Configuring Primary Authentication

This chapter includes the following sections:

- Primary Authentication, page 1
- Remote Authentication Providers, page 1
- Creating a Remote Authentication Provider, page 3
- Selecting a Primary Authentication Service, page 8

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

If a Cisco UCS instance uses RADIUS as the remote authentication provider, you must create a cisco-avpair 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 for the Cisco UCS roles. You must create the required attribute in RADIUS.

Required User Attribute for 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.

Creating a Remote Authentication Provider

Configuring Properties for LDAP Providers

The properties that you configure in this task apply to all LDAP provider connections.

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 # **commit-buffer**	Commits the transaction to the system configuration.

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:

```
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* # commit-buffer
UCS-A /security/ldap #
```

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 login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

Configure the properties for the LDAP provider connections in Cisco UCS Manager.

If SSL will be enabled, create a trustpoint in Cisco UCS Manager containing the certificate chain of the certificate authority (CA) that signed the LDAP server's certificate.

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 # **create server** *server-name*	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.
Step 4	UCS-A /security/ldap/server # **set ssl** {**yes** | **no**}	Enables or disables the use of encryption when communicating with the LDAP server. The options are as follows: • **yes**—Encryption is required. If encryption cannot be negotiated, the connection fails. • **no**—Encryption is disabled. Authentication information is sent as clear text.

	Command or Action	Purpose
Step 5	UCS-A /security/ldap/server # **set binddn** *bind-dist-name*	Specifies the distinguished name (DN) for the LDAP database superuser account.
Step 6	UCS-A /security/ldap/server # **set key**	Specifies the password for the LDAP database superuser account. To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt.
Step 7	UCS-A /security/ldap/server # **set port** *port-num*	(Optional) Specifies the port used to communicate with the LDAP server. The standard port number is 389.
Step 8	UCS-A /security/ldap/server # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures the properties for all LDAP provider connections, then creates an LDAP server instance named 10.193.169.246 and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # set attribute CiscoAVPair
UCS-A /security/ldap # set filter sAccountName=$userid
UCS-A /security/ldap* # set basedn "DC=qalab,DC=com"
UCS-A /security/ldap* # create server 10.193.169.246
UCS-A /security/ldap/server* # set ssl yes
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 key
Enter the key:
Confirm the key:
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

What to Do Next

Select LDAP as the primary authentication service.

Configuring Properties for RADIUS Providers

The properties that you configure in this task apply to all RADIUS provider connections.

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.

	Command or Action	Purpose
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 # **commit-buffer**	Commits the transaction to the system configuration.

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
UCS-A /security/radius #
```

What to Do Next

Create a RADIUS provider.

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 # **create server** *server-name*	Creates a RADIUS server instance and enters security RADIUS server mode
Step 4	UCS-A /security/radius/server # **set authport** *authport-num*	Specifies the port used to communicate with the RADIUS server.
Step 5	UCS-A /security/radius/server # **set key**	(Optional) Sets the RADIUS server key. To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt.
Step 6	UCS-A /security/radius/server # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a server instance named radiusserv7, sets the authentication port to 5858, sets the key to radiuskey321, 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* # commit-buffer
UCS-A /security/radius/server #
```

Configuring Properties for TACACS+ Providers

The properties that you configure in this task apply to all TACACS+ provider connections.

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 # **commit-buffer**	Commits the transaction to the system configuration.

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

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 # **create server** *server-name*	Creates an TACACS+ server instance and enters security TACACS+ server mode

	Command or Action	Purpose
Step 4	UCS-A /security/tacacs/server # **set key**	(Optional) 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.
Step 5	UCS-A /security/tacacs/server # **set port** *port-num*	Specifies the port used to communicate with the TACACS+ server.
Step 6	UCS-A /security/tacacs/server # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a server instance named tacacsserv680, sets the key to tacacskey321, 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
UCS-A /security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCS-A /security/tacacs/server* # set port 5859
UCS-A /security/tacacs/server* # commit-buffer
UCS-A /security/tacacs/server #
```

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: • **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
Step 3	UCS-A /security # **commit-buffer**	Commits the transaction to the system configuration.

The following example sets the console to use local authentication and commits the transaction:

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

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 • **none**—Allows local users to log on without specifying a password • **radius**—Specifies RADIUS authentication • **tacacs**—Specifies TACACS+ authentication
Step 3	UCS-A /security # **commit-buffer**	Commits the transaction to the system configuration.

The following example sets the default authentication to LDAP and commits the transaction:

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