Configuring Authentication

This chapter includes the following sections:

Authentication Services

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.

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 will be 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 Group Rule

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

Configuring LDAP Providers

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 Central. 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. This account should be given a non-expiring password.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Providers**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **LDAP** to access that option.

a) In the **Properties (LDAP)** dialog box, complete all fields on the **General** tab.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds. The default value is 30 seconds. This property is required.
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
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters. This property is required. If you do not specify a base DN on this tab then you must specify one on the **General** tab for every LDAP provider defined in this Cisco UCS domain.
Filter field	The LDAP search is restricted to those usernames that match the defined filter. This property is required. If you do not specify a filter on this tab then you must specify one on the **General** tab for every LDAP provider defined in this Cisco UCS domain.

b) Click **OK**.

Step 7 Click **Save**.

Creating an LDAP Provider

Cisco UCS Central 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. This account should be given 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 Central. 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 IP 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 Central.
- 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 Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Providers**.

Step 6 In the **Actions** area, click **Create LDAP Provider** and complete all fields.
You can also right-click **Providers** to access that option.

a) In the **Create LDAP Provider** dialog box, complete all **Properties** fields on the **General** tab.

Name	Description
Hostname field	The hostname or IP address on which the LDAP provider resides. **Note** If you use a hostname rather than an IP 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 in which Cisco UCS uses this LDAP provider to authenticate users.
Timeout field	The length of time in seconds the system should spend 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.
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 127 ASCII characters.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters. 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.
Filter field	The LDAP search is restricted to those usernames 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.

b) In the **Create LDAP Provider** dialog box, complete all **LDAP Group Rules** fields on the **General** tab.

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 Cisco UCS Central. 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.

Name	Description
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 Cisco UCS Central. 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.

c) Click **OK**.

Step 7 Click **Save**.

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 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Providers**.

Step 6 In the **Work** pane, click an **LDAP Provider**.

Step 7 In the **Actions** area, click **Properties**.
You can also right-click the **LDAP Provider** to access that option.

a) In the **Properties** dialog box, complete all **Properties** fields on the **General** tab.

Name	Description
Hostname field	The hostname or IP address on which the LDAP provider resides. **Note** If you use a hostname rather than an IP 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 in which Cisco UCS uses this LDAP provider to authenticate users.
Timeout field	The length of time in seconds the system should spend 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.
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 127 ASCII characters.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters. 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.

Name	Description
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.
Filter field	The LDAP search is restricted to those usernames that match the defined filter. This value is required unless a default filter has been set on the LDAP **General** tab.
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.

b) In the **Properties** dialog box, complete all **LDAP Group Rules** fields on the **General** tab.

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 Cisco UCS Central. 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.

Name	Description
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 Cisco UCS Central. 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.

c) Click **OK**.

Step 8 Click **Save**.

Deleting an LDAP Provider

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Providers**.

Step 6 In the **Work** pane, click the LDAP provider you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **LDAP Provider** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

LDAP Group Mapping

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 locale information in the LDAP user object when Cisco UCS Central is deployed.

Note LDAP group mapping is not supported for Cisco UCS Central for this release. However, LDAP group maps are supported for locally managed Cisco UCS domains from the Cisco UCS Central Domain Group root.

When a user logs in to Cisco UCS Central, information about the user's role and locale are pulled from the LDAP group map. If the role and locale criteria match the information in the policy, access is granted.

Role and locale definitions are configured locally in Cisco UCS Central and do not update automatically based on changes to an LDAP directory. When deleting or renaming LDAP groups in an LDAP directory, it is important that you update Cisco UCS Central with the change.

An LDAP group map can be configured 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 be configured to include user roles like server-profile and server-equipment. To restrict access to server administrators at a specific location, the locale could be set to a particular site name.

Note Cisco UCS Central includes many 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 Central (optional).
- Create custom roles in Cisco UCS Central (optional).

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Group Maps**.

Step 6 In the **Actions** area, click **Create LDAP Group Map** and complete all fields.
You can also right-click **Group Maps** to access that option.

a) In the **Create LDAP Group Map** dialog box, complete all fields on the **General** tab.

Name	Description
LDAP Group DN field	The distinguished name of the group in the LDAP database. **Important** This name must match the name in the LDAP database exactly.
Roles table	A list of the user roles defined in the selected Cisco UCS Central domain group and all of its parent groups. If the associated check box is checked, users in this LDAP group will be assigned that user role.
Locales table	A list of the user locales defined in the selected Cisco UCS Central domain group and all of its parent groups. If the associated check box is checked, users in this LDAP group will be assigned that locale.

b) Click **OK**.

What to Do Next

Set the LDAP group rule.

Deleting an LDAP Group Map

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Group Maps**.

Step 6 In the **Work** pane, click the group map you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **Group Map** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring 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 Central. If an individual provider includes a setting for any of these properties, Cisco UCS Central uses that setting and ignores the default setting.

Note RADIUS native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central under the Domain Group root and domain groups. RADIUS may be used to create global policies for Cisco UCS domains.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, click **RADIUS**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **RADIUS** to access that option.

a) In the **Properties (RADIUS)** dialog box, complete all fields on the **General** tab.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the RADIUS database before it times out. Enter an integer from 1 to 60 seconds. The default value is 5 seconds. This property is required.
Retries field	The number of times to retry the connection before the request is considered to have failed. Enter an integer between 0 and 5. The default value is 1. This property is required.

b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Create a RADIUS provider.

Creating a RADIUS Provider

Cisco UCS Central supports a maximum of 16 RADIUS providers. RADIUS native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central under the Domain Group root and domain groups. RADIUS may be used to create global policies for Cisco UCS domains.

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 Central. 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 IP 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 Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Actions** area, click **Create RADIUS Provider** and complete all fields.
You can also right-click **Providers** to access that option.

a) In the **Create RADIUS Provider** dialog box, complete all fields on the **General** tab.

Name	Description
Hostname field	The hostname or IP address on which the RADIUS provider resides. **Note** If you use a hostname rather than an IP 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 in which Cisco UCS uses this RADIUS provider to authenticate users.
Key field	The SSL encryption key for the database.
Set field	Whether the SSL key is active.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.
Authorization Port field	The port through which Cisco UCS communicates with the RADIUS database.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the RADIUS 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 RADIUS **General** tab. The default is 5 seconds.
Retries field	The number of times to retry the connection before the request is considered to have failed. If desired, enter an integer between 0 and 5. If you do not specify a value, Cisco UCS uses the value specified on the RADIUS **General** tab.

b) Click **OK**.

Step 7 Click **Save**.

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 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Work** pane, click the **RADIUS Provider** you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **RADIUS Provider** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring TACACS+ Providers

Configuring Properties for TACACS+ Providers

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

Note TACACS+ native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central. TACACS+ may be used to create global policies for Cisco UCS domains.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, click **TACACS+**.

Step 6 In the **Actions** area, click **Properties**.
You can also right-click **TACACS+** to access that option.

a) In the **Properties (TACACS+)** dialog box, complete all fields on the **General** tab.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the TACACS+ database before it times out. Enter an integer from 1 to 60 seconds. The default value is 5 seconds. This property is required.

b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Create an TACACS+ provider.

Creating a TACACS+ Provider

Cisco UCS Central supports a maximum of 16 TACACS+ providers. TACACS+ native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central. TACACS+ may be used to create global policies for Cisco UCS domains.

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 IP 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 Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** and click **Providers**.

Step 6 In the **Actions** area, click **Create TACACS+ Provider** and complete all fields.
You can also right-click **Providers** to access that option.

a) In the **Create TACACS+ Provider** dialog box, complete all fields on the **General** tab.

Name	Description
Hostname field	The hostname or IP address on which the TACAS+ provider resides. **Note** If you use a hostname rather than an IP 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 in which Cisco UCS uses this TACAS+ provider to authenticate users.
Key field	The SSL encryption key for the database.
Set field	Whether the SSL key is active.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.
Port field	The port through which Cisco UCS should communicate with the TACACS+ database. Enter an integer between 1 and 65535. The default port is 49.
Timeout field	The length of time in seconds the system should spend trying to contact the TACACS+ 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 TACACS+ **General** tab. The default is 5 seconds.
Retries field	The number of times to retry the connection before the request is considered to have failed. Enter an integer between 0 and 5. The default value is 1.

b) Click **OK**.

Step 7 Click **Save**.

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 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** > **Providers**.

Step 6 In the **Work** pane, click the TACACS+ provider you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **TACACS+ Provider** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring Multiple Authentication Systems

Multiple Authentication Systems

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

- Provider groups
- Authentication domains

Once provider groups and authentication domains have been configured in Cisco UCS Central GUI, the following syntax can be used to log in to the system using Cisco UCS Central CLI: **ucs-** *auth-domain*

When multiple authentication domains and native authentication are configured with a remote authentication service, use one of the following syntax examples to log in with SSH or Putty:

From a Linux terminal:

- **ssh ucs-***auth-domain**username*@*Cisco UCS domain-ip-address*

```
ssh ucs-example\\jsmith@192.0.20.11
```

- **ssh -l ucs-***auth-domain**username* {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*}

```
ssh -l ucs-example\\jsmith 192.0.20.11
```

- **ssh** {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*} **-l ucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
```

From a Putty client:

- Login as: **ucs-***auth-domain**username*

```
Login as: ucs-example\\jsmith
```

From a SSH client:

- Host Name: *Cisco UCS domain-ip-address*

  User Name: **ucs-***auth-domain**username*

```
Host Name: 192.0.20.11
User Name: ucs-example\\jsmith
```

Provider Groups

A provider group is a set of providers that will be used by Cisco UCS 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 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.

Creating an LDAP Provider Group

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

Note Authenticating with a single LDAP database does not require you to set up an LDAP provider group.

Before You Begin

Create one or more LDAP providers.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Provider Groups**.

Step 6 In the **Actions** area, click **Create LDAP Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create LDAP Provider Group** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	The name of the LDAP provider group.
Available Providers list box	The available LDAP providers that you can add to the LDAP group. You can use Shift+Click and Ctrl+Click to select multiple providers.
>> button	Adds all available providers to the group regardless of what providers are selected in the **Available Providers** list box.
> button	Adds the providers selected in the **Available Providers** list box to the group.
< button	Removes the providers selected in the **Assigned Providers** list box from the group.
<< button	Removes all providers from the group regardless of what providers are selected in the **Assigned Providers** list box.
Assigned Providers list box	The LDAP providers that are included in the LDAP group. Cisco UCS searches the providers in the order that they appear in the table. To change the provider priority, select a provider and use the arrow buttons above the list to move the provider to the desired position.

b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

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

Deleting an LDAP Provider Group

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Provider Groups**.

Step 6 In the **Work** pane, click the LDAP provider group you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **LDAP Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a RADIUS Provider Group

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

Note Authenticating with a single RADIUS database does not require you to set up a RADIUS provider group.

Before You Begin

Create one or more RADIUS providers.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Actions** area, click **Create RADIUS Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create RADIUS Provider** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	The name of the RADIUS provider group.
Available Providers list box	The available RADIUS providers that you can add to the RADIUS group. You can use Shift+Click and Ctrl+Click to select multiple providers.
>> button	Adds all available providers to the group regardless of what providers are selected in the **Available Providers** list box.
> button	Adds the providers selected in the **Available Providers** list box to the group.
< button	Removes the providers selected in the **Assigned Providers** list box from the group.
<< button	Removes all providers from the group regardless of what providers are selected in the **Assigned Providers** list box.
Assigned Providers list box	The RADIUS providers that are included in the RADIUS group. Cisco UCS searches the providers in the order that they appear in the table. To change the provider priority, select a provider and use the arrow buttons above the list to move the provider to the desired position.

b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting a RADIUS Provider Group

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** > **Provider Groups**.

Step 6 In the **Work** pane, click the RADIUS provider group you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **RADIUS Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a TACACS+ Provider Group

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

Note Authenticating with a single TACACS+ database does not require you to set up a TACACS+ provider group.

Before You Begin

Create one or more TACACS+ providers.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** and click **Provider Groups**.

Step 6 In the **Actions** area, click **Create TACACS+ Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create TACACS+ Provider Group** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	The name of the TACACS+ provider group.
Available Providers list box	The available TACACS+ providers that you can add to the TACACS+ group. You can use Shift+Click and Ctrl+Click to select multiple providers.
>> button	Adds all available providers to the group regardless of what providers are selected in the **Available Providers** list box.
> button	Adds the providers selected in the **Available Providers** list box to the group.
< button	Removes the providers selected in the **Assigned Providers** list box from the group.
<< button	Removes all providers from the group regardless of what providers are selected in the **Assigned Providers** list box.
Assigned Providers list box	The TACACS+ providers that are included in the TACACS+ group. Cisco UCS searches the providers in the order that they appear in the table. To change the provider priority, select a provider and use the arrow buttons above the list to move the provider to the desired position.

b) Click **OK**.

Step 7 Click **Save**.

Deleting a TACACS+ Provider Group

You cannot delete a provider group if it is being used by an authentication configuration.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** > **Provider Groups**.

Step 6 In the **Work** pane, click the **TACACS+ Provider Group** you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **TACACS+ Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Authentication Domains

Authentication domains are used by Cisco UCS Domain to leverage multiple authentication systems. Each authentication domain is specified and configured during login. If no authentication domain is specified, the default authentication service configuration is used.

You can create up to eight authentication domains. Each authentication domain is associated with a provider group and realm in Cisco UCS Domain. If no provider group is specified, all servers within the realm are used.

Note Authentication domains for LDAP are not supported for Cisco UCS Central for this release. However, Authentication domains are supported for managed Cisco UCS domains from the Cisco UCS Central Domain Group root.

Creating an Authentication Domain

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Authentication Domains**.

Step 6 In the **Actions** area, click **Create Authentication Domain** and complete all fields.
You can also right-click **Authentication Domains** to access that option.

a) In the **Create Authentication** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	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 after the object has been saved. **Note** 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.
Session Refresh Period field	When a web client connects to Cisco UCS Manager, the client needs to 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 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.
Session Timeout field	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.

Name	Description
Realm field	The authentication protocol that will be applied to users in this 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.
Provider Group drop-down list	If the **Realm** is set to **ldap**, **radius**, or **tacacs**, this field allows you to select an associated provider group.

b) Click **OK**.

Step 7 Click **Save**.

Selecting a 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 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Properties** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete all **Default Authentication** fields on the **General** tab.

Name	Description
Session Refresh Period field	When a web client connects to Cisco UCS Manager, the client needs to 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 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.
Session Timeout field	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.
Realm drop-down list	The default method by which a user is authenticated when logging remotely into a Cisco UCS domain included in the selected Cisco UCS Central domain group. 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. • **none**—If the user account is local to Cisco UCS Central or the Cisco UCS domain, no password is required when the user logs in remotely. • **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.
Provider Group drop-down list	If the **Realm** is set to **ldap**, **radius**, or **tacacs**, this field allows you to select an associated provider group.

b) In the **Properties (Native Authentication)** dialog box, complete all **Console Authentication** fields on the **General** tab.

Name	Description
Realm field	The method by which a user logging into the console is authenticated. 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. • **none**—If the user account is local to Cisco UCS Central or the Cisco UCS domain, no password is required when the user logs in remotely. • **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.
Provider Group drop-down list	If the **Realm** is set to **ldap**, **radius**, or **tacacs**, this field allows you to select an associated provider group.

c) In the **Properties (Native Authentication)** dialog box, complete **Remote Users Policy** field on the **General** tab.

Name	Description
Role Policy for Remote Users field	The action to take when a user attempts to log in and the LDAP, RADIUS, or TACACS+ server does not supply a user role with the authentication information. This can be one of the following: • **assign-default-role**—The user is allowed to log in with a read-only user role. • **no-login**—The user is not allowed to log in to the system, even if the username and password are correct.

d) Click **OK**.

Step 7 Click **Save**.

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 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Native Authentication** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete all **Default Authentication** fields on the **General** tab.

Name	Description
Session Refresh Period field	When a web client connects to Cisco UCS Manager, the client needs to 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 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.
Session Timeout field	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.

Name	Description
Realm drop-down list	The default method by which a user is authenticated when logging remotely into a Cisco UCS domain included in the selected Cisco UCS Central domain group. 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. • **none**—If the user account is local to Cisco UCS Central or the Cisco UCS domain, no password is required when the user logs in remotely. • **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.
Provider Group drop-down list	If the **Realm** is set to **ldap**, **radius**, or **tacacs**, this field allows you to select an associated provider group.

b) Click **OK**.

Step 7 Click **Save**.

Role Policy for Remote Users

By default, if user roles are not configured in Cisco UCS Central read-only access is granted to all users logging in to Cisco UCS Central from a remote server using the LDAP protocol (excluding RADIUS and TACACS+ authentication in this release).

Note RADIUS, TACACS+ and LDAP authentication are supported in locally managed Cisco UCS domains.

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

- **assign-default-role**

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

  This is the default behavior.

- **no-login**

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

For security reasons, it might be desirable to restrict access to those users matching an established user role in Cisco UCS Central.

Configuring the Role Policy for Remote Users

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Native Authentication** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete **Remote Users Policy** field on the **General** tab.

Name	Description
Role Policy for Remote Users field	The action to take when a user attempts to log in and the LDAP, RADIUS, or TACACS+ server does not supply a user role with the authentication information. This can be one of the following: • **assign-default-role**—The user is allowed to log in with a read-only user role. • **no-login**—The user is not allowed to log in to the system, even if the username and password are correct.

b) Click **OK**.

Step 7 Click **Save**.