Remote Authentication

Authentication Services

Cisco UCS supports the following two methods to authenticate user logins:

- Local user authentication - uses user accounts that exist locally in the Cisco UCS Manager
- Remote user authentication - uses one of the following protocols:
  - LDAP
  - RADIUS
  - TACACS+

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 Manager can communicate with the system. The following guidelines impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in Cisco UCS Manager or in the remote authentication server.

You can view the temporary sessions for users who log in through remote authentication services from the Cisco UCS Manager GUI and from the Cisco UCS Manager 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 Manager and that the names of those roles match the names used in Cisco UCS Manager. Based on the role policy, a user might not be allowed to log in, or is granted only read-only privileges.

User Attributes in Remote Authentication Providers

For RADIUS and TACACS+ configurations, you must configure a user attribute for Cisco UCS in each remote authentication provider through which users log in to Cisco UCS Manager. This user attribute holds the roles and locales assigned to each user.

Note This step is not required for LDAP configurations that use the LDAP Group Mapping to assign roles and locales.

When a user logs in, Cisco UCS Manager 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.

Table 1: Comparison of User Attributes by Remote Authentication Provider

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Not required if group mapping is used Optional if group mapping is not used	Optional. You can choose to 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 A sample OID is provided in the following section.

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
RADIUS	Optional	Optional. You can choose to 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 shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute: `shell:roles="admin,aaa" shell:locales="L1,abc"`. Use a comma "," as the delimiter to separate multiple values.
TACACS+	Required	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 shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`. Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values.

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
```

Two-Factor Authentication

Cisco UCS Manager uses two-factor authentication for remote user logins, which adds a level of security to account logins. Two-factor authentication login requires a username, a token, and a password combination in the password field. You can provide a PIN, a certificate, or a token.

Two-factor authentication uses authentication applications that maintain token servers to generate one-time tokens for users during the login process and store passwords in the AAA server. Requests are sent to the token server to retrieve a vendor-specific attribute. Cisco UCS Manager expects the token server to integrate with the AAA server, therefore it forwards the request to the AAA server. The password and token are validated at the same time by the AAA server. Users must enter the token and password sequence in the same order as it is configured in the AAA server.

Two-factor authentication is supported by associating RADIUS or TACACS+ provider groups with designated authentication domains and enabling two-factor authentication for those domains. Two-factor authentication does not support IPM and is not supported when the authentication realm is set to LDAP, local, or none.

Web Session Refresh and Web Session Timeout Period

The **Web Session Refresh Period** is the maximum amount of time allowed between refresh requests for a Cisco UCS Manager GUI web session. The **Web Session Timeout** is the maximum amount of time that can elapse after the last cookie/token refresh request has failed before a Cisco UCS Manager GUI web session becomes inactive.

You can increase the **Web Session Refresh Period** to a value greater than 60 seconds up 172800 seconds to avoid frequent session timeouts that requires regenerating and re-entering a token and password multiple times. The default value is 7200 seconds when two-factor authentication is enabled, and is 600 seconds when two-factor authentication is not enabled.

You can specify a value between 300 and 172800 for the **Web Session Timeout Period**. The default is 8000 seconds when two-factor authentication is enabled, and 7200 seconds when two-factor authentication is not enabled.

LDAP Providers and Groups

Nested LDAP Groups

You can add an LDAP group as a member of another group and nest groups to consolidate member accounts and to reduce the replication of traffic. Cisco UCS Manager release 2.1(2) and higher enables you to search LDAP groups that are nested within another group defined in an LDAP group map.

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.

By default, user rights are inherited when you nest an LDAP group within another group. For example, if you make Group_1 a member of Group_2, the users in Group_1 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 do not always need to create subgroups in a group map in Cisco UCS Manager.

LDAP Group Rule

The LDAP group rule determines whether Cisco UCS should use LDAP groups when assigning user roles and locales to a remote user.

Configuring Properties for LDAP Providers

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

Before you begin

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with Cisco UCS. Give this account a non-expiring password.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 In the **Properties** area, complete all fields.

Note User login fails if the userDn for an LDAP user exceeds 255 characters.

Step 4 Click **Save Changes**.

What to do next

Create an LDAP provider.

Creating an LDAP Provider

Cisco UCS Manager supports a maximum of 16 LDAP providers.

Before you begin

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with Cisco UCS. Give this account a non-expiring password.

- In the LDAP server, perform one of the following configurations:
  - Configure LDAP groups. LDAP groups contain user role and locale information.

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

  The Cisco LDAP implementation requires a unicode type attribute.

  If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1

- For a cluster configuration, add the management port IPv4 or IPv6 addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IPv4 or IPv6 address used by Cisco UCS Manager.

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

- If you need to change the LDAP providers or add or delete them, change the authentication realm for the domain to local, make the changes to the providers, then change the domain authentication realm back to LDAP.

Attention LDAP remote usernames that include special characters cannot log in to systems that are running versions 2.2(3a) and later. The user cannot log in because of the Nexus OS limitations where special characters, !,%,^, are not supported in the username.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Create LDAP Provider**.

Step 5 On the **Create LDAP Provider** page of the wizard, complete all fields with appropriate LDAP service information.

a) Complete the following fields with information about the LDAP service you want to use:

Name	Description
Hostname/FDQN (or IP Address) field	The hostname, or IPv4 or IPv6 address on which the LDAP provider resides. If SSL is enabled, this field must exactly match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Order field	The order that the Cisco UCS uses this provider to authenticate users. Enter an integer between 1 and 16, or enter `lowest-available` or `0` (zero) if you want Cisco UCS to assign the next available order based on the other providers defined in this Cisco UCS domain.
Bind DN field	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 255 ASCII characters.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server begins a search when a remote user logs in and the system attempts to obtain the user's DN based on their username. You can set the length of the base DN to a maximum of 255 characters minus the length of CN=username, where username identifies the remote user attempting to access Cisco UCS Manager using LDAP authentication. This value is required unless a default base DN has been set on the LDAP **General** tab.
Port field	The port through which Cisco UCS communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	If checked, encryption is required for communications with the LDAP database. If unchecked, authentication information will be sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389. If checked, do not change the port to 636, leave it as 389. Cisco UCS negotiates a TLS session on port 636 for SSL, but initial connection starts unencrypted on 389.
Filter field	The LDAP search is restricted to those user names that match the defined filter. This value is required unless a default filter has been set on the LDAP **General** tab.

Name	Description
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: `1.3.6.1.4.1.9.287247.1` This value is required unless a default attribute has been set on the LDAP **General** tab.
Password field	The password for the LDAP database account specified in the **Bind DN** field. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
Confirm Password field	The LDAP database password repeated for confirmation purposes.
Timeout field	The length of time in seconds the system spends trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the LDAP **General** tab. The default is 30 seconds.
Vendor radio button	The LDAP vendor that you want to use. This can be one of the following: • Open Ldap—The open source implementation of the LDAP protocol. • MS AD—Microsoft Active Directory.

b) Click **Next**.

Step 6 On the **LDAP Group Rule** page of the wizard, complete all fields with appropriate LDAP group rule information.

Note Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.

What to do next

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

For implementations involving multiple LDAP databases, configure an LDAP provider group.

Changing the LDAP Group Rule for an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Expand **LDAP Providers** and choose the LDAP provider for which you want to change the group rule.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **LDAP Group Rules** area, complete the following fields:

Name	Description
Group Authorization field	Whether Cisco UCS also searches LDAP groups when authenticating and assigning user roles and locales to remote users. This can be one of the following: • **Disable**—Cisco UCS does not access any LDAP groups. • **Enable**—Cisco UCS searches all LDAP groups mapped in this Cisco UCS domain. If the remote user is found, Cisco UCS assigns the user roles and locales defined for that LDAP group in the associated LDAP group map. **Note** Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.
Group Recursion field	Whether Cisco UCS searches both the mapped groups and their parent groups. This can be one of the following: • **Non Recursive**—Cisco UCS searches only the groups mapped in this Cisco UCS domain. If none of the groups containing the user explicitly set the user's authorization properties, Cisco UCS uses the default settings. • **Recursive**—Cisco UCS searches each mapped group and all its parent groups for the user's authorization properties. These properties are cumulative, so for each group Cisco UCS finds with explicit authorization property settings, it applies those settings to the current user. Otherwise it uses the default settings.
Target Attribute field	The attribute Cisco UCS uses to determine group membership in the LDAP database. The supported string length is 63 characters. The default string is `memberOf`.

Name	Description
Use Primary Group field	The attribute Cisco UCS uses to determine if the primary group can be configured as an LDAP group map for membership validation. With this option Cisco UCS Manager can download and verify the primary-group membership of the user.

Step 6 Click **Save Changes**.

Deleting an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Expand **LDAP Providers**.

Step 4 Right-click the LDAP provider that you want to delete and choose **Delete**.

Step 5 If a confirmation dialog box displays, click **Yes**.

LDAP Group Mapping

LDAP group mapping eliminates having to define role or locale information in the LDAP user object. UCSM can use group membership information to assign a role or locale to an LDAP user during login for organizations using LDAP groups to restrict access to LDAP databases.

When a user logs in to Cisco UCS Manager, the LDAP group map pulls information about the user's role and locale. If the role and locale criteria match the information in the policy, access is granted. Cisco UCS Manager supports a maximum of 28, 128, or 160 LDAP group maps depending on the release version.

Note Cisco UCS Manager Release 3.1(1) supports a maximum of 128 LDAP group maps, and Release 3.1(2) and later releases support a maximum of 160 LDAP group maps.

The role and locale definitions that you configure locally in the Cisco UCS Manager do not update automatically based on changes to an LDAP directory. When deleting or renaming LDAP groups in an LDAP directory, you must also update the Cisco UCS Manager with the change.

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

- Roles only
- Locales only
- Both roles and locales

For example, consider an LDAP group representing a group of server administrators at a specific location. The LDAP group map might include user roles such as server profile and server equipment. To restrict access to server administrators at a specific location, you can set the locale to a particular site name.

Note Cisco UCS Manager includes out-of-the-box user roles, but does not include any locales. Mapping an LDAP provider group to a locale requires that you create a custom locale.

Creating an LDAP Group Map

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Right-click **LDAP Group Maps** and choose **Create LDAP Group Map**.

Step 4 In the **Create LDAP Group Map** dialog box, specify all LDAP group map information, as appropriate.

Important The name that you specify in the **LDAP Group DN** field must match the name in the LDAP database.

Note If you use a special character in the **LDAP Group DN** field, you must prefix the special character with an escape character \ (single back slash).

What to do next

Set the LDAP group rule.

Deleting an LDAP Group Map

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Expand **LDAP Group Maps**.

Step 4 Right-click the LDAP group map that you want to delete and choose **Delete**.

Step 5 If a confirmation dialog box displays, click **Yes**.

RADIUS Providers

Configuring Properties for RADIUS Providers

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

Note RADIUS authentication uses Password Authentication Protocol (PAP).

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Choose**User Management** > **RADIUS**.

Step 3 In the **Properties** area, complete all fields.

Step 4 Click **Save Changes**.

What to do next

Create a RADIUS provider.

Creating a RADIUS Provider

Cisco UCS Manager supports a maximum of 16 RADIUS providers.

Before you begin

Perform the following configuration in the RADIUS server:

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

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

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

- For a cluster configuration, add the management port IPv4 or IPv6 addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **RADIUS**.

Step 3 In the **Create RADIUS Provider** dialog box, specify all appropriate RADIUS service information.

Note If you use a hostname rather than an IPv4 or IPv6 address, you must ensure that a DNS server is configured for the hostname.

Step 4 Click **Save Changes**.

What to do next

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

For implementations involving multiple RADIUS databases, configure a RADIUS provider group.

Deleting a RADIUS Provider

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Choose**User Management** > **RADIUS**.

Step 3 Right-click the RADIUS provider that you want to delete and choose **Delete**.

Step 4 If a confirmation dialog box displays, click **Yes**.

TACACS+ Providers

Configuring Properties for TACACS+ Providers

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

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Choose**User Management** > **TACACS+**.

Step 3 In the **Properties** area, complete the **Timeout** field.

Step 4 Click **Save Changes**.

What to do next

Create a TACACS+ provider.

Creating a TACACS+ Provider

Cisco UCS Manager supports a maximum of 16 TACACS+ providers.

Before you begin

Perform the following configuration in the TACACS+ server:

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

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

  The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`. Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values.

- For a cluster configuration, add the management port IPv4 or IPv6 addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **TACACS+**.

Step 3 In the **Actions** area of the **General** tab, click **Create TACACS+ Provider**.

Step 4 In the **Create TACACS+ Provider** dialog box:

a) Complete all fields with TACACS+ service information, as appropriate.

Note If you use a hostname rather than an IPv4 or IPv6 address, you must ensure a DNS server is configured for the hostname.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to do next

For implementations involving a single TACACS+ database, select TACACS+ as the primary authentication service.

For implementations involving multiple TACACS+ databases, configure a TACACS+ provider group.

Deleting a TACACS+ Provider

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Choose**User Management** > **TACACS+**.
Step 3 Right-click the TACACS+ provider that you want to delete and choose **Delete**.
Step 4 If a confirmation dialog box displays, click **Yes**.

Primary Authentication Service

Selecting the Console Authentication Service

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **Authentication**.
Step 3 Click **Native Authentication**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Console Authentication** area, complete the following fields:

Name	Description
Realm field	The method by which a user logging into the console is authenticated. This can be one of the following: • **Local**—The user account must be defined locally in this Cisco UCS domain. • **Radius**—The user must be defined on the RADIUS server specified for this Cisco UCS domain. • **Tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS domain. • **Ldap**—The user must be defined on the LDAP server specified for this Cisco UCS domain. • **None**—If the user account is local to this Cisco UCS domain, no password is required when the user logs into the console.
Provider Group drop-down list	The provider group to be used to authenticate a user logging into the console. **Note** The**Provider Group** drop-down list is displayed when you select Ldap, Radius, or Tacacs as the method by which a user is authenticated.
Two Factor Authentication	Two-factor authentication is available only when the **Realm** is set to **Radius** or **Tacacs**. When this checkbox is selected, the Console requires users whose accounts are authenticated by Radius or Tacacs servers to enter a token plus a password to log in.

Step 6 Click **Save Changes**.

Selecting the Default Authentication Service

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **Authentication**.

Step 3 Click **Native Authentication**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Default Authentication** area, complete the following fields:

Name	Description
Realm drop-down list	The default method by which a user is authenticated during remote login. This can be one of the following: • **Local**—The user account must be defined locally in this Cisco UCS domain. • **Radius**—The user account must be defined on the RADIUS server specified for this Cisco UCS domain. • **Tacacs**—The user account must be defined on the TACACS+ server specified for this Cisco UCS domain. • **Ldap**—The user account must be defined on the LDAP server specified for this Cisco UCS domain. • **None**—If the user account is local to this Cisco UCS domain, no password is required when the user logs in remotely.
Provider Group drop-down list	The default provider group to be used to authenticate the user during remote login. **Note** The **Provider Group** drop-down is displayed when you select Ldap, Radius, or Tacacs as the method by which a user is authenticated.
Web Session Refresh Period (sec)	When a web client connects to Cisco UCS Manager, the client must send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Manager considers the web session inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds when Two-Factor Authentication is not enabled and 7200 seconds when it is enabled.
Web Session Timeout (sec)	The maximum amount of time that can elapse after the last cookie/token refresh request has failed before Cisco UCS Manager considers a web session as inactive. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session. Specify an integer between 300 and 172800. The default is 7200 seconds when Two-Factor Authentication is not enabled and 8000 seconds when it is enabled.

Name	Description
Two Factor Authentication checkbox	Two-Factor Authentication is available only when the **Realm** is set to **Radius** or **Tacacs**. When you select this check box, Cisco UCS Manager and the KVM launch manager require users whose accounts are authenticated by Radius or Tacacs servers to enter a token plus a password to log in. When 60 seconds remain for the **Web Session Refresh Period** to expire, users must generate a new token and enter the token plus their password to continue the session. **Note** After you enable two factor authentication and save the configuration, the default **Web Session Refresh Period (sec)** changes to 7200, and the default **Web Session Timeout (sec)** changes to 8000.

Step 6 Click **Save Changes**.

Role Policy for Remote Users

By default, if user roles are not configured in Cisco UCS Manager read-only access is granted to all users logging in to Cisco UCS Manager from a remote server using the LDAP, RADIUS, or TACACS protocols. For security reasons, it might be desirable to restrict access to those users matching an established user role in Cisco UCS Manager.

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

assign-default-role

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

This is the default behavior.

no-login

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

Configuring the Role Policy for Remote Users

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **Authentication**.

Step 3 Click **Native Authentication**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Role Policy for Remote Users** field, click one of the following radio buttons to determine what happens when a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information:

- **No Login**—The user is not allowed to log in to the system, even if the username and password are correct.
- **Assign Default Role**—The user is allowed to log in with a read-only user role.

Step 6 Click **Save Changes**.

Multiple Authentication Services Configuration

Multiple Authentication Services

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

- Provider groups
- Authentication domains

Provider Groups

A provider group is a set of providers that the Cisco UCS accesses during the authentication process. All of the providers within a provider group are accessed in the order that the Cisco UCS provider uses to authenticate users. If all of the configured servers are unavailable or unreachable, Cisco UCS Manager automatically falls back to the local authentication method using the local username and password.

Cisco UCS Manager allows you to create a maximum of 16 provider groups, with a maximum of eight providers allowed per group.

Creating an LDAP Provider Group

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

Before you begin

Create one or more LDAP providers.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Right-click **LDAP Provider Groups** and choose **Create LDAP Provider Group**.

Note If you use a hostname rather than an IPv4 or IPv6 address, you must ensure a DNS server is configured for the hostname.

Step 4 In the **Create LDAP Provider Group** dialog box, specify all of the appropriate LDAP provider group information.

What to do next

Configure an authentication domain or select a default authentication service.

Deleting an LDAP Provider Group

Before you begin

Remove the provider group from an authentication configuration.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **LDAP**.
Step 3 Expand **LDAP Provider Groups**.
Step 4 Right-click the LDAP provider group that you want to delete and choose **Delete**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Creating a RADIUS Provider Group

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

Before you begin

Create one or more RADIUS providers.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **RADIUS**.
Step 3 Right-click **RADIUS Provider Groups** and choose **Create RADIUS Provider Group**.
Step 4 In the **Create RADIUS Provider Group** dialog box, do the following:
a) In the **Name** field, enter a unique name for the group.

This name can be between 1 and 127 ASCII characters.

b) In the **RADIUS Providers** table, choose one or more providers to include in the group.
c) Click the >> button to add the providers to the **Included Providers** table.

You can use the << button to remove providers from the group.

d) (Optional) Use the **Move Up** or **Move Down** arrows in the **Included Providers** list to change the order in which the RADIUS providers authenticate providers.
e) After you add all of the required providers to the provider group, click **OK**.

What to do next

Configure an authentication domain or select a default authentication service.

Deleting a RADIUS Provider Group

You cannot delete a provider group if another authentication configuration is using that provider group.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **RADIUS**.
Step 3 Expand **RADIUS Provider Groups**.
Step 4 Right-click the RADIUS provider group you want to delete and choose **Delete**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Creating a TACACS+ Provider Group

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

Before you begin

Create one or more TACACS+ providers.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **TACACS+**.
Step 3 Right-click **TACACS+ Provider Groups** and choose **Create TACACS+ Provider Group**.
Step 4 In the **Create TACACS+ Provider Group** dialog box, specify all TACACS+ provider group information, as appropriate.

Deleting a TACACS+ Provider Group

You cannot delete a provider group if another authentication configuration is using that provider group.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **TACACS+**.

Step 3 Expand **TACACS+ Provider Groups**.

Step 4 Right-click the TACACS+ provider group that you want to delete and choose **Delete**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Authentication Domains

The Cisco UCS Manager uses Authentication Domains to leverage multiple authentication systems. You can specify and configure each authentication domain during login; otherwise, Cisco UCS Manager uses the default authentication service configuration.

You can create up to eight authentication domains. Each authentication domain is associated with a provider group and a realm in the Cisco UCS Manager. The Cisco UCS Manager uses all servers within the realm if you do not specify a provider group.

Creating an Authentication Domain

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **Authentication**.

Step 3 Right-click **Authentication Domains** and choose **Create a Domain**.

Step 4 In the **Create a Domain** dialog box, complete the following fields:

Name	Description
Name	The name of the domain. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), and . (period), and you cannot change this name after the object is saved. **Note** For systems using the remote authentication protocol, the authentication domain name is considered part of the username and counts toward the 32-character limit for locally created usernames. Because Cisco UCS inserts 5 characters for formatting, authentication fails if the domain name and username combined characters total exceeds 27.

Name	Description
Web Session Refresh Period (sec)	When a web client connects to Cisco UCS Manager, the client must send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Manager considers the web session inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds when Two-Factor Authentication is not enabled and 7200 seconds when it is enabled. **Note** The number of seconds set for the **Web Session Refresh Period** must be less than the number of seconds set for the **Web Session Timeout**. Do not set the **Web Session Refresh Period** to the same value as the **Web Session Timeout**.
Web Session Timeout (sec)	The maximum amount of time that can elapse after the last cookie/token refresh request has failed before Cisco UCS Manager considers a web session as inactive. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session. Specify an integer between 300 and 172800. The default is 7200 seconds when Two-Factor Authentication is not enabled and 8000 seconds when it is enabled.
Realm	The authentication protocol to apply to users in this domain. This can be one of the following: • **Local**—The user account must be defined locally in this Cisco UCS domain. • **Radius**—The user must be defined on the RADIUS server specified for this Cisco UCS domain. • **Tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS domain. • **Ldap**—The user must be defined on the LDAP server specified for this Cisco UCS domain.
Provider Group	The default provider group to use to authenticate users during remote login. **Note** The **Provider Group** drop-down list displays when you select Ldap Radius, or Tacacs as the method to authenticate users.

Name	Description
Two Factor Authentication	Two-Factor Authentication is available only when the **Realm** is set to **Radius** or **Tacacs**. When you select this check box, Cisco UCS Manager and the KVM launch manager require users whose accounts are authenticated by Radius or Tacacs servers to enter a token plus a password to log in. When 60 seconds remain for the **Web Session Refresh Period** to expire, users must generate a new token and enter the token plus their password to continue the session.

Step 5 Click **OK**.