Remote Authentication

Authentication Services

Cisco UCS Central supports the following methods for authenticating user logins:

- Local user authentication for user accounts that exist locally in Cisco UCS Central
- Remote user authentication for registered UCS domains with one of the following protocols:
  - LDAP
  - RADIUS
  - TACACS+

Guidelines and Recommendations for Remote Authentication Providers

If you configure a system for one of the supported remote authentication services, you must create a provider for that service to ensure that Cisco UCS Central can communicate with it. In addition, be aware of the following guidelines that impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in Cisco UCS Central or in the remote authentication server. You can view the temporary sessions for users who log in through remote authentication services through Cisco UCS Central GUI or Cisco UCS Central CLI.

User Roles in Remote Authentication Services

If you create user accounts in the remote authentication server, ensure that:

- Accounts include the roles those users require for working in Cisco UCS Central.
- Names of those roles match the names used in Cisco UCS Central.

Depending on the role policy, a user may not have permission to log in, or they may only have read-only privileges.

Local and Remote User Authentication Support

Cisco UCS Central uses LDAP, RADIUS and TACACS+ for remote authentication.

User Attributes in Remote Authentication Providers

When a user logs in, Cisco UCS Central:

1. Queries the remote authentication service.
2. Validates the user.
3. Checks for the roles and locales assigned to that user, (if user passed validation).

The following table contains a comparison of the user attribute requirements for the remote authentication providers supported by Cisco UCS Central.

Table 1: Comparison of User Attributes by Remote Authentication Provider

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	Do one of the following: • Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements. • Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair.	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 The following section contains a sample OID (object identifier).
RADIUS	Optional	Do one of the following: • Do not extend the RADIUS schema and use an existing unused attribute that meets the requirements. • Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.	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.

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
TACACS+	Required	You must extend the schema and create a custom attribute with the name cisco-av-pair.	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.

Sample OID for LDAP User Attribute

The following is a sample OID for a custom CiscoAVPair attribute:

```
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
```

Configuring Multiple Authentication Systems

Multiple Authentication Systems

You can configure Cisco UCS to use multiple authentication systems by configuring the following features:

- Provider groups
- Authentication domains

Once you have configured provider groups and authentication domains in Cisco UCS Central, you can use the following syntax to log in to the system using Cisco UCS Central CLI: **ucs-** *auth-domain*

When you configure multiple authentication domains and native authentication with a remote authentication service, use one of the following syntax examples to log in with SSH or Putty:

From a Linux terminal:

- **ssh ucs-***auth-domain**username@Cisco UCS domain-ip-address*

  ```
  ssh ucs-example\\jsmith@192.0.20.11
  ```

- **ssh -l ucs-***auth-domain**username* {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*}

  ```
  ssh -l ucs-example\\jsmith 192.0.20.11
  ```

- **ssh** {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*} **-l ucs-***auth-domain**username*

  ```
  ssh 192.0.20.11 -l ucs-example\\jsmith
  ```

From a Putty client:

- Login as: **ucs-***auth-domain**username*

  ```
  Login as: ucs-example\\jsmith
  ```

From a SSH client:

- Host Name: *Cisco UCS domain-ip-address*

  User Name: **ucs-***auth-domain**username*

  ```
  Host Name: 192.0.20.11
  ```

  ```
  User Name: ucs-example\\jsmith
  ```

Provider Groups

A provider group is a set of providers that Cisco UCS uses during the authentication process. Cisco UCS Central allows you to create a maximum of 16 provider groups, with a maximum of eight providers allowed per group.

During authentication, all of 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 Group

Creating an LDAP provider group allows you to authenticate using multiple LDAP databases.

Note Authenticating with a single LDAP database does not require you to set up an LDAP provider group.

Before You Begin

Create one or more LDAP providers.

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 auth-server-group** *auth-server-group-name*	Creates an LDAP provider group. Enters authentication server group security LDAP mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **create server-ref** *ldap-provider-name*	Adds the specified LDAP provider to the LDAP provider group. Enters server reference authentication server group security LDAP mode.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **set order** *order-num*	Specifies the order in which Cisco UCS uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority. Setting the order to no-value is equivalent to giving that server reference the highest priority.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Creates an LDAP provider group called ldapgroup
- Adds two previously configured providers called ldap1 and ldap2 to the provider group
- Sets the order
- 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 auth-server-group ldapgroup
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # create server-ref
```

```
ldap1
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # set order
 1
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # up
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # create server-ref
ldap2
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # set order
 2
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* #
commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref #
```

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting an LDAP Provider Group

Before You Begin

Remove the provider group from an authentication configuration.

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 auth-server-group** *auth-server-group-name*	Deletes the LDAP provider group.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Deletes an LDAP provider group called ldapgroup
- 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 auth-server-group ldapgroup
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap #
```

Creating a RADIUS Provider Group

Creating a RADIUS provider group allows you to authenticate using multiple RADIUS databases.

Note Authenticating with a single RADIUS database does not require you to set up a RADIUS provider group.

Before You Begin

Create one or more RADIUS providers.

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 auth-server-group** *auth-server-group-name*	Creates a RADIUS provider group. Enters authentication server group security RADIUS mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # **create server-ref** *radius-provider-name*	Adds the specified RADIUS provider to the RADIUS provider group. Enters server reference authentication server group security RADIUS mode.
Step 8	UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # **set order** *order-num*	Specifies the order in which Cisco UCS uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority. Setting the order to no-value is equivalent to giving that server reference the highest priority.
Step 9	UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Creates a RADIUS provider group called radiusgroup
- Adds two previously configured providers called radius1 and radius2 to the provider group
- Sets the order
- 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 auth-server-group radiusgroup
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # create server-ref
 radius1
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref* # set
order 1
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref* # up
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # create server-ref
 radius2
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref* # set
order 2
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref* #
commit-buffer
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref #
```

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting a RADIUS Provider Group

Remove the provider group from an authentication configuration.

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 # **delete auth-server-group** *auth-server-group-name*	Deletes the RADIUS provider group.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/radius* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Deletes a RADIUS provider group called radiusgroup
- 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 auth-server-group radiusgroup
UCSC(policy-mgr) /org/device-profile/security/radius* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/radius #
```

Creating a TACACS+ Provider Group

Creating a TACACS+ provider group allows you to authenticate using multiple TACACS+ databases.

Note Authenticating with a single TACACS+ database does not require you to set up a TACACS+ provider group.

Before You Begin

Create 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 # **create auth-server-group** *auth-server-group-name*	Creates a TACACS+ provider group and enters authentication server group security TACACS+ mode.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # **create server-ref** *ldap-provider-name*	Adds the specified TACACS+ provider to the TACACS+ provider group. Enters server reference authentication server group security TACACS+ mode.
Step 8	UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # **set order** *order-num*	Specifies the order in which Cisco UCS uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority. Setting the order to no-value is equivalent to giving that server reference the highest priority.
Step 9	UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Creates a TACACS+ provider group called tacacsgroup
- Adds two previously configured providers called tacacs1 and tacacs2 to the provider group
- Sets the order
- 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 auth-server-group tacacsgroup
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # create server-ref
 tacacs1
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref* # set
order 1
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref* # up
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # create server-ref
 tacacs2
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref* # set
order 2
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref* #
commit-buffer
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref #
```

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting a TACACS+ Provider Group

Remove the provider group from an authentication configuration.

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 auth-server-group** *auth-server-group-name*	Deletes the TACACS+ provider group.
Step 7	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Deletes a TACACS+ provider group called tacacsgroup
- 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 auth-server-group tacacsgroup
UCSC(policy-mgr) /org/device-profile/security/tacacs* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/tacacs #
```

Authentication Domains

Cisco UCS Central uses authentication domains to leverage multiple authentication systems. You specify and configure each authentication domain during login. If you do not specify an authentication domain, Cisco UCS Central uses the default authentication service configuration.

You can create up to eight authentication domains. Each authentication domain is associated with a provider group and realm in Cisco UCS Domain. If no provider group is specified, all servers within the realm are used.

Creating an Authentication Domain

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 auth-realm**	Enters authentication realm mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/auth-realm # **create auth-domain** *domain-name*	Creates an authentication domain and enters authentication domain mode. The Radius related settings are applicable only for the sub-domains in the domain group root and sub-domain groups. **Note** For systems using the remote authentication protocol, the authentication domain name is considered part of the username and counts toward the 32-character limit for locally created usernames. Because Cisco UCS inserts 5 characters for formatting, authentication fails if the domain name and username combined characters total exceeds 27.
Step 7	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **set refresh-period** *seconds*	(Optional) When a web client connects to Cisco UCS Central, the client must send refresh requests to Cisco UCS Central to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain.

	Command or Action	Purpose
		If the client exceeds the time limit, Cisco UCS Central considers the web session inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds.
Step 8	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **set session-timeout** *seconds*	(Optional) The maximum amount of time that can elapse after the last refresh request before Cisco UCS Central considers a web session to have ended. If the client exceeds the time limit, Cisco UCS Central automatically terminates the web session. Specify an integer between 60 and 172800. The default is 7200 seconds.
Step 9	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **create default-auth**	(Optional) Creates a default authentication for the specified authentication domain.
Step 10	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **set auth-server-group** *auth-serv-group-name*	(Optional) Specifies the provider group for the specified authentication domain.
Step 11	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **set realm** {**ldap** | **local** | **radius** | **tacacs**}	Specifies the realm for the specified authentication domain.
Step 12	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Creates an authentication domain called domain1
- Creates a web refresh period of 3600 seconds (1 hour)
- Creates a session timeout period of 14400 seconds (4 hours)
- Configures domain1 to use the providers in ldapgroup1

- Sets the realm type to ldap
- 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 auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # create auth-domain domain1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # set refresh-period
 3600
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # set session-timeout
 14400
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # create default-auth
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # set
auth-server-group ldapgroup1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # set
realm ldap
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* #
commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth #
```

Selecting the Console Authentication Service

Before You Begin

If the system uses a remote authentication service, create a provider for that authentication service. If the system uses only local authentication through Cisco UCS, you do not need to create a provider first.

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 auth-realm**	Enters authentication realm security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/auth-realm # **scope console-auth**	Enters console authorization security mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth # **set realm** *auth-type*	Specifies the console authentication, where the *auth-type* argument is one of the following keywords: • **ldap —**Specifies LDAP authentication

	Command or Action	Purpose
		• **local —**Specifies local authentication • **none —**Allows local users to log on without specifying a password • **radius —**Specifies RADIUS authentication • **tacacs —**Specifies TACACS+ authentication
Step 8	UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth* # **set auth-server-group** *auth-serv-group-name*	The associated provider group, if any.
Step 9	UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Sets the authentication to LDAP
- Sets the console authentication provider group to provider1
- 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 auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # scope console-auth
UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth # set realm local
UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth* # set auth-server-group
 provider1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth #
```

Selecting a Primary Authentication Service

Selecting the Default Authentication Service

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.

	Command or Action	Purpose
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 auth-realm**	Enters authentication realm security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/auth-realm # **scope default-auth**	Enters default authorization security mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth # **set realm** *auth-type*	Specifies the default authentication, where *auth-type* 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 8	UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth* # **set auth-server-group** *auth-serv-group-name*	(Optional) The associated provider group, if any.
Step 9	UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth* # **set refresh-period** *seconds*	(Optional) When a web client connects to Cisco UCS Central, the client must send refresh requests to Cisco UCS Central to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If the client exceeds the time limit, Cisco UCS Central considers the web session inactive, but it does not terminate the session.
Step 10	UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth* # **set session-timeout** *seconds*	(Optional) The maximum amount of time that can elapse after the last refresh request before Cisco UCS Central considers a web session to have ended. If the client exceeds the time limit, Cisco UCS Central automatically terminates the web session. Specify an integer between 60 and 172800. The default is 7200 seconds.

	Command or Action	Purpose
Step 11	UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Sets the default authentication to LDAP
- Sets the default authentication provider group to provider1
- Sets the refresh period to 7200 seconds (2 hours)
- Sets the session timeout period to 28800 seconds (8 hours)
- 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 auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # scope default-auth
UCSC(policy-mgr) /org/device-profile/security/default-auth # set realm ldap
UCSC(policy-mgr) /org/device-profile/security/default-auth* # set auth-server-group provider1
UCSC(policy-mgr) /org/device-profile/security/default-auth* # set refresh-period 7200
UCSC(policy-mgr) /org/device-profile/security/default-auth* # set session-timeout 28800
UCSC(policy-mgr) /org/device-profile/security/default-auth* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/default-auth #
```

Role Policy for Remote Users

By default, if you do not configure user roles in Cisco UCS Central, then it grants read-only access to all users logging in from a remote server.

Note

You can configure the role policy for remote users in the following ways:

- **assign-default-role**

  Does not restrict user access to Cisco UCS Central based on user roles. Cisco UCS Central grants read-only access to all users unless you defined other user roles in Cisco UCS Central.

  This is the default behavior.

- **no-login**

  Restricts user access to Cisco UCS Central based on user roles. If you did not assign user roles for the remote authentication system, access is denied.

For security reasons, you can restrict access to those users matching an established user role in Cisco UCS Central.

Configuring the Role Policy for Remote Users

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 auth-realm**	Enters authentication realm security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/auth-realm # **set remote-user default-role** {**assign-default-role** | **no-login**}	Specifies if user access to Cisco UCS Central is restricted based on user roles.
Step 7	UCSC(policy-mgr) /org/device-profile/security/auth-realm* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Sets the role policy for remote users
- 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 auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # set remote-user default-role
assign-default-role
UCSC(policy-mgr) /org/device-profile/security/auth-realm* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm #
```

Remote Access Policies

Cisco UCS Central supports global remote access policies defining the interfaces monitoring policy, displaying SSH configuration status, and providing policy settings for HTTP, Telnet, web session limits and CIM XML.

Configuring HTTP

Configuring an HTTP Remote Access Policy

Before You Begin

Create this policy before configuring an HTTP remote access policy in a domain group. Policies in the domain group root were previously created by the system and are ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create http**	(Optional) If scoping into a domain group previously created, creates the HTTP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope http**	(Optional) If scoping into the domain group root previously created, scopes the default HTTP policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/http # **enable** | **disable** {**http** | **http-redirect**}	Specifies whether the HTTP remote access policy is enabled or disabled in HTTP or HTTP-redirect mode.
Step 6	UCSC(policy-mgr) /domain-group/http* # **set http port** *port-number*	Specifies the HTTP service port number from the port range 1-65535.
Step 7	UCSC(policy-mgr) /domain-group/http* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the domain group root (which has an existing HTTP policy by default)
- Enables the HTTP remote access policy to HTTP redirect mode
- Sets the HTTP service port to 1111
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope http
UCSC(policy-mgr) /domain-group/http # enable http-redirect
UCSC(policy-mgr) /domain-group/http* # set port 1111
```

```
UCSC(policy-mgr) /domain-group/http* # commit-buffer
UCSC(policy-mgr) /domain-group/http #
```

The following example:

- Scopes into the domain group domaingroup01
- Creates the HTTP remote access policy and enable it to HTTP mode
- Sets the HTTP service port to 222
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create http
UCSC(policy-mgr) /domain-group/http* # enable http
UCSC(policy-mgr) /domain-group/http* # set port 222
UCSC(policy-mgr) /domain-group/http* # commit-buffer
UCSC(policy-mgr) /domain-group/http #
```

The following example:

- Scopes into the domain group root (which has an existing HTTP policy by default)
- Disables the HTTP remote access policy for HTTP redirect mode
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope http
UCSC(policy-mgr) /domain-group/http # disable http-redirect
UCSC(policy-mgr) /domain-group/http* # commit-buffer
UCSC(policy-mgr) /domain-group/http #
```

The following example:

- Scopes into the domain group domaingroup01
- Disables the HTTP remote access policy for HTTP mode
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group/http # disable http
UCSC(policy-mgr) /domain-group/http* # commit-buffer
UCSC(policy-mgr) /domain-group/http #
```

What to Do Next

Optionally, configure the following remote access policies:

- Telnet
- Web Session Limits
- CIM XML
- Interfaces Monitoring Policy
- SSH Configuration

Deleting an HTTP Remote Access Policy

You can delete an HTTP remote access policy from a sub-domain group under the domain group root. You cannot delete HTTP remote access policies in the domain groups root.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root. You cannot delete system default HTTP policies under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete http**	Deletes the HTTP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group/http* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the domain group domaingroup01
- Deletes the HTTP policy for that domain group
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group/domain-group # delete http
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Configuring Web Session Limits

Configuring a Web Session Limits Remote Access Policy

Before You Begin

Create this policy before configuring a web session limits remote access policy under a domain group. Policies under the domain groups root were already created by the system and are ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create web-session-limits**	(Optional) If scoping into a domain group previously created, creates the web session limits policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope web-session-limits**	(Optional) If scoping into the domain group root previously created, scopes the default web session limits policy's configuration mode from the domain group root.
Step 5	UCSC(policy-mgr) /domain-group/web-session-limits* # **set sessionsperuser** *sessions-per-user*	Sets the sessions per user limit (1-256).
Step 6	UCSC(policy-mgr) /domain-group/web-session-limits* # **set totalsessions** *total-sessions*	Sets the total sessions limit (1-256).
Step 7	UCSC(policy-mgr) /domain-group/web-session-limits* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the domain group root (which has an existing web sessions limit policy by default)
- Sets the sessions per user limit to 12 sessions
- Sets the total sessions limit to 144 sessions
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope web-session-limits
UCSC(policy-mgr) /domain-group/web-session-limits # set sessionsperuser 12
UCSC(policy-mgr) /domain-group/web-session-limits* # set totalsessions 144
UCSC(policy-mgr) /domain-group/web-session-limits* # commit-buffer
UCSC(policy-mgr) /domain-group/web-session-limits #
```

The following example:

- Scopes into the domain group domaingroup01

- Creates a web sessions limit policy
- Sets the sessions per user limit to 12 sessions
- Sets the total sessions limit to 144 sessions
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create web-session-limits
UCSC(policy-mgr) /domain-group/web-session-limits* # set sessionsperuser 12
UCSC(policy-mgr) /domain-group/web-session-limits* # set totalsessions 144
UCSC(policy-mgr) /domain-group/web-session-limits* # commit-buffer
UCSC(policy-mgr) /domain-group/web-session-limits #
```

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- CIM XML
- Interfaces Monitoring Policy

Deleting a Web Session Limits Remote Access Policy

You can delete a web session limits remote access policy from a sub-domain group in the domain group root. You cannot delete web session limits remote access policies under the domain groups root.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 3	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group in the domain group root. **Note** Do not enter the domain group root. You cannot delete system default web session limits policies under the domain group root.
Step 4	UCSC(policy-mgr) /domain-group # **delete web-session-limits**	Deletes the web session limits policy for that domain group.
Step 5	UCSC(policy-mgr) /domain-group/http* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the domain group domaingroup01

- Deletes a web sessions limit policy
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete web-session-limits
UCSC(policy-mgr) /domain-group/web-session-limits* # commit-buffer
UCSC(policy-mgr) /domain-group/web-session-limits #
```

Configuring CIM XML

Configuring a CIM XML Remote Access Policy

Before You Begin

Create the policy before configuring a CIM XML remote access policy in a sub-domain group. Policies under the domain group root were already created by the system and are ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create cimxml**	(Optional) If scoping into a domain group previously created, it creates the CIM XML policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope cimxml**	(Optional) If scoping into the domain group root previously created, it scopes the default CIM XML's policy's configuration mode from the domain group root.
Step 5	UCSC(policy-mgr) /domain-group/cimxml # **enable cimxml**	Enables CIM XML mode.
Step 6	UCSC(policy-mgr) /domain-group/cimxml* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the domain group root (which has an existing CIM XML policy by default)
- Enables CIM XML mode

- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope cimxml
UCSC(policy-mgr) /domain-group/cimxml # enable cimxml
UCSC(policy-mgr) /domain-group/cimxml* # commit-buffer
UCSC(policy-mgr) /domain-group/cimxml #
```

The following example:

- Scopes into the domain group domaingroup01
- Creates a CIM XML policy
- Enables CIM XML mode
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create cimxml
UCSC(policy-mgr) /domain-group/cimxml* # enable cimxml
UCSC(policy-mgr) /domain-group/cimxml* # commit-buffer
UCSC(policy-mgr) /domain-group/cimxml #
```

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- Web Session Limits
- Interfaces Monitoring Policy

Deleting a CIM XML Remote Access Policy

You can delete a CIM XML remote access policy from a sub-domain group in the domain group root. You cannot delete CIM XML remote access policies in the domain group root.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root. You cannot delete system default CIM XML policies under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete cimxml**	Deletes the CIM XML policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group/cimxml* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the domain group domaingroup01
- Deletes the CIM XML policy
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete cimxml
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring Interfaces Monitoring

Configuring an Interfaces Monitoring Remote Access Policy

Before You Begin

Create the monitoring remote access policy before configuring it in a domain group. Policies in the domain group root were already created by the system and are ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create mgmt-if-mon-policy**	(Optional) If scoping into a domain group previously created, creates the management interface monitor policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope mgmt-if-mon-policy**	(Optional) If scoping into the domain group root previously created, scopes the default management interface monitors policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/cimxml # **set admin-state enabled** | **disabled**	Enables or disabled the administrator status mode.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/cimxml # **set arp-deadline** *arp-response-deadline*	Enter the deadline time in minutes to wait for ARP (Address Resolution Protocol) responses (5-15).
Step 7	UCSC(policy-mgr) /domain-group/cimxml # **set arp-requests** *arp-requests*	Enter the number of ARP requests (1-5).
Step 8	UCSC(policy-mgr) /domain-group/cimxml # **set arp-target1** *arp-ip-target-1*	Enter the ARP IP Target1 (in format 0.0.0.0) to remove.
Step 9	UCSC(policy-mgr) /domain-group/cimxml # **set arp-target2** *arp-ip-target-1*	Enter the ARP IP Target2 (in format 0.0.0.0) to remove.
Step 10	UCSC(policy-mgr) /domain-group/cimxml # **set arp-target3** *arp-ip-target-1*	Enter the ARP IP Target3 (in format 0.0.0.0) to remove.
Step 11	UCSC(policy-mgr) /domain-group/cimxml # **set max-fail-reports** *arp-ip-target-1*	Enter the number of failure reports at which the interface is considered down (2-5).
Step 12	UCSC(policy-mgr) /domain-group/cimxml # **set mii-retry-count** *mii-retry-count*	Enter the maximum number of retries when using the Media Independent Interface (MII) status to perform monitoring (1-3).
Step 13	UCSC(policy-mgr) /domain-group/cimxml # **set mii-retry-interval** *mii-retry-interval*	Enter the interval between MII status monitoring retries (3-10).
Step 14	UCSC(policy-mgr) /domain-group/cimxml # **set monitor-mechanism mii-status** | **ping-arp-targets** | **ping-getaway**	Enter the MII monitoring mechanism of MII status (mii-status), ping ARP targets (ping-arp-targets), or ping getaway (ping-getaway).
Step 15	UCSC(policy-mgr) /domain-group/cimxml # **set ping-deadline** *ping-deadline*	Enter the deadline time to wait for ping responses (5-15).
Step 16	UCSC(policy-mgr) /domain-group/cimxml # **set ping-requests** *ping-requests*	Enter the number of ping requests (1-5).
Step 17	UCSC(policy-mgr) /domain-group/cimxml # **set poll-interval** *poll-interval*	Enter the polling interval in seconds (90-300).
Step 18	UCSC(policy-mgr) /domain-group/cimxml* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the domain group root (which has an existing Management Interfaces Monitoring policy by default)
- Enables Management Interfaces Monitoring mode
- Enters the status settings

- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope mgmt-if-mon-policy
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy # set admin-state enabled
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-deadline 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-requests 1
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target1 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target2 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target3 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set max-fail-reports 2
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set mii-retry-count 1
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set mii-retry-interval 3
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set monitor-mechanism ping-getaway
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set ping-deadline 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set ping-requests 1
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set poll-interval 90
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy #
```

The following example:

- Scopes into the domain group domaingroup01
- Creates the Management Interfaces Monitoring policy
- Enters the status settings
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create mgmt-if-mon-policy
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set admin-state enabled
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-deadline 15
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-requests 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target1 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target2 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target3 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set max-fail-reports 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set mii-retry-count 3
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set mii-retry-interval 10
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set monitor-mechanism ping-getaway
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set ping-deadline 15
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set ping-requests 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set poll-interval 300
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy #
```

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- Web Session Limits
- CIM XML

Deleting an Interfaces Monitoring Remote Access Policy

You can delete an interfaces monitoring remote access policy from a sub-domain group in the domain group root. You cannot delete interfaces monitoring remote access policies under the domain group root.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root. You cannot delete system default Management Interfaces Monitoring policies in the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete mgmt-if-mon-policy**	Deletes the Management Interfaces Monitoring policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the domain group domaingroup01
- Deletes the Management Interfaces Monitoring policy
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # delete mgmt-if-mon-policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```