LDAP Authentication

LDAP Providers

You can configure remote users, assign roles and locales from Cisco UCS Central the same way as you can create LDAP users from Cisco UCS Manager. You should always create the LDAP provider from Cisco UCS Central Domain Group root.

LDAP Provider Groups

You can define up to 28 LDAP provider groups and nest them up to as many levels as the Active Directory supports for nesting in Cisco UCS Central. When you assign a provider to a nested group, even if the provider is a member of a different LDAP group, they become authenticated member of the parent nested group. During authentication, all the providers within a provider group are tried in order. If all of the configured servers are unavailable or unreachable, Cisco UCS Central automatically falls back to the local authentication method using the local username and password.

Creating an LDAP Provider

Create and configure LDAP remote users, and assign roles and locales from Cisco UCS Central, in the same manner as Cisco UCS Manager. Always create the LDAP provider from the Cisco UCS Central domain group root.

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 Central. You can choose 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 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 Central.

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 Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create server** *server-name*	• Creates an LDAP server instance • Enters LDAP security server mode

	Command or Action	Purpose
		Note • If SSL is enabled, the server-name must match a common name (CN) in the LDAP server's security certificate. • If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. • If the Cisco UCS domain is not registered with Cisco UCS Central, or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. • If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Step 7	(Optional) UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set attribute** *attribute*	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.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set basedn** *basedn-name*	The name in the LDAP hierarchy, where the server begins a search, when a remote user logs in. After log in, 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 Central using LDAP authentication.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set binddn** *binddn-name*	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 255 ASCII characters.
Step 10	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set filter** *filter-value*	Restricts the LDAP search to those user names that match the defined filter.

	Command or Action	Purpose
Step 11	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set password**	To set the password, press **Enter** after typing the **set password** command and enter the key value at the prompt.
Step 12	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set order** *order-num*	The order in which Cisco UCS Central uses this provider to authenticate users.
Step 13	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set port** *port-num*	The port through which Cisco UCS Central communicates with the LDAP database. The standard port number is 389.
Step 14	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set ssl** {**yes** | **no**}	Enables or disables encryption when communicating with the LDAP server. The options are as follows: • **yes** —Encryption required. If Cisco UCS Central cannot negotiate encryption, the connection fails. • **no** —Encryption disabled. Authentication information sent as clear text.
Step 15	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set timeout** *timeout-num*	If the LDAP provider does not receive an LDAP response within the specified period, it aborts the read attempt.
Step 16	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set vendor**	Specifies the vendor for the LDAP group. • **ms-ad** —Specifies Microsoft Active Directory. • **openldap** —Specifies OpenLDAP server.
Step 17	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the organization
- Creates an LDAP server instance named 10.193.169.246
- Configures the binddn
- Configures the password
- Configures the order
- Configures the port

- Configures the SSL settings
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # create server 10.193.169.246
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set password
Enter the password:
Confirm the password:
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set order 2
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set port 389
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set ssl yes
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set timeout 30
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap/server #
```

Configuring Default Settings 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 Central. 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

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **set attribute** *attribute*	Restricts database searches to records that contain the specified attribute.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **set basedn** *distinguished-name*	Restricts database searches to records that contain the specified distinguished name.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap* # **set filter** *filter*	Restricts database searches to records that contain the specified filter.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap* # **set timeout** *seconds*	Sets the time interval. The system waits for a response from the LDAP server before noting the server as down.
Step 10	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the LDAP attribute to CiscoAvPair
- Sets the base distinguished name to "DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
- Sets the filter to sAMAccountName=$userid
- Sets the timeout interval to 5 seconds
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # set attribute CiscoAvPair
UCSC(policy-mgr) /org/device-profile/security/ldap* # set basedn
"DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCSC(policy-mgr) /org/device-profile/security/ldap* # set filter sAMAccountName=$userid
UCSC(policy-mgr) /org/device-profile/security/ldap* # set timeout 5
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap #
```

What to do next

Create an LDAP provider.

Changing the LDAP Group Rule for an LDAP Provider

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **scope server** *ldap-provider*	Enters security LDAP provider mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/server # **scope ldap-group-rule**	Enters LDAP group rule mode.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule # **set authorization** {**enable** | **disable**}	Specifies if Cisco UCS searches LDAP groups when assigning user roles and locales to a remote user. • **disable**—Cisco UCS does not access any LDAP groups. • **enable**—Cisco UCS searches the LDAP provider groups mapped in this Cisco UCS domain. If it finds the remote user, Cisco UCS assigns the user roles and locales defined for that LDAP group in the associated LDAP group map. **Note** 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.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # **set member-of-attribute** *attr-name*	The attribute Cisco UCS uses to determine group membership in the LDAP database. The supported string length is 63 characters. The default string is **`memberOf`**.
Step 10	UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # **set traversal** {**non-recursive** | **recursive**}	Specifies if Cisco UCS inherits the settings for a group member's parent group:

	Command or Action	Purpose
		• **non-recursive**—Cisco UCS only searches those groups to which the user belongs. • **recursive**—Cisco UCS searches all of the ancestor groups belonging to the user.
Step 11	UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # **commit-buffer**	Commits the transaction to the system configuration.

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
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # scope server ldapprovider
UCSC(policy-mgr) /org/device-profile/security/ldap/server # scope ldap-group-rule
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule # set authorization
 enable
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # set
member-of-attribute memberOf
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # set traversal
 non-recursive
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule #
```

Deleting an LDAP Provider

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete server** *serv-name*	Deletes the specified server.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the LDAP server called ldap1
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # delete server ldap1
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap #
```

LDAP Group Maps

For organizations that use LDAP groups to restrict access to LDAP databases, Cisco UCS domains can use group membership information to assign a role or locale to an LDAP user during login. This eliminates the need to define roles or locale information in the LDAP user object when Cisco UCS Central deploys.

Cisco UCS Central uses LDAP group rule to determine LDAP groups when assigning user roles and locales to a remote user. When a user logs in, Cisco UCS Central retrieves information about the user's role and locale from the LDAP group map. If the role and locale criteria match the information in the policy, Cisco UCS Central provides access to the user.

The number of LDAP group maps you can define depends upon the version of Cisco UCS Manager.

You can nest LDAP group maps up to as many levels as the Windows Active Directory supports for nesting in Cisco UCS Central. When you assign a provider to a nested group, even if the provider is a member of a different LDAP group, they become an authenticated member of the parent nested group. During authentication, Cisco UCS Central tries all of the providers within a provider group in order. If Cisco UCS Central cannot reach all of the configured servers, it automatically falls back to the local authentication method using the local username and password.

Role and locale definitions are configured locally in Cisco UCS Central and do not update automatically based on changes to an LDAP directory. If you delete or rename LDAP groups in the LDAP directory, make sure to update the changes in Cisco UCS Central.

You can configure an LDAP group map to include any of the following combinations of roles and locales:

- Roles only
- Locales only
- Roles and locales

For example, if you want to configure authentication for an LDAP group representing a group of server administrators at a specific location, you can include user roles such as server-profile and server-equipment to the LDAP group. If you want to restrict access to server administrators at a specific location, you can specify locales with specific site names.

Note Cisco UCS Central includes many out-of-the-box user roles but does not include any locales. You must create a custom locale to map an LDAP provider group to a locale.

Nested LDAP Groups

You can nest LDAP groups as members of other groups to consolidate accounts and reduce replication.

By default, an LDAP group inherits user rights when nested within another group. For example, if you make Group_1 a member of Group_2, the users in Group_1 will 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 can search nested groups that are defined in LDAP group maps. Nesting groups eliminates the need to create subgroups.

Note Searching nested LDAP groups is supported for Microsoft Active Directory servers only. The supported versions are Microsoft Windows 2003 SP3, Microsoft Windows 2008 R2, and Microsoft Windows 2012.

If you include special characters in nested group names, make sure to escape them using the syntax shown in the following example.

```
create ldap-group CN=test1\\(\\),CN=Users,DC=ucsm,DC=qasam-lab,DC=in
```

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 Central (optional).

- Create custom roles in Cisco UCS Central (optional).

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create ldap-group** *group-dn*	Creates an LDAP group map for the specified DN.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **create locale** *locale-name*	Maps the LDAP group to the specified locale.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **create role** *role-name*	Maps the LDAP group to the specified role.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Maps the LDAP group mapped to a DN
- Sets the locale to pacific
- Sets the role to admin
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # create ldap-group
cn=security,cn=users,dc=lab,dc=com
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # create locale pacific
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # create role admin
```

```
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group #
```

What to do next

Set the LDAP group rule.

Deleting an LDAP Group Map

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete ldap-group** *group-dn*	Deletes the LDAP group map for the specified DN.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes an LDAP group map
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # delete ldap-group
cn=security,cn=users,dc=lab,dc=com
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap #
```

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

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope radius**	Enters RADIUS security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/radius # **set retries** *retry-num*	Sets the number of times to retry communicating with the RADIUS server before noting the server as down.
Step 7	UCSC(policy-mgr) /org/device-profile/security/radius* # **set timeout** *seconds*	Sets the time interval that the system waits for a response from the RADIUS server before noting the server as down.
Step 8	UCSC(policy-mgr) /org/device-profile/security/radius* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the RADIUS retries to 4
- Sets the timeout interval to 30 seconds
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope radius
```

```
UCSC(policy-mgr) /org/device-profile/security/radius # set retries 4
UCSC(policy-mgr) /org/device-profile/security/radius* # set timeout 30
UCSC(policy-mgr) /org/device-profile/security/radius* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/radius #
```

What to do next

Create a RADIUS provider.

Creating a RADIUS Provider

Cisco UCS Central 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 Central. You can choose 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 specifies multiples 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 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 Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope radius**	Enters RADIUS security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/radius # **create server** *server-name*	Creates a RADIUS server instance and enters security RADIUS server mode.

	Command or Action	Purpose
Step 7	(Optional) UCSC(policy-mgr) /org/device-profile/security/radius/server* # **set authport** *authport-num*	Specifies the port used to communicate with the RADIUS server.
Step 8	UCSC(policy-mgr) /org/device-profile/security/radius/server* # **set key**	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 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/radius/server* # **set order** *order-num*	Specifies when in the order this server is tried.
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/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 11	(Optional) UCSC(policy-mgr) /org/device-profile/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.
Step 12	UCSC(policy-mgr) /org/device-profile/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
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope radius
UCSC(policy-mgr) /org/device-profile/security/radius # create server radiusserv7
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set authport 5858
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set order 2
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set retries 4
```

```
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set timeout 30
UCSC(policy-mgr) /org/device-profile/security/radius/server* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/radius/server #
```

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

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters security policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope radius**	Enters RADIUS security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/radius # **delete server** *serv-name*	Deletes the specified server.
Step 7	UCSC(policy-mgr) /org/device-profile/security/radius* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the RADIUS server called radius1
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope radius
UCSC(policy-mgr) /org/device-profile/security/radius # delete server radius1
```

```
UCSC(policy-mgr) /org/device-profile/security/radius* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/radius #
```

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

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope tacacs**	Enters TACACS+ security mode. The TACACS+ related settings are applicable only for the Cisco UCS domains under the domain group root and sub-domain groups.
Step 6	UCSC(policy-mgr) /org/device-profile/security/tacacs # **set key**	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 7	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **set order** *order-num*	Specifies when in the order this server will be tried.
Step 8	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **set timeout** *seconds*	Sets the time interval that the system waits for a response from the TACACS+ server before noting the server as down.
Step 9	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **set port** *port-num*	Specifies the port used to communicate with the TACACS+ server.
Step 10	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the key to tacacskey321
- Sets the order to 4
- Sets the timeout interval to 45 seconds
- Sets the authentication port to 5859
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope tacacs
UCSC(policy-mgr) /org/device-profile/security/tacacs # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCSC(policy-mgr) /org/device-profile/security/tacacs* # set order 4
UCSC(policy-mgr) /org/device-profile/security/tacacs* # set timeout 45
UCSC(policy-mgr) /org/device-profile/security/tacacs* # set port 5859
UCSC(policy-mgr) /org/device-profile/security/tacacs* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/tacacs #
```

What to do next

Create a TACACS+ provider.

Creating a TACACS+ Provider

Cisco UCS Central 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 specifies 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 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 Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope tacacs**	Enters TACACS+ security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/tacacs # **create server** *server-name*	Creates an TACACS+ server instance and enters security TACACS+ server mode
Step 7	(Optional) UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **set key**	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 8	(Optional) UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **set order** *order-num*	Specifies when in the order this server is tried.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **set timeout** *seconds*	Sets the time interval that the system waits for a response from the TACACS+ server before noting the server as down.
Step 10	UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **set port** *port-num*	Specifies the port used to communicate with the TACACS+ server.
Step 11	UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates a server instance named tacacsserv680
- Sets the key to tacacskey321
- Sets the order to 4

- Sets the authentication port to 5859
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope tacacs
UCSC(policy-mgr) /org/device-profile/security/tacacs # create server tacacsserv680
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # set order 4
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # set timeout 45
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # set port 5859
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/tacacs/server #
```

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

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope tacacs**	Enters TACACS+ security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/tacacs # **delete server** *serv-name*	Deletes the specified server.
Step 7	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the TACACS server called tacacs1
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope tacacs
UCSC(policy-mgr) /org/device-profile/security/tacacs # delete server TACACS1
UCSC(policy-mgr) /org/device-profile/security/tacacs* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/tacacs #
```