Configuring Primary Authentication

This chapter includes the following sections:

Primary Authentication

Cisco UCS supports two methods to authenticate user logins:

- Local to Cisco UCS Manager
- Remote through one of the following protocols:
  - LDAP
  - RADIUS
  - TACACS+

Note You can only use one authentication method. For example, if you select LDAP as your authentication provider, you cannot use RADIUS or TACACS+ for authentication. However, if the user account in the remote authentication provider does not have at least one Cisco UCS role, Cisco UCS Manager checks the local database to determine whether an account with the same name exists in the local database.

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 it. In addition, you need to be aware of the following guidelines that impact user authorization:

User Accounts in Remote Authentication Services

You can create user accounts in Cisco UCS Manager or in the remote authentication server.

The temporary sessions for users who log in through remote authentication services can be viewed through Cisco UCS Manager GUI or 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. If an account does not have the required roles, the user is granted only read-only privileges.

User Attribute for LDAP

If a Cisco UCS instance uses LDAP as the remote authentication provider, you can do one of the following:

- Map an existing attribute to the user roles and locale for the Cisco UCS instance.
- Create a CiscoAVPair or other unique attribute in the LDAP service and map that attribute to the user roles and locale for the Cisco UCS instance.

You must configure the LDAP provider in Cisco UCS Manager with the attribute that holds the user roles and locales. When a user logs in, Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service and validates the user.

If you create a CiscoAVPair attribute for the Cisco UCS instance, use the following definition for the OID:

```
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
```

Required User Attribute for RADIUS and TACACS+

If a Cisco UCS instance uses either RADIUS or TACACS+ as the remote authentication provider, you must create a cisco-av-pair attribute in the remote authentication service and map that attribute to the user roles and locale for the Cisco UCS instance. When a user logs in, Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service and validates the user.

Note You cannot use any other attribute in RADIUS or TACAC+ for the Cisco UCS roles. You must create the attribute required for that specific remote authentication service.

Configuring LDAP Providers

Configuring Properties for LDAP Providers

The properties that you configure in this task apply to all LDAP provider connections defined in Cisco UCS Manager.

Procedure

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

Step 2 In the Admin tab, expand **User Management ➤ LDAP**.

Step 3 Complete the following fields in the **Properties** area:

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. The valid range is from 1 to 60 seconds. The default value is 5 seconds. This property is optional.
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 map an existing LDAP attribute to the Cisco UCS roles and locales, 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 **Note** If you do not specify this property, user access is restricted to read-only.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when it receives an authorization request. The maximum supported string length is 128 characters. This property is required.
Filter field	If specified, the LDAP search is restricted to those usernames that match the defined filter. This property is optional.

Step 4 Click **Save Changes**.

What to Do Next

Create an LDAP provider.

Creating an LDAP Provider

Before You Begin

Perform the following configuration in the LDAP server:

- Configure users with the attribute that holds the user role and locale information for Cisco UCS Manager. You can use an existing LDAP attribute that is mapped to the Cisco UCS user roles and locales or create a custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 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 log-in requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

If you have not already done so, configure the properties for the LDAP provider connections in Cisco UCS Manager.

Procedure

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

Step 2 In the Admin tab, expand **User Management ➤ LDAP**.

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

Step 4 In the **Create LDAP Provider** dialog box:

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

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 in Cisco UCS Manager.
Order field	The order in which Cisco UCS uses this provider to authenticate users. Enter an integer between 0 and 16.
Bind DN field	The distinguished name (DN) for the LDAP database superuser account. The maximum supported string length is 128 characters.
Port field	The port through which Cisco UCS communicates with the LDAP database.

Name	Description
Enable SSL check box	If checked, communications to the LDAP database require SSL encryption.
Key field	If **Enable SSL** is checked, the SSL encryption key for the database.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to Do Next

Select LDAP as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 9.

Deleting an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **User Management ➤ LDAP** .
Step 3 Right-click the LDAP provider you want to delete and choose **Delete**.
Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring RADIUS Providers

Configuring Properties for RADIUS Providers

The properties that you configure in this task apply to all RADIUS provider connections defined in Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **User Management ➤ RADIUS** .
Step 3 Complete the following fields in the **Properties** area:

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 a value from 1 to 60 seconds. The default value is 5 seconds.
Retries field	The number of times to retry the connection before the re3quest is considered to have failed.

Step 4 Click **Save Changes**.

What to Do Next

Create a RADIUS provider.

Creating a RADIUS Provider

Before You Begin

Perform the following configuration in the RADIUS server:

- Create the cisco-av-pairs attribute. You cannot use an existing RADIUS attribute.
- 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 log-in requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

If you have not already done so, configure the properties for the RADIUS provider connections in Cisco UCS Manager.

Procedure

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

Step 2 In the **Admin** tab, expand **User Management ➤ RADIUS** .

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

Step 4 In the **Create RADIUS Provider** dialog box:

a) Complete the fields with the information about the RADIUS service you want to use.

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 in Cisco UCS Manager.
Order field	The order in which Cisco UCS uses this provider to authenticate users.

Name	Description
	Enter an integer between 0 and 16.
Key field	The SSL encryption key for the database.
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.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to Do Next

Select RADIUS as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 9.

Deleting a RADIUS Provider

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **User Management ➤ RADIUS** .
Step 3 Right-click the RADIUS provider you want to delete and choose **Delete**.
Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Configuring TACACS+ Providers

Configuring Properties for TACACS+ Providers

The properties that you configure in this task apply to all RADIUS provider connections defined in Cisco UCS Manager.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **User Management ➤ TACACS+** .
Step 3 In the **Properties** area, complete the **Timeout** field:

The length of time in seconds the system should spend trying to contact the TACACS+ database before it times out.

Enter a value from 1 to 60 seconds. The default is 5 seconds.

Step 4 Click **Save Changes**.

What to Do Next

Create an TACACS+ provider.

Creating a TACACS+ Provider

Before You Begin

Perform the following configuration in the TACACS+ server:

- Create the cisco-av-pairs attribute. You cannot use an existing TACACS+ attribute.
- 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 log-in requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

If you have not already done so, configure the properties for the TACACS+ provider connections in Cisco UCS Manager.

Procedure

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

Step 2 In the **Admin** tab, expand **User Management ➤ TACACS+** .

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

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

a) Complete the fields with the information about the TACACS service you want to use.

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 in Cisco UCS Manager.
Order field	The order in which Cisco UCS uses this provider to authenticate users. Enter an integer between 0 and 16.
Key field	The SSL encryption key for the database.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.

Name	Description
Port field	The port through which Cisco UCS should communicate with the TACACS+ database.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to Do Next

Select TACACS as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 9.

Deleting a TACACS+ Provider

Procedure

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

Step 2 In the **Admin** tab, expand **User Management ➤ TACACS+** .

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

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Selecting a Primary Authentication Service

Before You Begin

If the system uses a remote authentication service, create a provider for that authentication service. If you chose console, you do not need to create a provider first.

Procedure

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

Step 2 In the **Admin** tab, expand **User Management ➤ Authorization** .

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

Step 4 On the **General** tab, complete the following fields:

Name	Description
Console field	The method by which a user logging into the console is authenticated. This can be:

Name	Description
	• **ldap**—The user must be defined on the LDAP server specified for this Cisco UCS instance. • **local**—The user account must be defined locally in this Cisco UCS instance. • **none**—If the user account is local to this Cisco UCS instance, no password is required when the user logs into the console. • **radius**—The user must be defined on the RADIUS server specified for this Cisco UCS instance. • **tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS instance.
Default field	The default method by which a user is authenticated during remote login. This can be: • **ldap**—The user must be defined on the LDAP server specified for this Cisco UCS instance. • **local**—The user account must be defined locally in this Cisco UCS instance. • **none**—If the user account is local to this Cisco UCS instance, no password is required when the user logs in remotely. • **radius**—The user must be defined on the RADIUS server specified for this Cisco UCS instance. • **tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS instance.
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: • **no-login**—The user is not allowed to log into the system, even if the user name and password are correct. • **assign-default-role**—The user is allowed to log in with a read-only user role.

Step 5 Click **Save Changes**.