supports only the OS MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the MIB Reference for Cisco UCS Manager for B-series servers, and MIB Reference for Cisco UCS Standalone C-Series Servers C-series servers.

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 the SNMP manager send the requests. 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 than Informs because the SNMP manager does not send any acknowledgment when it receives a trap. Therefore, Cisco UCS Central cannot determine if it received the trap.

An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If Cisco UCS Central does not receive the PDU, it can send the inform request again.

SNMP Security Features

SNMPv3 provides secure access to devices through 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 nothing has altered or destroyed any messages in an unauthorized manner. Also ensures that nothing has altered data sequences to an extent greater than can occur non-maliciously.

Message Origin Authentication

Confirms the claimed identity of the user who received the data.

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. A security model is an authentication strategy that is set up for a user and the role in which the user resides. The security model combines with the selected security level to determine the security mechanism applied when Cisco UCS Central processes the SNMP message.

The security level determines the privileges required to view the message associated with an SNMP trap. The security level determines whether Cisco UCS Central must protect the message from disclosure, or authenticate it. The supported security level depends upon which security model is implemented. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. 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.

SNMP Security Models and Levels

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

Table 4: 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: • Hash-based Message Authentication code (HMAC) • Message Digest 5 (MD5) algorithm • HMAC Secure Hash algorithm (SHA)
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on: • Hash-based Message Authentication code (HMAC) • Message Digest 5 (MD5) algorithm • HMAC Secure Hash algorithm (SHA) • Provides Data Encryption Standard (DES) 56-bit encryption. • Provides 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 and Cisco 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 uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security 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.

Enabling SNMP

Procedure

Step 1 Click the **System Configuration** icon and choose **SNMP**.

This launches the **UCS Central SNMP Manage** dialog box.

Step 2 On the **Basic** tab, select **Enabled** or **Disabled**. If you selected **Enabled**, complete the following fields.

a) In **Community/User Name**, enter the default SNMP v1 or v2c community name or SNMP v3 username.

b) In **System Contact**, enter the system contact person responsible for the SNMP implementation.

Enter a string of up to 255 characters, such as an email address or a name and telephone number.

c) In **System Location**, enter the location of the host on which the SNMP agent (server) runs.

Enter an alphanumeric string up to 510 characters.

Step 3 Click **Save**.

What to do next

Create SNMP traps and users.

Creating and Editing an SNMP Trap or Inform

After creating an SNMP trap, you can edit the SNMP trap information as required.

Procedure

Step 1 Click the **System Configuration** icon and choose **SNMP**.

This launches the **UCS Central SNMP Manage** dialog box.

Step 2 On the **SNMP Traps** tab, click **Add**.

Step 3 In **Trap Host Name/IP Address**, enter the IP address of the SNMP host to which to send the trap.

Step 4 In **SNMP Trap Properties**:

a) In **Community/User Name**, enter the default SNMP v1 or v2c community name or SNMP v3 username.

b) In **Port**, enter the port on which the system communicates with the SNMP host for the trap.

Enter an integer between 1 and 65535. The default port is 162.

c) For **Version**, select **V1**, **V2C**, or **V3**.

d) If you selected V2C or V3, then for **Type**, select **Traps** or **Informs**.

e) If you selected V3, then select the **V3Privilege**:

- **Auth**—Authentication but no encryption
- **NoAuth**—No authentication or encryption
- **Priv**—Authentication and encryption

Step 5 Click **Save**.

What to do next

Create an SNMP user.

Creating and Editing an SNMP User

After creating an SNMP user, you can edit the SNMP user information as required.

Procedure

Step 1 Click the **System Configuration** icon and choose **SNMP**.

This launches the **UCS Central SNMP Manage** dialog box.

Step 2 On the **SNMP Users** tab, click **Add**.

Step 3 In **SNMP User Name**, enter the username assigned to the SNMP user.

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).

Step 4 In **SNMP User Properties**:

a) In **Authentication Type**, select the **MD5** or **SHA** as the authorization type.
b) For **AES-128 Encryption**, click **Enabled** or **Disabled**.
c) Enter and confirm the **Password** and **Privacy Password**.

Step 5 Click **Save**.