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 local, RADIUS, or TACACS+ for authentication.

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 and Related Attributes 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.

The following table contains the name of the attribute that contains the value of the roles. Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service during login.

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

Remote Authentication Protocol	Attribute Name
LDAP	CiscoAVPair
RADIUS	cisco-av-pair
TACACS+	cisco-av-pair

For LDAP, the following is the full definition for the CiscoAVPair 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
```

Creating a Remote Authentication Provider

Creating an LDAP Provider

Before You Begin

Perform the following configuration in the LDAP server:

- Create a CiscoAVPair attribute with an attribute ID of 1.3.6.1.4.1.9.287247.1. You cannot use an existing LDAP 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.

Procedure

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

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

Step 3 Complete all fields in the **Properties** area, except for those in the **States** section:

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 contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. You must create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: 1.3.6.1.4.1.9.287247.1 The CiscoAVPair attribute stores the values of role and locales for the user. **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.
States Section	
Current Task field	This field shows the task that is executing on behalf of this component. For details, see the associated **FSM** tab.

Name	Description
	Note If there is no current task, this field is not displayed.

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

Step 5 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 (or IP Address) field	The hostname or IP address on which the LDAP provider resides.
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.
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 6 Click **Save Changes**.

What to Do Next

Select LDAP as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 8.

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.

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 request is considered to have failed.
States Section	
Current Task field	This field shows the task that is executing on behalf of this component. For details, see the associated **FSM** tab. **Note** If there is no current task, this field is not displayed.

Step 4 In the **Actions** area of the **General** tab, click **Create RADIUS Provider**.

Step 5 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 (or IP Address) field	The hostname or IP address on which the RADIUS provider resides.
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 6 Click **Save Changes**.

What to Do Next

Select RADIUS as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 8.

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.

Procedure

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

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

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

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

Step 4 In the **Actions** area of the **General** tab, click **Create TACACS Provider**.

Step 5 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 (or IP Address) field	The hostname or IP address on which the TACAS provider resides.
Key field	The SSL encryption key for the database.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.
Port field	The port through which the system should communicate with the TACACS+ database.

b) Click **OK**.

Step 6 Click **Save Changes**.

What to Do Next

Select TACACS as the primary authentication service. For more information, see Selecting a Primary Authentication Service, page 8.

Deleting a Remote Authentication Provider

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 displays a confirmation dialog box, click **Yes**.

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 displays a confirmation dialog box, click **Yes**.

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 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 On the **General** tab, click the radio button for the primary authentication method you want to use.

Step 4 Click **Save Changes**.