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**.