LDAP Authentication

- LDAP Providers, on page 1
- Managing UCS Central LDAP Configuration, on page 3

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 2.

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.