Authentication

This chapter includes the following sections:

Authentication

From Cisco UCS Central you can configure LDAP, RADIUS, and TACACS+ for a registered UCS domain authentication.

Note Only LDAP can be used 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 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 Group Maps

You can define up to 28 LDAP provider group maps 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 the configured LDAP 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 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 a 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
- 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 capability, you need not 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.

Note When you create nested LDAP group in MS-AD, if you use special characters in the name, make sure to configure the characters with \\(, \\). Following is an example of creating a nested LDAP group using the 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 an LDAP group is 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.

Managing UCS Central Authentication

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

After creating an authentication domain, you can edit the authentication information as required.

Step 1 On the menu bar, click the **Operations** icon and select **Authentication**.
This launches **Manage Cisco UCS Central Authentication** dialog box.

Step 2 In **LDAP**, complete the appropriate fields for the **Basic**, **Providers**, **Groups**, and **Group Maps** tabs.

Step 3 In **Authentication Domains**, do the following:

Step 4 Click **Native(Default)** and complete the following information:

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

b) Enter values for the **Web Session Refresh Period(Seconds)** and **Web Session Timeout(Seconds)**.
c) Choose whether **Authentication** should be **Enabled** or **Disabled**.
d) If you selected **Enabled**, choose whether the **Authentication Realm** should be **Local** or **LDAP**.
e) If you selected **LDAP**, select a **Provider Group**.

Step 5 Click **Console(Default)** and complete the following information:

a) Choose whether **Authentication** should be **Enabled** or **Disabled**.
b) If you selected **Enabled**, choose whether the **Authentication Realm** should be **Local** or **LDAP**.
c) If you selected **LDAP**, select a **Provider Group**.

Step 6 Click **Add** to create 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), and you cannot change this name once you save it.

For systems using RADIUS as the preferred authentication protocol, the authentication domain name is considered part of the user name and counts toward the 32 character limit for locally created user names. 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 user name.

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 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 between 60 and 172800. 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 before Cisco Cisco UCS Central considers a web session to have ended. If this time limit is exceeded, Cisco UCS Central automatically terminates the web session.
Specify between 60 and 172800. The default is 7200 seconds.

d) Select the **Authentication Realm** applied to users in the domain. This can be one of the following:

- **LDAP—**The user must be defined on the LDAP server specified in Cisco UCS Central.
- **Local—**The user account must be defined locally in Cisco UCS Central or the Cisco UCS domain.

e) If the **Realm** is set to LDAP, you can select an associated provider group from the **Provider Group** drop-down list.

Step 7 Click **Save**.

Managing UCS Central LDAP Configuration

Step 1 In the Task bar, type **Create Domain Group** and press Enter.
This launches the **Create Domain Group** dialog box.

Step 2 In **LDAP**, complete the following sections as required:

a) On the **Basic** tab, type values for the **Database Conection Timeout**, **Filter**, **Attribute**, and **Base DN**.
b) On the **Providers** tab, click **Add** to add a provider, and complete the necessary information in the **Basic** and **Group Rules** tabs.
c) On the **Groups** tab, click **Add** to add a provider group, and optionally associate it with a provider.
d) On the **Group Maps** tab, add a **Provider Group Map DN**, and then optionally add **Roles** and **Locales**.

Step 3 In **Authentication Domains**, add a new domain and update the values.

Step 4 Click **Save**.

Managing Domain Group Authentication

Step 1 On the task bar, type **Manage Domain Group Authentication** and press **Enter**.
This launches the **Manage Domain Group Authentication** dialog box.

Step 2 In **LDAP**, complete the following sections as required:

a) On the **Basic** tab, type values for the **Database Conection Timeout**, **Filter**, **Attribute**, and **Base DN**.
b) On the **Providers** tab, click **Add** to add a provider, and complete the necessary information in the **Basic** and **Group Rules** tabs.
c) On the **Groups** tab, click **Add** to add a provider group, and optionally associate it with a provider.
d) On the **Group Maps** tab, add a **Provider Group Map DN**, and then optionally add **Roles** and **Locales**.

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

a) On the **Basic** tab, type values for the **Database Conection Timeout** and **Retry Count**.
b) On the **Providers** tab, click **Add** 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 **Add** 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 Conection Timeout** and **Retry Count**.
b) On the **Providers** tab, click **Add** 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 **Add** to add a provider group, and optionally associate it with a provider.

Step 5

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

a) Click **Add** to create an authentication policy for the selected user-created domain group that overrides the settings inherited from its parent group.
b) Enter the name of the authentication domain.
This name can be between 1 and 16 alphanumeric characters. For systems using RADIUS as their preferred authentication protocol, the authentication domain name is considered part of the user name and counts toward the 32 character limit for locally created user names. Because Cisco UCS inserts 5 characters for formatting, authentication will fail if the combined total of the domain name plus the user name 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 Manager 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 after the last refresh request before Cisco UCS Manager considers a web session to have ended. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session.
Specify an integer between 60 and 172800. The default is 7200 seconds.

e) Select the **Authentication Realm** that will be applied to users in the domain.
This can be one of the following:

- **LDAP—**The user must be defined on the LDAP server specified in Cisco UCS Central.
- **Local—**The user account must be defined locally in Cisco UCS Central or the Cisco UCS domain.
- **RADIUS—**The user must be defined on the RADIUS server specified in Cisco UCS Central.
- **TACACS+—**The user must be defined on the TACACS+ server specified in Cisco UCS Central.

Step 7 Click **Save**.

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.
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).

Model	Level	Authentication	Encryption	What Happens
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.

Related Topics

Enabling SNMP, on page 11
Creating and Editing an SNMP User, on page 12
Creating and Editing an SNMP Trap, on page 11

Enabling SNMP

Step 1 On the menu bar, click **Operations** icon, and select **SNMP**.

- You can select SNMP by typing **Manage UCS Central SNMP** on the **Task** bar and press **Enter**.

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

Step 2 In **Basic**, complete the following fields:

Step 3 In **Community/User Name**, enter the default SNMP v1 or v2c community name or SNMP v3 username.

Step 4 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.

Step 5 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 6 Click **Save**.

What to Do Next

Create SNMP traps and users.

Creating and Editing an SNMP Trap

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

Step 1 On the menu bar, click the **Operations** icon and select **SNMP**.

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

Step 2 In **Trap Host Name/IP Address**, enter the IP address of the SNMP host to where the trap should be sent.

Step 3 In **SNMP Trap Properties** area, complete the following:

Step 4 In **Community/User Name**, enter the SNMP v1 or v2c community name or the SNMP v3 username that the system includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service.
Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.

Step 5 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.

Step 6 Click **V1**, **V2C**, or **V3** to choose the SNMP Version.

Step 7 Click **Trap** to choose the SNMP trap **Type**.

Step 8 To define **V3Privilege**, choose one of the following:

Step 9 Click **Save**.

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

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.

Step 1 On the menu bar, click the **Operations** icon and select **SNMP**.
This launches **Manage UCS Central SNMP** dialog box.

Step 2 On the **Manage UCS Central SNMP** page, click **SNMP User**.

Step 3 Click the **Plus** sign to create SNMP user.

Step 4 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 5 In **SNMP User Properties**, complete the following:

Step 6 In **Authentication Type**, select the authorization type. This can be one of the following:

- **MDS**
- **SHA**

Step 7 Enable **AES-128 Encryption**. If enabled, this user uses AES-128 encryption.

Step 8 Enter the password for the user.

Step 9 Enter the privacy password for this user.

Step 10 Click **Save**.