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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **scope ldap**	Enters security LDAP mode.
Step 3	UCS-A /security/ldap # **set attribute** *attribute*	Restricts database searches to records that contain the specified attribute.
Step 4	UCS-A /security/ldap # **set basedn** *distinguished-name*	Restricts database searches to records that contain the specified distinguished name.
Step 5	UCS-A /security/ldap # **set filter** *filter*	Restricts database searches to records that contain the specified filter.
Step 6	UCS-A /security/ldap # **set timeout** *seconds*	(Optional) Sets the time interval the system waits for a response from the LDAP server before noting the server as down.
Step 7	UCS-A /security/ldap # **create server** *server-name*	Creates an LDAP server instance and enters security LDAP server mode
Step 8	UCS-A /security/ldap/server # **set ssl** {**yes** | **no**}	Enables or disables the use of SSL when communicating with the LDAP server.
Step 9	UCS-A /security/ldap/server # **set key**	(Optional) Sets the LDAP server key. To set the key value, press Return after typing the **set key** command and enter the key value at the prompt.
Step 10	UCS-A /security/ldap/server # **set port** *port-num*	Specifies the port used to communicate with the LDAP server.
Step 11	UCS-A /security/ldap/server # **set binddn** *bind-dist-name*	Specifies the distinguished name for the LDAP database superuser account.

The following example sets the LDAP attribute to CiscoAvPair, the base distinguished name to "DC=nuova-sam-aaa3,DC=qalab,DC=com", the filter to sAMAccountName=$userid, the timeout interval to 5 seconds, creates a server instance named 10.193.169.246, disables SSL, sets the key, sets the authentication port to 389, and sets the root distinguished name to "cn=Administrator,cn=Users,DC=nuova-sam-aaa3,DC=qalab,DC=com":

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # set attribute CiscoAvPair
```

```
UCS-A /security/ldap* # set basedn "DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap* # set filter sAMAccountName=$userid
UCS-A /security/ldap* # set timeout 5
UCS-A /security/ldap* # create server 10.193.169.246
UCS-A /security/ldap/server* # set ssl no
UCS-A /security/ldap/server* # set key
Enter the key:
Confirm the key:
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

Creating a RADIUS Provider

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **scope radius**	Enters security RADIUS mode.
Step 3	UCS-A /security/radius # **set retries** *retry-num*	(Optional) Sets the number of times to retry communicating with the RADIUS server before noting the server as down.
Step 4	UCS-A /security/radius # **set timeout** *seconds*	(Optional) Sets the time interval the system waits for a response from the RADIUS server before noting the server as down.
Step 5	UCS-A /security/radius # **create server** *server-name*	Creates a RADIUS server instance and enters security RADIUS server mode
Step 6	UCS-A /security/radius/server # **set authport** *authport-num*	Specifies the port used to communicate with the RADIUS server.
Step 7	UCS-A /security/radius/server # **set key**	(Optional) Sets the RADIUS server key. To set the key value, press Return after typing the **set key** command and enter the key value at the prompt.

The following example sets the RADIUS retries to 4, the timeout interval to 30 seconds, creates a server instance named radiusserv7, sets the authentication port to 5858, and sets the key to radiuskey321:

```
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 # 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
```

Creating a TACACS+ Provider

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **scope tacacs**	Enters security TACACS+ mode.
Step 3	UCS-A /security/tacacs # **set timeout** *seconds*	(Optional) Sets the time interval the system waits for a response from the TACACS+ server before noting the server as down.
Step 4	UCS-A /security/tacacs # **create server** *server-name*	Creates an TACACS+ server instance and enters security TACACS+ server mode
Step 5	UCS-A /security/tacacs/server # **set key**	(Optional) Sets the TACACS+ server key. To set the key value, press Return after typing the **set key** command and enter the key value at the prompt.
Step 6	UCS-A /security/tacacs/server # **set port** *port-num*	Specifies the port used to communicate with the TACACS+ server.

The following example sets the TACACS+ timeout interval to 45 seconds, creates a server instance named tacacsserv680, sets the key to tacacskey321, and the authentication port to 5859:

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # set timeout 45
UCS-A /security/tacacs # create server tacacsserv680
UCS-A /security/tacacs/server # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCS-A /security/tacacs/server # set port 5859
```

Selecting a Primary Authentication Service

Selecting the Console Authentication Service

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **set authentication console** *auth-type*	Specifies the console authentication, where the *auth-type* argument is one of the following keywords:

	Command or Action	Purpose
		• **ldap**—Specifies LDAP authentication • **local**—Specifies local authentication • **radius**—Specifies RADIUS authentication • **tacacs**—Specifies TACACS+ authentication

The following example sets the console to use local authentication:

```
UCS-A# scope security
UCS-A /security # set authentication console local
```

Selecting the Default Authentication Service

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **set authentication default** *auth-type*	Specifies the default authentication, where the *auth-type* argument is one of the following keywords: • **ldap**—Specifies LDAP authentication • **local**—Specifies local authentication • **radius**—Specifies RADIUS authentication • **tacacs**—Specifies TACACS+ authentication

The following example sets the default authentication to LDAP:

```
UCS-A# scope security
UCS-A /security # set authentication default ldap
```