Remote Authentication

- Authentication Services, on page 1
- Guidelines and Recommendations for Remote Authentication Providers, on page 1
- User Attributes in Remote Authentication Providers, on page 2
- Two-Factor Authentication, on page 4
- LDAP Providers and Groups, on page 4
- RADIUS Providers, on page 15
- TACACS+ Providers, on page 18
- Configuring Multiple Authentication Systems, on page 21
- Configuring Multiple Authentication Systems, on page 22
- Primary Authentication Service, on page 30

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

<table>
<thead>
<tr>
<th>Authentication Provider</th>
<th>Custom Attribute</th>
<th>Schema Extension</th>
<th>Attribute ID Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Not required if group mapping is used Optional if group mapping is not used</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Authentication Provider</td>
<td>Custom Attribute</td>
<td>Schema Extension</td>
<td>Attribute ID Requirements</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------</td>
<td>-----------------</td>
<td>---------------------------</td>
</tr>
</tbody>
</table>
| 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 multiple 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 multiple 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
```
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 refresh request 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.

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>UCS-A# <code>scope security</code></td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>UCS-A /security # <code>scope ldap</code></td>
<td>Enters security LDAP mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>UCS-A /security/ldap # <code>set attribute attribute</code></td>
<td>Restricts database searches to records that contain the specified attribute.</td>
</tr>
<tr>
<td>Step 4</td>
<td>UCS-A /security/ldap # <code>set basedn distinguished-name</code></td>
<td>Restricts database searches to records that contain the specified distinguished name.</td>
</tr>
<tr>
<td>Step 5</td>
<td>UCS-A /security/ldap # <code>set filter filter</code></td>
<td>Restricts database searches to records that contain the specified filter.</td>
</tr>
<tr>
<td>Step 6</td>
<td>(Optional) UCS-A /security/ldap # <code>set timeout seconds</code></td>
<td>Sets the time interval the system waits for a response from the LDAP server before noting the server as down.</td>
</tr>
<tr>
<td>Step 7</td>
<td>UCS-A /security/ldap # <code>commit-buffer</code></td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

**Example**

The following example sets the LDAP attribute to CiscoAvPair, the base distinguished name to "DC=cisco-ucsm-aaa3,DC=qalab,DC=com", the filter to sAMAccountName=$userid, and the timeout interval to 5 seconds, and commits the transaction:
User login will fail if the userdn for an LDAP user exceeds 255 characters.

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, you need to change the authentication realm for the domain to local, make the changes to the providers, and then change the domain authentication realm back to LDAP.

  - If you want to use the special characters listed in the following table for defining the attributes of an Active Directory bind distinguished name, you must replace the special character with an escape, by using a backslash (\) followed by the corresponding hexadecimal value of the character.
<table>
<thead>
<tr>
<th>Special Character</th>
<th>Description</th>
<th>Hexadecimal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>,</td>
<td>comma</td>
<td>0x2C</td>
</tr>
<tr>
<td>+</td>
<td>plus sign</td>
<td>0x2B</td>
</tr>
<tr>
<td>&quot;</td>
<td>double quote</td>
<td>0x22</td>
</tr>
<tr>
<td>\</td>
<td>backslash</td>
<td>0x5C</td>
</tr>
<tr>
<td>&lt;</td>
<td>left angle bracket</td>
<td>0x3C</td>
</tr>
<tr>
<td>&gt;</td>
<td>right angle bracket</td>
<td>0x3E</td>
</tr>
<tr>
<td>;</td>
<td>semicolon</td>
<td>0x3B</td>
</tr>
<tr>
<td>LF</td>
<td>line feed</td>
<td>0x0A</td>
</tr>
<tr>
<td>CR</td>
<td>carriage return</td>
<td>0x0D</td>
</tr>
<tr>
<td>=</td>
<td>equals sign</td>
<td>0x0D</td>
</tr>
<tr>
<td>/</td>
<td>forwards slash</td>
<td>0x2F</td>
</tr>
</tbody>
</table>


**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>UCS-A /security # scope ldap</td>
<td>Enters security LDAP mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>UCS-A /security/ldap # create server server-name</td>
<td>Creates an LDAP server instance and enters security LDAP server mode. If SSL is enabled, the server-name, typically an IP address or FQDN, must exactly match a Common Name (CN) in the LDAP server’s security certificate. Unless an IP address is specified, a DNS server must be configured in Cisco UCS Manager.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) UCS-A /security/ldap/server # set attribute attr-name</td>
<td>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</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) UCS-A/security/ldap/server # set basedn basedn-name</td>
<td>This value is required unless a default attribute has been set on the LDAP <strong>General</strong> tab.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) UCS-A/security/ldap/server # set binddn binddn-name</td>
<td>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 <strong>General</strong> tab.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> (Optional) UCS-A/security/ldap/server # set filter filter-value</td>
<td>The maximum supported string length is 255 ASCII characters.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> Required: UCS-A/security/ldap/server # set password</td>
<td>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 <strong>General</strong> tab.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> (Optional) UCS-A/security/ldap/server # set order order-num</td>
<td>The password for the LDAP database account specified in the <strong>Bind DN</strong> field. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign). To set the password, press <strong>Enter</strong> after typing the <strong>set password</strong> command and enter the key value at the prompt.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> (Optional) UCS-A/security/ldap/server # set port port-num</td>
<td>The order that the Cisco UCS uses this provider to authenticate users.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> UCS-A/security/ldap/server # set ssl {yes no}</td>
<td>Enables or disables the use of encryption when communicating with the LDAP server. The options are as follows:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>• yes — Encryption is required. If encryption cannot be negotiated, the connection fails. If enabled, 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• no — Encryption is disabled. Authentication information is sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 12**

UCS-A/security/ldap/server # set **timeout**

*timeout-num*

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.

**Step 13**

UCS-A/security/ldap/server # set **vendor**

{**ms-ad** | openldap}

Enables or disables the use of the nested LDAP group search capability on the LDAP server. The options are as follows:

• **ms-ad**—Nested LDAP group searches are supported with this option. If you set the vendor to ms-ad (Microsoft Active Directory), and enable and set the ldap-group-rule to recursive, Cisco UCS Manager can search through any nested LDAP groups.

• **openldap**—Nested LDAP group searches are not supported with this option. If you set the vendor to openldap, and enable and set the ldap-group-rule to recursive, Cisco UCS Manager will not search through any nested LDAP groups. If you choose this option, you must create each LDAP subgroup as an LDAP group map in Cisco UCS Manager, even if the parent group is already set up in a group map.
When you upgrade Cisco UCS Manager from an earlier version to release 2.1(2), the LDAP provider's vendor attribute is set to `openldap` by default, and LDAP authentication continues to operate successfully.

**Step 14**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS-A/security/ldap/server # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

**Example**

The following example creates an LDAP server instance named 10.193.169.246, configures the binddn, password, order, port, SSL settings, vendor attribute, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap* # create server 10.193.169.246
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set password
Enter the password:
Confirm the password:
UCS-A /security/ldap/server* # set order 2
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # set ssl yes
UCS-A /security/ldap/server* # set timeout 30
UCS-A /security/ldap/server* # set vendor ms-ad
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

The following example creates an LDAP server instance named 12:31:71:1231:45b1:0011:011:900, configures the binddn, password, order, port, SSL settings, vendor attribute, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set password
Enter the password:
Confirm the password:
UCS-A /security/ldap/server* # set order 1
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # set ssl yes
UCS-A /security/ldap/server* # set timeout 45
UCS-A /security/ldap/server* # set vendor ms-ad
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

**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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>UCS-A /security # scope ldap</td>
<td>Enters security LDAP mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>UCS-A /security/ldap # scope server ldap-provider</td>
<td>Enters security LDAP provider mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>UCS-A /security/ldap/server # scope ldap-group-rule</td>
<td>Enters LDAP group rule mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>UCS-A /security/ldap/server/ldap-group-rule# set authorization {enable</td>
<td>disable}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>disable</strong>—Cisco UCS does not access any LDAP groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>enable</strong>—Cisco UCS searches the LDAP provider 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Step 6</td>
<td>UCS-A /security/ldap/server/ldap-group-rule# set member-of-attribute attr-name</td>
<td>The attribute Cisco UCS uses to determine group membership in the LDAP database. The supported string length is 63 characters. The default string is <strong>memberOf</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>UCS-A /security/ldap/server/ldap-group-rule# set traversal {non-recursive</td>
<td>recursive}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>non-recursive</strong>—Cisco UCS only searches those groups that the user belongs to.</td>
</tr>
</tbody>
</table>
Deleting an LDAP Provider

**Remote Authentication**

**Deleting an LDAP Provider**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> UCS-A/security/ldap/server/ldap-group-rule# set use-primary-group {yes</td>
<td>no}</td>
</tr>
<tr>
<td><strong>Step 9</strong> UCS-A/security/ldap/server/ldap-group-rule# commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

**Example**

The following example sets the LDAP group rule to enable authorization, sets the member of attribute to memberOf, sets the traversal to non-recursive, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # scope server ldapprovider
UCS-A /security/ldap/server # scope ldap-group-rule
UCS-A /security/ldap/server/ldap-group-rule # set authorization enable
UCS-A /security/ldap/server/ldap-group-rule* # set member-of-attribute memberOf
UCS-A /security/ldap/server/ldap-group-rule* # set traversal non-recursive
UCS-A /security/ldap/server/ldap-group-rule* # set use-primary-group yes
UCS-A /security/ldap/server/ldap-group-rule* # commit-buffer
```

**Dealing with LDAP Providers**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# scope security</td>
<td>Enters security mode</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A /security # scope ldap</td>
<td>Enters security LDAP mode</td>
</tr>
<tr>
<td><strong>Step 3</strong> UCS-A /security/ldap # delete server serv-name</td>
<td>Deletes the specified server.</td>
</tr>
<tr>
<td><strong>Step 4</strong> UCS-A /security/ldap # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

**Example**

The following example deletes the LDAP server called ldap1 and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
```
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).
Deleting an LDAP Group Map

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# <code>scope security</code></td>
<td>Enters security mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A <code>/security # scope ldap</code></td>
<td>Enters security LDAP mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> UCS-A <code>/security/ldap # create ldap-group group-dn</code></td>
<td>Creates an LDAP group map for the specified DN. The maximum number of characters for <code>group-dn</code> is 240. <strong>Note</strong> If you plan to enter a special character for this command, you need to prefix the special character with an escape character <code>\</code> (double back slash).</td>
</tr>
<tr>
<td><strong>Step 4</strong> UCS-A <code>/security/ldap/ldap-group # create locale locale-name</code></td>
<td>Maps the LDAP group to the specified locale.</td>
</tr>
<tr>
<td><strong>Step 5</strong> UCS-A <code>/security/ldap/ldap-group # create role role-name</code></td>
<td>Maps the LDAP group to the specified role.</td>
</tr>
<tr>
<td><strong>Step 6</strong> UCS-A <code>/security/ldap/ldap-group # commit-buffer</code></td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

**Example**

The following example maps the LDAP group mapped to a DN, sets the locale to pacific, sets the role to admin, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # create ldap-group group-dn cn=security,cn=users,dc=lab,dc=com
UCS-A /security/ldap/ldap-group* # create locale pacific
UCS-A /security/ldap/ldap-group* # create role admin
UCS-A /security/ldap/ldap-group* # commit-buffer
UCS-A /security/ldap/ldap-group #
```

**What to do next**

Set the LDAP group rule.

Deleting an LDAP Group Map

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# <code>scope security</code></td>
<td>Enters security mode.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2, 4</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Deletes the LDAP group map for the specified DN.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

### Example

The following example deletes an LDAP group map and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete ldap-group cn=security,cn=users,dc=lab,dc=com
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

---

### 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.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enters security RADIUS mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Sets the number of times to retry communicating with the RADIUS server before noting the server as down.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Sets the time interval that the system waits for a response from the RADIUS server before noting the server as down.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>
Example

The following example sets the RADIUS retries to 4, sets the timeout interval to 30 seconds, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # set retries 4
UCS-A /security/radius* # set timeout 30
UCS-A /security/radius* # commit-buffer
```

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 multiple 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>UCS-A /security # scope radius</td>
<td>Enters security RADIUS mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>UCS-A /security/radius # create server server-name</td>
<td>Creates a RADIUS server instance and enters security RADIUS server mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) UCS-A /security/radius/server # set authport authport-num</td>
<td>Specifies the port used to communicate with the RADIUS server.</td>
</tr>
</tbody>
</table>
### Command or Action

| Step 5 | UCS-A/security/radius/server # set key | **Purpose**
|---|---|---
| Specifies when in the order this server will be tried. |
| Step 6 | (Optional) UCS-A/security/radius/server # set order order-num | Specifies when in the order this server will be tried. |
| Step 7 | (Optional) UCS-A/security/radius/server # set retries retry-num | Sets the number of times to retry communicating with the RADIUS server before noting the server as down. |
| Step 8 | (Optional) UCS-A/security/radius/server # set timeout seconds | Sets the time interval that the system waits for a response from the RADIUS server before noting the server as down. |
| Tip | It is recommended that you configure a higher Timeout value if you select two-factor authentication for RADIUS providers. |
| Step 9 | UCS-A/security/radius/server # commit-buffer | Commits the transaction to the system configuration. |

### Example

The following example creates a server instance named radiusserv7, sets the authentication port to 5858, sets the key to radiuskey321, sets the order to 2, sets the retries to 4, sets the timeout to 30, enables two-factor authentication, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create server radiusserv7
UCS-A /security/radius/server* # set authport 5858
UCS-A /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
UCS-A /security/radius/server* # set order 2
UCS-A /security/radius/server* # set retries 4
UCS-A /security/radius/server* # set timeout 30
UCS-A /security/radius/server* # commit-buffer
```

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A /security # scope RADIUS</td>
<td>Enters security RADIUS mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> UCS-A /security/radius # delete server serv-name</td>
<td>Deletes the specified server.</td>
</tr>
<tr>
<td><strong>Step 4</strong> UCS-A /security/radius # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

### Example

The following example deletes the RADIUS server called radius1 and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # delete server radius1
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

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

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A /security # scope tacacs</td>
<td>Enters security TACACS+ mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) UCS-A /security/tacacs # set timeout seconds</td>
<td>Sets the time interval that the system waits for a response from the TACACS+ server before noting the server as down.</td>
</tr>
<tr>
<td><strong>Step 4</strong> UCS-A /security/tacacs # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>
Example

The following example sets the TACACS+ timeout interval to 45 seconds and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # set timeout 45
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>UCS-A /security # scope tacacs</td>
<td>Enters security TACACS+ mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>UCS-A /security/tacacs # create server server-name</td>
<td>Creates a TACACS+ server instance and enters security TACACS+ server mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) UCS-A /security/tacacs/server # set key</td>
<td>Sets the TACACS+ server key. To set the key value, press Enter after typing the set key command and enter the key value at the prompt.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) UCS-A /security/tacacs/server # set order order-num</td>
<td>Specifies when in the order this server will be tried.</td>
</tr>
</tbody>
</table>
Deleting a TACACS+ Provider

### Command or Action | Purpose
--- | ---
**Step 6** | (Optional) UCS-A /security/tacacs/server # set timeout seconds
**Step 7** | UCS-A /security/tacacs/server # set port port-num
**Step 8** | UCS-A /security/tacacs/server # commit-buffer

**Example**

The following example creates a server instance named tacacsserv680, sets the key to tacacskey321 and confirms the key, sets the order to 4, sets the authentication port to 5859, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create server tacacsserv680
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCS-A /security/tacacs/server* # set order 4
UCS-A /security/tacacs/server* # set port 5859
UCS-A /security/tacacs/server* # commit-buffer
```

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>UCS-A# scope security</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>UCS-A /security # scope tacacs</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>UCS-A /security/tacacs # delete server serv-name</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> UCS-A /security/tacacs # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

### Example

The following example deletes the TACACS server called tacacs1 and commits the transaction:

```text
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # delete server TACACS1
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

### Configuring Multiple Authentication Systems

#### Multiple Authentication Services

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

- Provider groups
- Authentication domains

After provider groups and authentication domains are configured in Cisco UCS Manager, you can use the following syntax to log in to the system using Cisco UCS Manager CLI: `ucs: auth-domain \ user-name`

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, Telnet or Putty.

**Note**

SSH log in is case-sensitive.

From a Linux terminal using SSH:

- `ssh ucs-auth-domain\\username@{UCSM-ip-address | UCMS-ipv6-address}`
- `ssh ucs-example\\jsmith@192.0.20.11`
- `ssh ucs-example\\jsmith@2001::1`
- `ssh -l ucs-auth-domain\\username \UCSM-ip-address|UCSM-ipv6-address\UCSM-host-name`
- `ssh -l ucs-example\\jsmith 192.0.20.11`
- `ssh -l ucs-example\\jsmith 2001::1`
- `ssh \UCSM-ip-address \ UCMS-ipv6-address \ UCMS-host-name -l ucs-auth-domain\\username`
- `ssh 192.0.20.11 -l ucs-example\\jsmith`
- `ssh 2001::1 -l ucs-example\\jsmith`
- `ssh ucs-auth-domain\\username@{UCSM-ip-address | UCMS-ipv6-address}`
ssh ucs-ldap23\jsmith@192.0.20.11
ssh ucs-ldap23\jsmith@2001::1

From a Linux terminal using Telnet:

- `telnet ucs-UCSM-host-name ucs-auth-domain\username`
  
  `telnet ucs-qa-10`
  `login: ucs-ldap23\blradmin`

- `telnet {UCSM-ip-address | UCSM-ipv6-address} ucs-auth-domain\username`
  
  `telnet 10.106.19.12 2052`
  `ucs-qa-10-A login: ucs-ldap23\blradmin`

From a Putty client:

- Login as: `ucs-auth-domain\username`
  
  Login as: `ucs-example\jsmith`

---

**Note**

If the default authentication is set to local, and the console authentication is set to LDAP, you can log in to the fabric interconnect from a Putty client using `ucs-local\admin`, where admin is the name of the local account.

---

# Configuring Multiple Authentication Systems

## 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
</tbody>
</table>
Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>UCS-A /scope ldap</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>UCS-A/security/ldap # create auth-server-group auth-server-group-name</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>UCS-A/security/ldap/auth-server-group # create server-ref ldap-provider-name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>UCS-A/security/ldap/auth-server-group/server-ref # set order order-num</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>UCS-A/security/ldap/auth-server-group/server-ref # commit-buffer</td>
</tr>
</tbody>
</table>

**Example**

The following example creates an LDAP provider group called ldapgroup, adds two previously configured providers called ldap1 and ldap2 to the provider group, sets the order, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # create auth-server-group ldapgroup
UCS-A /security/ldap/auth-server-group* # create server-ref ldap1
UCS-A /security/ldap/auth-server-group/server-ref* # set order 1
UCS-A /security/ldap/auth-server-group/server-ref* # up
UCS-A /security/ldap/auth-server-group* # create server-ref ldap2
UCS-A /security/ldap/auth-server-group/server-ref* # set order 2
UCS-A /security/ldap/auth-server-group/server-ref* # commit-buffer
```

**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.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: UCS-A# <code>scope security</code></td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2: UCS-A /security # <code>scope radius</code></td>
<td>Enters security RADIUS mode.</td>
</tr>
<tr>
<td>Step 3: UCS-A /security/radius # <code>create auth-server-group auth-server-group-name</code></td>
<td>Creates a RADIUS provider group and enters authentication server group security RADIUS mode.</td>
</tr>
<tr>
<td>Step 4: UCS-A /security/RADIUS/auth-server-group # <code>create server-ref radius-provider-name</code></td>
<td>Adds the specified RADIUS provider to the RADIUS provider group and enters server reference authentication server group security RADIUS mode.</td>
</tr>
<tr>
<td>Step 5: UCS-A /security/radius/auth-server-group/server-ref # <code>set order order-num</code></td>
<td>Specifies the order in which Cisco UCS uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the order to no-value is equivalent to giving that server reference the highest priority.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 6

- **UCS-A**
  - `scope security/radius/auth-server-group/server-ref` # commit-buffer

Commits the transaction to the system configuration.

---

### Example

The following example creates a RADIUS provider group called radiusgroup, adds two previously configured providers called radius1 and radius2 to the provider group, sets the order, and commits the transaction:

```plaintext
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create auth-server-group radiusgroup
UCS-A /security/radius/auth-server-group # create server-ref radius1
UCS-A /security/radius/auth-server-group/server-ref # set order 1
UCS-A /security/radius/auth-server-group/server-ref # up
UCS-A /security/radius/auth-server-group # create server-ref radius2
UCS-A /security/radius/auth-server-group/server-ref # set order 2
UCS-A /security/radius/auth-server-group/server-ref # commit-buffer
```

### What to do next

Configure an authentication domain or select a default authentication service.

---

### Deleting a RADIUS Provider Group

Remove the provider group from an authentication configuration.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# <code>scope security</code></td>
<td>Enters security mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A <code>/security # scope radius</code></td>
<td>Enters security RADIUS mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> UCS-A <code>/security/radius # delete auth-server-group auth-server-group-name</code></td>
<td>Deletes the RADIUS provider group.</td>
</tr>
<tr>
<td><strong>Step 4</strong> UCS-A <code>/security/radius # commit-buffer</code></td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

#### Example

The following example deletes a RADIUS provider group called radiusgroup and commits the transaction:
Creating a TACACS Provider Group

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

Before you begin

Create a TACACS provider.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>UCS-A# scope security</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>UCS-A /security # scope tacacs</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>UCS-A /security/tacacs # create auth-server-group auth-server-group-name</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>UCS-A /security/tacacs/auth-server-group # create server-ref tacacs-provider-name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>UCS-A /security/tacacs/auth-server-group/server-ref # set order order-num</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>UCS-A /security/tacacs/auth-server-group/server-ref # commit-buffer</td>
</tr>
</tbody>
</table>

Example

The following example creates a TACACS provider group called tacacsgroup, adds two previously configured providers called tacacs1 and tacacs2 to the provider group, sets the order, and commits the transaction:

UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create auth-server-group tacacsgroup
UCS-A /security/tacacs/auth-server-group* # create server-ref tacacs1
UCS-A /security/tacacs/auth-server-group/server-ref* # set order 1
Deleting a TACACS Provider Group

Remove the provider group from an authentication configuration.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>UCS-A /security # scope tacacs</td>
<td>Enters security TACACS mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>UCS-A /security/tacacs # delete auth-server-group auth-server-group-name</td>
<td>Deletes the TACACS provider group.</td>
</tr>
<tr>
<td>Step 4</td>
<td>UCS-A /security/tacacs # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

**Example**

The following example deletes a TACACS provider group called tacacsgroup and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # delete auth-server-group tacacsgroup
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

**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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>UCS-A /security # create auth-domain domain-name</td>
<td>Creates an authentication domain and enters authentication domain mode. <strong>Note</strong>: 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.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) UCS-A /security/auth-domain # set refresh-period seconds</td>
<td>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. <strong>Note</strong>: 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.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) UCS-A /security/auth-domain # set session-timeout seconds</td>
<td>The maximum amount of time that can elapse after the last refresh request before Cisco UCS Manager considers a web session as inactive. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>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. <strong>Note</strong> If you set two-factor authentication for a RADIUS or TACACS+ realm, consider increasing the <strong>session-refresh</strong> and <strong>session-timeout</strong> periods so that remote users will not have to re-authenticate too frequently.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) UCS-A /security/auth-domain # create default-auth Creates a default authentication for the authentication domain.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) UCS-A /security/auth-domain/default-auth # set auth-server-group auth-serv-group-name Sets the provider group for the authentication domain.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>UCS-A /security/auth-domain/default-auth # set realm {ldap</td>
<td>local</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>(Optional) UCS-A /security/auth-domain/default-auth # set use-2-factor yes Sets the authentication method to two-factor authentication for the realm. <strong>Note</strong> Two-factor authentication applies only to the RADIUS and TACACS+ realms.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>UCS-A /security/auth-domain/default-auth # commit-buffer Commits the transaction to the system configuration.</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

The following example creates an authentication domain called domain1 with a web refresh period of 3600 seconds (1 hour) and a session timeout period of 14400 seconds (4 hours). It then configures domain1 to use the providers in radius1, sets the realm type to radius, enables two-factor authentication, and commits the transaction:

```bash
UCS-A# scope security
UCS-A /security # create auth-domain domain1
UCS-A /security/auth-domain# * set refresh-period 3600
UCS-A /security/auth-domain# * set session-timeout 14400
UCS-A /security/auth-domain# * create default-auth
UCS-A /security/auth-domain/auth-domain# * set auth-server-group radius1
UCS-A /security/auth-domain/auth-domain# * set realm radius
UCS-A /security/auth-domain/auth-domain# * set user-2-factor yes
UCS-A /security/auth-domain/auth-domain# commit-buffer
```
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2 UCS-A/security # scope console-auth</td>
<td>Enters console authorization security mode.</td>
</tr>
<tr>
<td>Step 3 UCS-A/security/console-auth # set realm auth-type</td>
<td>Specifies the console authentication, where the auth-type argument is one of the following keywords:</td>
</tr>
<tr>
<td></td>
<td>• ldap — Specifies LDAP authentication</td>
</tr>
<tr>
<td></td>
<td>• local — Specifies local authentication</td>
</tr>
<tr>
<td></td>
<td>• none — Allows local users to log on without specifying a password</td>
</tr>
<tr>
<td></td>
<td>• radius — Specifies RADIUS authentication</td>
</tr>
<tr>
<td></td>
<td>• tacacs — Specifies TACACS+ authentication</td>
</tr>
<tr>
<td>Step 4 (Optional) UCS-A/security/console-auth # set auth-server-group auth-serv-group-name</td>
<td>The associated provider group, if any.</td>
</tr>
<tr>
<td>Step 5 (Optional) UCS-A/security/default-auth # set use-2-factor yes</td>
<td>Sets the authentication method to two-factor authentication for the realm.</td>
</tr>
<tr>
<td></td>
<td>Note Two-factor authentication applies only to the RADIUS and TACACS+ realms.</td>
</tr>
<tr>
<td>Step 6 UCS-A/security/console-auth # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>
Example

The following example sets the authentication realm to TACACS+, sets the console authentication provider group to provider1, enables two-factor authentication, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope console-auth
UCS-A /security/console-auth # set realm tacacs
UCS-A /security/console-auth # set auth-server-group provider1
UCS-A /security/console-auth* # set use-2-factor yes
UCS-A /security/console-auth* # commit-buffer
```

Selecting the Default Authentication Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>2</td>
<td>UCS-A /security # scope default-auth</td>
<td>Enters default authorization security mode.</td>
</tr>
</tbody>
</table>
| 3    | UCS-A /security/default-auth # set realm auth-type | Specifies the default authentication, where `auth-type` is one of the following keywords:  
  - ldap—Specifies LDAP authentication
  - local—Specifies local authentication
  - none—Allows local users to log on without specifying a password
  - radius—Specifies RADIUS authentication
  - tacacs—Specifies TACACS+ authentication |
| 4    | (Optional) UCS-A /security/default-auth # set auth-server-group auth-serv-group-name | The associated provider group, if any. |
| 5    | (Optional) UCS-A /security/default-auth # set refresh-period seconds | 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 |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> (Optional) UCS-A /security/default-auth # set session-timeout seconds</td>
<td>The maximum amount of time that can elapse after the last refresh request 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. <strong>Note</strong> If you set two-factor authentication for a RADIUS or TACACS+ realm, consider increasing the session-refresh and session-timeout periods so that remote users will not have to re-authenticate too frequently.</td>
</tr>
<tr>
<td><strong>Step 7</strong> (Optional) UCS-A /security/default-auth # set use-2-factor yes</td>
<td>Sets the authentication method to two-factor authentication for the realm. <strong>Note</strong> Two-factor authentication applies only to the RADIUS and TACACS+ realms.</td>
</tr>
<tr>
<td><strong>Step 8</strong> UCS-A /security/default-auth # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

### Example

The following example sets the default authentication to RADIUS, the default authentication provider group to provider1, enables two-factor authentications, sets the refresh period to 7200 seconds (2 hours), the session timeout period to 28800 seconds (8 hours), and enables two-factor authentication. It then commits the transaction.

```
UCS-A# scope security
UCS-A /security # scope default-auth
UCS-A /security/default-auth # set realm radius
UCS-A /security/default-auth* # set auth-server-group provider1
UCS-A /security/default-auth* # set use-2-factor yes
UCS-A /security/default-auth* # set refresh-period 7200
UCS-A /security/default-auth* # set session-timeout 28800
UCS-A /security/default-auth* # commit-buffer
UCS-A /security/default-auth #
```
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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>UCS-A# scope security</td>
<td>Enters security mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>UCS-A /security # set remote-user default-role</td>
<td>Specifies whether user access to Cisco UCS</td>
</tr>
<tr>
<td></td>
<td>{assign-default-role</td>
<td>no-login}</td>
</tr>
<tr>
<td>Step 3</td>
<td>UCS-A /security # commit-buffer</td>
<td>Commits the transaction to the system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration.</td>
</tr>
</tbody>
</table>

### Example

The following example sets the role policy for remote users and commits the transaction:

```
UCS-A# scope security
UCS-A /security # set remote-user default-role assign-default-role
UCS-A /security* # commit-buffer
UCS-A /security 
```
Configuring the Role Policy for Remote Users