Managing Administrators

This chapter explains how to set up network administrators at the local and regional clusters. The chapter also includes local and regional cluster tutorials for many of the administration features.

- Administrators, Groups, Roles, and Tenants, on page 1
- External Authentication Servers, on page 6
- Managing Tenants, on page 10
- Managing Administrators, on page 15
- Managing Passwords, on page 17
- Managing Groups, on page 18
- Managing Roles, on page 19
- Granular Administration, on page 20
- Centrally Managing Administrators, on page 24
- Session Management, on page 33

Administrators, Groups, Roles, and Tenants

The types of functions that network administrators can perform in Cisco Prime Network Registrar are based on the roles assigned to them. Local and regional administrators can define these roles to provide granularity for the network administration functions. Cisco Prime Network Registrar predefines a set of base roles that segment the administrative functions. From these base roles you can define further constrained roles that are limited to administering particular addresses, zones, and other network objects.

The mechanism to associate administrators with their roles is to place the administrators in groups that include these roles.

The data and configuration that can be viewed by an administrator can also be restricted by tenant. When an administrator is assigned a tenant tag, access is further restricted to configuration objects that are assigned to the tenant or made available for tenant use as read-only core configuration objects.

How Administrators Relate to Groups, Roles, and Tenants

There are four administrator objects in Cisco Prime Network Registrar—administrator, group, role, and tenant:

- **Administrator**—An account that logs in and that, through its association with one or more administrator groups, can perform certain functions based on its assigned role or roles. At the local cluster, these functions are administering the local Central Configuration Management (CCM) server and databases, hosts, zones, address space, and DHCP. At the regional cluster, these functions administer the regional CCM server and databases, central configuration, and regional address space. An administrator must be assigned to at least one group to be effective.

Adding administrators is described in Managing Administrators, on page 15.

- **Group**—A grouping of roles. You must associate one or more groups with an administrator, and a group must be assigned at least one role to be usable. The predefined groups that Cisco Prime Network Registrar provides map each role to a unique group.

  Adding groups is described in Managing Groups, on page 18.

- **Role**—Defines the network objects that an administrator can manage and the functions that an administrator can perform. A set of predefined roles are created at installation, and you can define additional constrained roles. Some of the roles include subroles that provide further functional constraints.

  Adding roles is described in Managing Roles, on page 19.

- **Tenant**—Identifies a tenant organization or group that is associated with a set of administrators. When you create tenants, the data stored on both regional and local clusters is segmented by tenant. A tenant cannot access the data of another tenant.

  Adding tenants is described in Managing Tenants, on page 10.

Administrator Types

There are two basic types of administrators: superusers and specialized administrators:

- **Superuser**—Administrator with unrestricted access to the web UI, CLI, and all features. This administrator type should be restricted to a few individuals. The superuser privileges of an administrator override all its other roles.

  Tip You have to create the superuser and password at installation, or when you first log in to the web UI.

  When a superuser is assigned a tenant tag, unrestricted access is only granted for corresponding tenant data. Data of other tenants cannot be viewed, and core objects are restricted to read-only access.

- **Specialized**—Administrator created by name to fulfill specialized functions, for example, to administer a specific DNS forward or reverse zone, based on the administrator assigned role (and subrole, if applicable). Specialized administrators, like the superuser, require a password, but must also be assigned at least one administrator group that defines the relevant roles. The CLI provides the **admin** command.

  For an example of creating a local zone or host administrator, see Create the Administrators.

  A specialized user that is assigned a tenant tag can only access corresponding tenant or core data that also matches the relevant roles. Core data is further restricted to read-only access.

Roles, Subroles, and Constraints

A license type is associated with each role-subrole combination. A role-subrole is enabled only if that license is available in that cluster.

You can limit an administrator role by applying constraints. For example, you can use the host-admin base role to create a host administrator, named 192.168.50-host-admin, who is constrained to the 192.168.50.0 subnet. The administrator assigned a group that includes this role then logs in with this constraint in effect. Adding roles and subroles is described in Managing Roles, on page 19.

You can further limit the constraints on roles to read-only access. An administrator can be allowed to read any of the data for that role, but not modify it. However, if the constrained data is also associated with a read-write role, the read-write privilege supersedes the read-only constraints.

Tip An example of adding role constraints is in Create a Host Administrator Role with Constraints.

The interplay between DNS and host administrator role assignments is such that you can combine an unconstrained dns-admin role with any host-admin role in a group. For example, combining the dns-admin-readonly role and a host-admin role in a group (and naming the group host-rw-dns-ro) provides full host access and read-only access to zones and RRs. However, if you assign a constrained dns-admin role along with a host-admin role to a group and then to an administrator, the constrained dns-admin role takes precedence, and the administrator privileges at login will preclude any host administration.

Certain roles provide subroles with which you can further limit the role functionality. For example, the local ccm-admin or regional-admin, with just the owner-region subrole applied, can manage only owners and regions. By default, all the possible subroles apply when you create a constrained role.

The predefined roles are described in Table 1: Local Cluster Administrator Predefined and Base Roles , on page 3 (local), and Table 2: Regional Cluster Administrator Predefined and Base Roles , on page 5 (regional).

Table 1: Local Cluster Administrator Predefined and Base Roles

Local Role	Subroles and Active Functionality
addrblock-admin	Core functionality: Manage address block, subnets, and reverse DNS zones (also requires dns-admin); and notify of scope activity. • *ric-management*: Push to, and reclaim subnets from, DHCP failover pairs and routers. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases, and reservations. • *lease-history*: Query, poll, and trim lease history data.
ccm-admin	Core functionality: Manage access control lists (ACLs), and encryption keys. • *authentication*: Manage administrators. • *authorization*: Manage roles and groups. • *owner-region*: Manage owners and regions. • *database*: View database change entries and trim the CCM change sets. • *security-management*: Manage ACLs and DNSSEC configuration.

Local Role	Subroles and Active Functionality
cdns-admin	Core functionality: Manage in-memory cache (flush cache and flush cache name). • *security-management*: Manage ACLs and DNSSEC configuration. • *server-management*: Manage DNSSEC configuration, as well as forwarders, exceptions, DNS64, and scheduled tasks, and stop, start, or reload the server.
cfg-admin	Core functionality: Manage clusters. • *ccm-management*: Manage the CCM server configuration. • *dhcp-management*: Manage the DHCP server configuration. • *dns-management*: Manage the DNS server configuration. • *cdns-management*: Manage Caching DNS server configuration. • *ric-management*: Manage routers. • *snmp-management*: Manage the SNMP server configuration. • *tftp-management*: Manage the TFTP server configuration.
dhcp-admin	Core functionality: Manage DHCP scopes and templates, policies, clients, client-classes, options, leases, and reservations. • *lease-history*: Query, poll, and trim lease history data. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases, and reservations. • *server-management*: Manage the DHCP server configuration, failover pairs, LDAP servers, extensions, and statistics.
dns-admin	Core functionality: Manage DNS zones and templates, resource records, secondary servers, and hosts. • *security-management*: Manage DNS update policies, ACLs, and encryption keys. • *server-management*: Manage DNS server configurations and zone distributions, synchronize zones and HA server pairs, and push update maps. • *ipv6-management*: Manage IPv6 zones and hosts. • *enum-management*: Manage DNS ENUM domains and numbers.
host-admin	Core functionality: Manage DNS hosts. (Note that if an administrator is also assigned a constrained dns-admin role that overrides the host-admin definition, the administrator is not assigned the host-admin role.)

Table 2: Regional Cluster Administrator Predefined and Base Roles

Regional Role	Subroles and Active Functionality
central-cfg-admin	Core functionality: Manage clusters and view replica data. • *dhcp-management*: Manage DHCP scope templates, policies, client-classes, failover pairs, virtual private networks (VPNs), and options; modify subnets; and replicate data. • *ric-management*: Manage routers and router interfaces, and pull replica router data. • *ccm-management*: Manage CCM Server configuration • *snmp-management*: Manage SNMP Server configuration. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases and reservations. • *cdns-management*: Manage CDNS Server configuration.
central-dns-admin	Core functionality: Manage DNS zones and templates, hosts, resource records, and secondary servers; and create subzones and reverse zones. • *security-management*: Manage DNS update policies, ACLs, and encryption keys. • *server-management*: Synchronize DNS zones and HA server pairs, manage zone distributions, pull replica zone data, and push update maps. • *ipv6-management*: Manage IPv6 zones and hosts. • *enum-management*: Manage DNS ENUM domains and numbers.
central-host-admin	Core functionality: Manage DNS hosts. (Note that if an administrator is also assigned a constrained central-dns-admin role that overrides the central-host-admin definition, the administrator is not assigned the central-host-admin role.)
regional-admin	Core functionality: Manage licenses and encryption keys. • *authentication*: Manage administrators. • *authorization*: Manage roles and groups. • *owner-region*: Manage owners and regions. • *database*: View database change entries and trim the CCM change sets. • *security-management*: Manage ACLs and DNSSEC configuration.

Regional Role	Subroles and Active Functionality
regional-addr-admin	Core functionality: Manage address blocks, subnets, and address ranges; generate allocation reports; and pull replica address space data. • *dhcp-management*: Push and reclaim subnets; and add subnets to, and remove subnets from, DHCP failover pairs. • *lease-history*: Query, poll, and trim lease history data. • *subnet-utilization*: Query, poll, trim, and compact subnet and prefix utilization data. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases and reservations.

Groups

Administrator groups are the mechanism used to assign roles to administrators. Hence, a group must consist of one or more administrator roles to be usable. When you first install Cisco Prime Network Registrar, a predefined group is created to correspond to each predefined role.

Roles with the same base role are combined. A group with an unconstrained dhcp-admin role and a constrained dns-admin role, does not change the privileges assigned to the dns-admin role. For example, if one of the roles is assigned unconstrained read-write privileges, the group is assigned unconstrained read-write privileges, even though other roles might be assigned read-only privileges. Therefore, to limit the read-write privileges of a user while allowing read-only access to all data, create a group that includes the unconstrained read-only role along with a constrained read-write role. (See Roles, Subroles, and Constraints, on page 2 for the implementation of host-admin and dns-admin roles combined in a group.)

External Authentication Servers

Cisco Prime Network Registrar includes a RADIUS client component and Active Directory (AD) client component, which are integrated with the authentication and authorization modules of the CCM server. To enable external authentication, you must configure a list of external RADIUS or an AD server at local and regional clusters, and ensure all authorized users are appropriately configured on the respective servers.

When external authentication is enabled, the CCM server handles attempts to log in via the web UI, SDK, or CLI, by issuing a RADIUS request to a RADIUS server or a LDAP request to a AD server that is selected from the configured list. If the corresponding server validates the login request, access is granted, and the CCM server creates an authorized session with the group assignments specified by the RADIUS or the AD server.

Note Any administrators defined in the CCM server's database are ignored when external authentication is enabled. Attempting to log in with these usernames and passwords will fail. To disable external authentication, you must remove or disable all the configured external servers or change the *auth-type* attribute value to Local.

Tip If all logins fail because the external authentication servers are inaccessible or misconfigured, use alternative method to login and resolve the issues. See Managing Administrators, on page 15 for more details.

Configuring a RADIUS External Authentication Server

Once you have your RADIUS server up and running and have created a user, there are some specific groups and vendor specific attributes (VSA) needed for RADIUS user to login to Cisco Prime Network Registrar. Using the Cisco vendor id (9), create the Cisco Prime Network Registrar groups attribute for each administrator, using the format **cnr:groups=**group1, group2, group3.

For example, to assign an administrator to the built-in groups **dhcp-admin-group** and **dns-admin-group**, enter:

```
cnr:groups=dhcp-admin-group,dns-admin-group
```

To assign superuser access privileges, the reserved group name **superusers** is used. To provide superuser privileges to an administrator, enter:

```
cnr:groups=superusers
```

The superuser privileges override all other groups.

The VSA name used for Cisco Prime Network Registrar is cisco-avpair. Below is an example configuration of FreeRadius server for Cisco Prime Network Registrar:

For the user: (this contains default info from the server)

```
ciscoprime Cleartext-Password := "Cisco123" -> CPNR Username/Password
       Service-Type = Framed-User,
       cisco-avpair += "cnr:groups=superusers", -> CPNR group for CNR. This is the VSA.
       Framed-Protocol = PPP,
       Framed-IP-Address = 192.168.1.2, -> CPNR IP
       Framed-Filter-Id = "std.ppp",
       Framed-MTU = 1500,
```

For the Client:

```
client CNR-HOST {
       ipaddr = 192.168.1.2 -> IP of CPNR server
       secret = P@$$W0rd! -> Password for CPNR Radius
```

Once you save and reload your RADIUS server (assuming all configuration is correct), you can then login to Cisco Prime Network Registrar using the user created in RADIUS and it will allow authentication.

Note You cannot add, delete, or modify external user names and their passwords or groups using Cisco Prime Network Registrar. You must use the RADIUS server to perform this configuration.

Adding a RADIUS External Configuration Server

To add an external configuration server, do the following:

Local Advanced and Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Radius** under the **External Authentication** submenu. The List/Add Radius Server page is displayed.

Step 2 Click the **Add Radius** icon in the Radius pane, enter the name, IPv4 and/or IPv6 address of the server you want to configure as the external authentication server, and you can set the *key* attribute which will be used for communicating with this server in the Add External Authentication Server dialog box, and click **Add External Authentication Server**. The CCM server uses the key to set the *key-secret* attribute which is the secret key shared by client and the server.

Step 3 To enable the external authentication server, check the **enabled** check box of the *ext-auth* attribute in the Edit Radius Server page, and then click **Save**.

Step 4 Change the *auth-type* attribute to RADIUS in the Manage Servers page, click **Save**, and then restart Cisco Prime Network Registrar.

Note At this point, if you are not able to login to Cisco Prime Network Registrar since local authentication is disabled, you need to create a backdoor account under /var/nwreg2/{local | regional}/conf/priv and create a file name "local.superusers" with a username and password.

CLI Commands

To create an external authentication server, use **auth-server** *name* **create** <*address* | *ip6address*> [*attribute*=*value* ...] (see the **auth-server** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Deleting a RADIUS External Authentication Server

To delete a RADIUS external authentication server, select the server in the Radius pane, click the **Delete Radius** icon, and then confirm the deletion. You can also cancel the deletion by clicking the Close button.

Configuring an AD External Authentication Server

Cisco Prime Network Registrar administrators must be assigned to one or more administrator groups to perform management functions. When using an AD server for external authentication, these are set as a vendor specific attribute for each user. Using the Cisco vendor id (9), create the Cisco Prime Network Registrar groups attribute for each administrator, using the format **cnr:groups=***group1*, *group2*, *group3*.

For example, to assign an administrator to the built-in groups **dhcp-admin-group** and **dns-admin-group**, enter:

```
cnr:groups=dhcp-admin-group,dns-admin-group
```

To assign superuser access privileges, the reserved group name **superusers** is used. To provide superuser privileges to an administrator, enter:

```
cnr:groups=superusers
```

The superuser privileges override all other groups.

A group needs to be created to access Cisco Prime Network Registrar and users need to be added to that group. Select an user attribute and provide the group information in the format **cnr:group1,group2,..**

To configure an Active Directory (AD) external authentication server:

Step 1 In AD server, create a new group, for example **CPNR**, with the group scope *Domain Local*.

Step 2 Select a user and click **Add** to a group.

Step 3 In Enter the Object Names window, select **CPNR** and click **OK**.

Step 4 In AD Server Object windows, select **CPNR** for the *ad-group-name* attribute and **info** for the *ad-user-attr-map* attribute.

Note You cannot add, delete, or modify external user names and their passwords or groups using Cisco Prime Network Registrar. You must use the AD server to perform this configuration.

Configuring Kerbero's Realm and KDC

For the Cisco Prime Network Registrar to communicate with the AD server, the Kerbero's Realm and KDC servers are required. The changes need to be configured in **krb5.conf** *(/etc/krb5.conf)* file as shown below:

```
default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
[libdefaults]
 ticket_lifetime = 1d
 default_realm = ECNR.COM
 default_tkt_enctypes = rc4-hmac
 default_tgs_enctypes = rc4-hmac
 dns_lookup_realm = false
 dns_lookup_kdc = false
 forwardable = true
[realms]
 ECNR.COM = {
 kdc = <kdc server host name>
admin_server = <kdc server host name>
 }
[domain_realm]
 .ecnr.com = ECNR.COM
 ecnr.com = ECNR.COM
```

Adding an AD External Configuration Server

To add an external configuration server, do the following:

Local Advanced and Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Active Directory** under the **External Authentication** submenu. The List/Add Active Directory Server page is displayed.

Step 2 Click the **Add Active Directory Server** icon in the Active Directory pane, enter the name, hostname of the server, and domain you want to configure as the external authentication server. You can set the base domain, LDAP user attribute map, and AD group name which will be used for communicating with this server in the Add Active Directory Server dialog box. Click **Add Active Directory Server**.

Step 3 Change the *auth-type* attribute to Active Directory in the Manage Servers page, click **Save**, and then restart Cisco Prime Network Registrar.

CLI Commands

To create an external authentication server, use **auth-server** *name* **create** <*address* | *ip6address*> [*attribute*=*value* ...].

Deleting an AD External Authentication Server

To delete an AD external authentication server, select the server in the Active Directory pane, click the **Delete Active Directory Server** icon, and then confirm the deletion. You can also cancel the deletion by clicking the Close button.

Managing Tenants

The multi-tenant architecture of Cisco Prime Network Registrar provides the ability to segment the data stored on both regional and local clusters by tenant. When tenants are defined, data is partitioned by tenant in the embedded databases of each cluster. This provides data security and privacy for each tenant, while allowing cloud or managed service providers the flexibility to consolidate many smaller customer configurations on a set of infrastructure servers, or distribute a larger customer configuration across several dedicated servers.

Any given local cluster may be associated with one or more tenants, but within a local cluster, the address pools and domain names assigned to a given tenant must not overlap.

For larger customers, clusters may be explicitly assigned to a tenant. In this case, all data on the local cluster will be associated with the tenant, and may include customized server settings. Alternatively, infrastructure servers may service many tenants. With this model, the tenants can maintain their own address space and domain names, but share common server settings that would be administered by the service provider. Their use of public or private network addresses needs to be managed by the service provider, to ensure that the tenants are assigned non-overlapping addresses.

The following are the key points you should know while configuring tenants:

- Tenant administrators are linked to their data by a tenant object that defines their tenant tag and identifier.
- Tenant objects should be consistent and unique across all clusters.
- You should not reuse tags or identifiers for different tenants.
- You can configure multiple tenants on a single cluster.
- A tenant administrator cannot create, modify, or remove tenant objects.
- A tenant administrator cannot view or modify the data of another tenant.
- Objects that are not assigned to a tenant are defined as core data, and are visible to all tenants in read-only mode.

Adding a Tenant

To add a tenant, do the following:

Local and Regional Web UI

Step 1 From the **Administration** menu, choose **Tenants** under the **User Access** submenu. This opens the List/Add Tenants page.

Step 2 Click the **Add Tenants** icon in the Tenants pane, enter the tenant tag and tenant ID and click **Add Tenant**. The Name and Description attributes are optional.

Note You cannot create more than one tenant with the same tenant ID or tenant tag.

Step 3 Click **Save**.

The Settings drop-down list on the toolbar at the top of the page will display the tenant under the **Tenant** submenu.

You can use this drop-down list to select a tenant when you have to do tenant specific configurations.

CLI Commands

To add a tenant, use **tenant** *tag* **create** *tenant-id* [*attribute*=*value*] (see the **tenant** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Editing a Tenant

To edit a tenant, do the following:

Local and Regional Web UI

Step 1 On the List/Add Tenants page, click the name of the desired tenant in the Tenants pane and the Edit Tenant page appears with the details of the selected tenant.

Step 2 You can modify the tenant tag, name, or description of the tenant on the Edit Tenant page and click **Save**. The tenant ID cannot be modified.

Deleting a Tenant

Warning **Deleting the tenant will also delete all data for the tenant.**

To delete a tenant, select the name of the desired tenant in the Tenants pane, click the **Delete** icon in the Tenants pane, and then confirm the deletion. You can also cancel the deletion by clicking the Close button.

Note A user constrained to a specific tenant cannot delete tenants.

Managing Tenant Data

You can create two types of data for tenants:

- Tenant data, which is assigned to a specified tenant and cannot be viewed by other tenants
- Core data, which is visible to all tenants in read-only mode

Local and Regional Web UI

To create tenant data objects in the web UI, do the following:

Step 1 To set the data for a desired tenant, click the Settings drop-down list on the toolbar at the top of the page and select the desired tenant under the Tenant submenu.

Step 2 Create the object.

When creating tenant data, most object names are only required to be unique for the specified tenant. For example, tenants *abc* and *xyz* may both use their own scope *test* that is private to their configuration.

Note Administrators (Admin), zones (CCMZone, CCMReverseZone, and CCMSecondaryZone), keys (Key), and clients (ClientEntry) must be unique across all tenants.

Administrator names must be unique to perform initial login authentication and establish whether the user is a tenant. Zone and key classes must be unique because these require a DNS domain name that is expected to be unique across the internet. Client names must correspond to a unique client identifier that the DHCP server can use to match its incoming requests.

Local and Regional Web UI

To create core data objects in the web UI, do the following:

Step 1 Ensure that you select **[all]** from the Settings drop-down list on toolbar at the top of the page and select the desired tenant under the Tenant submenu.

Step 2 Create the object, leaving the object tenant assignment set to **none**. By default **none** is selected in the Tenant drop-down list. Leave it as it is, so that the object is not constrained to any specific tenant.

Core data can be used to provide common configuration elements such as policies or client classes that you choose to offer to tenants. Tenants can view and reference these objects in their configuration, but cannot change or delete them. Because core data is visible to all tenants, objects names must be unique across all tenants.

CLI Commands

Use **session set tenant**=*tag* to set the selected tenant. Use **session unset tenant** to clear the tenant selection, if set (see the **session** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Note Once created, you cannot change the tenant or core designation for the object. You must delete and recreate the object to change its tenant assignment.

Tip You can use the cnr_exim tool to move a set of tenant data from one tenant to another.

Assigning a Local Cluster to a Single Tenant

When assigned to a single tenant, core data on the local cluster is not restricted to read-only access. This means tenants may be given the ability to stop and start servers, modify defaults, and install custom extensions. After the cluster is assigned to a specific tenant, other tenants cannot log in to the cluster.

Note If synchronization with the local cluster fails, the cluster will not be assigned to the tenant. Resolve any connectivity issues and use the resynchronization icon to set the local cluster tenant.

Regional Web UI

To assign a local cluster to a single tenant, do the following:

Step 1 Add the tenant in the List/Add Tenant page if you want to assign the cluster to a new tenant (see the Adding a Tenant, on page 10).

Step 2 From the **Operate** menu, Choose **Manage Clusters** under the **Servers** submenu. The List/Add Clusters page is displayed.

Step 3 Choose the tenant you added in **Step 1** from the Settings drop-down list on the toolbar at the top of the page and select the desired tenant under the Tenant submenu.

Step 4 Click the **Add Manage Clusters** icon in the Manage Clusters pane. The Add Cluster dialog box appears.

Step 5 Click **Add Cluster** to add the cluster. For information on adding the cluster, see the Create the Local Clusters.

Note Once a cluster is assigned to a particular tenant, it cannot be changed or unset.

Pushing and Pulling Tenant Data

In the regional web UI, list pages include push options that let you distribute objects to a list of local clusters, and pull options that let you merge local cluster objects from the Replica data into the central configuration. These operations can be performed on both tenant and core data, but only one set of data can be pushed or pulled in a single operation.

Use the Settings drop-down list on the toolbar at the top of the page and select the desired tenant under the Tenant submenu to specify the set of data to be pushed or pulled.

Note To maintain a consistent view of tenant data, all related clusters should be configured with the same list of tenants. See Pushing and Pulling Tenants, on page 32 for steps that help you manage tenant lists.

CLI Commands

When connected to a regional cluster, you can use the following pull, push, and reclaim commands. For push and reclaim, a list of clusters or "all" may be specified.

- **tenant** < *tag* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**]
- **tenant** < *tag* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**]

- **tenant** *tag* **reclaim** *cluster-list* [**-report-only** | **-report**]

Assigning Tenants When Using External Authentication

When external RADIUS authentication is configured, the groups that are assigned in the RADIUS server configuration establish the access privileges of the user. The implicit group name ccm-tenant-*tag* or ccm-tenant-*id* must be added to the list of groups of tenant user to designate the tenant status. Other assigned groups must be core groups or groups assigned to the same tenant. Invalid groups will be ignored when building user credentials at login.

For example, to assign superuser access for the tenant *abc*, specify the groups attribute as:

```
cnr:groups=superusers,ccm-tenant-abc
```

See External Authentication Servers, on page 6.

Using cnr_exim With Tenant Data

The cnr_exim tool lets you export tenant data, and optionally re-assign the data to a different tenant on import (See the Using the cnr_exim Data Import and Export Tool). You can use these features to:

- Create a standard set of objects for each tenant
- Move tenant data to a new tenant

Note A user constrained to a specific tenant can only export or import data for that tenant.

Creating a Standard Set of Tenant Objects

You can use a standard set of tenant objects to provide common objects such as scope and zone templates, policies, and client classes. You can use these instead of core data objects to give tenants the option to customize their settings.

To create a standard set of tenant objects, do the following:

Step 1 Create a template tenant user to use as a placeholder, with tag=*template* and id=*9999*, and create the set of objects to be reused for each tenant.

Step 2 Use the cnr_exim tool to export the template configuration:

```
cnr_exim  -f template -x -e template.bin
```

Step 3 Use the cnr_exim tool to import the template configuration for the tenant *abc* :

```
cnr_exim -f  template -g abc -i template.bin
```

Note The template tenant user does not need to be present on the cluster to import the data, which lets you reuse the template.bin export file on other clusters. Once you have created the export file, you can also delete the placeholder tenant on the original cluster to remove all associated template data, if desired.

Moving Tenant Data

The ID of a tenant can only be changed by deleting and re-creating the tenant. To retain the data of the tenant when this is required, do the following (assuming the tenant tag for the tenant is *xyz*):

Step 1 Use the cnr_exim tool to export the configuration for the tenant *xyz*:

```
cnr_exim -f xyz -x -e xyz.bin
```

Step 2 Delete the tenant *xyz*.

Step 3 Recreate the tenant with the corrected tenant id.

Step 4 Use the cnr_exim tool to re-import the configuration:

```
cnr_exim -f xyz -g  xyz -i xyz.bin
```

Managing Administrators

When you first log in, Cisco Prime Network Registrar will have one administrator—the superuser account. This superuser can exercise all the functions of the web UI and usually adds the other key administrators. However, ccm-admin and regional-admin administrators can also add, edit, and delete administrators. Creating an administrator requires:

- Adding its name.
- Adding a password.
- Specifying if the administrator should have superuser privileges (usually assigned on an extremely limited basis).
- If not creating a superuser, specifying the group or groups to which the administrator should belong. These groups should have the appropriate role (and possibly subrole) assignments, thereby setting the proper constraints.

If you accidentally delete all the roles by which you can log in to Cisco Prime Network Registrar (those having superuser, ccm-admin, or regional-admin privileges), you can recover by creating an admin name/password pair in the /var/nwreg2/{local | regional}/conf/priv/local.superusers file. You must create this file and include a line in it with the format *admin password*. Use this admin name and password for the next login session. All users in the local.superusers file must be prefixed with "local$". This helps to identify when the local.superusers file is used, as all users are prefixed by local$. Users that start with local$ will be validated against the local.superusers file entries. They will neither be checked against users in the local CCM user database nor using external authentication.

Note

- As admin names are case blind, the local$ and internal$ prefixes are case blind as well.
- When using **nrcmd -N** *admin* with a local$ or internal$ user, one must escape the $ (so, use local\$ or internal\$). The alternative is to let nrcmd prompt one for the user, as then no escaping is needed.

Important Using the local.superusers file causes reduced security. Therefore, use this file only in emergencies such as when temporarily losing all login access. After you log in, create a superuser account in the usual way, then delete the local.superusers file or its contents. You must create a new administrator account for each individual, to track administrative changes.

If you want to keep this file in place, make sure it is protected against general read access (read access to it is only needed by ccmsrv).

If external authentication is enabled and login fails because the external authentication servers are inaccessible or misconfigured, you can log in using any administrators defined in the CCM server's database. In this case, the username should be prefixed with “internal$” (during login) to specify that internal CCM server’s database should be used for authentication and authorization of administrator.

Adding Administrators

To add an administrator, do the following:

Local and Regional Web UI

Step 1 From the **Administration** menu, choose **Administrators** under the **User Access** submenu. This opens the List/Add Administrators page (see the Create the Administrators for an example).

Step 2 Click the **Add Administrators** icon in the Administrators pane, enter the name in the Name field, enter the password in the Password field, retype the password in the Confirm Password field in the Add Admin dialog box, and then click **Add Admin**.

Step 3 Choose one or more existing groups from the Groups Available list (or whether the administrator should be a superuser) and then click **Save**.

Editing Administrators

To edit an administrator, select the administrator in the Administrators pane, modify the name, password, superuser status, or group membership on the Edit Administrator page, and then click **Save**. The active group or groups should be in the Selected list.

You can select the **Unlimited Sessions?** checkbox to indicate that the administrator is permitted an unlimited number of concurrent token and user sessions, when a session limit has been configured. For more information, see Session Management, on page 33.

Note The web UI logs out whenever there is a change in user role for the currently logged in admins.

Deleting Administrators

To delete an administrator, select the administrator in the Administrators pane, click the **Delete Administrators** icon, and then confirm or cancel the deletion.

Suspending/Reinstating Administrators

To suspend login access for an administrator, select the administrator in the Administrators pane, click the **Suspend** button at the top of the Edit Administrator page on the right pane.

Note When administrator login is enabled, only the Suspend action will be available. When suspended, only the Reinstate action will be available.

CLI Commands

Use **admin** *name* **create** [*attribute*=*value*] to create an administrator.

Use **admin** *name* **delete** to delete an administrator.

Use **admin** *name* **suspend** to suspend login access for administrators.

Use **admin** *name* **reinstate** to reinstate login access for administrators.

When connected to a regional cluster, you can use the following pull, push, and reclaim commands. For push and reclaim, a list of clusters or "all" may be specified. For push, unless **-omitrelated** is specified, associated roles and groups are also pushed (using replace mode).

- **admin** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**]
- **admin** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-report-only** | **-report**]
- **admin** *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

Managing Passwords

Passwords are key to administrator access to the web UI and CLI. In the web UI, you enter the password on the Login page. In the CLI, you enter the password when you first invoke the **nrcmd** program. The local or regional CCM administrator or superuser can change any administrator password.

You can prevent exposing a password on entry. In the web UI, logging in or adding a password never exposes it on the page, except as asterisks. In the CLI, you can prevent exposing the password by creating an administrator, omitting the password, then using **admin** *name* **enterPassword**, where the prompt displays the password as asterisks. You can do this instead of the usual **admin** *name* **set password** command that exposes the password as plain text.

Administrators can change their own passwords on clusters. If you want the password change propagated from the regional server to all local clusters, log in to the regional cluster. First ensure that your session admin-edit-mode is set to synchronous, and then update your password.

Note The password should not be more than 255 characters long.

Managing Groups

A superuser, ccm-admin, or regional-admin can create, edit, and delete administrator groups. Creating an administrator group involves:

- Adding its name.
- Adding an optional description.
- Choosing associated roles.

Adding Groups

To add a group, do the following:

Local Advanced and Regional Web UI

Step 1 From the **Administration** menu, choose **Groups** under the **User Access** submenu. This opens the List/Add Administrator Groups page (see the Create a Group to Assign to the Host Administrator for an example).

Step 2 Click the **Add Groups** icon in the Groups pane, enter a name and an optional description in the Add CCMAdminGroup dialog box, and then click **Add CCMAdminGroup**.

Step 3 Choose one or more existing roles from the **Roles Available** list and then click **Save**.

Editing Groups

To edit a group, click the name of the group that you want to edit in the Groups pane to open the Edit Administrator Group page. You can modify the name, description, or role membership in this page. You can view the active roles in the Selected list.

Deleting Groups

To delete a group, select the group in the Groups pane, click the **Delete Groups** icon, and then confirm the deletion. You can also cancel the deletion by clicking the Close button.

CLI Commands

Use **group** *name* **create** [*attribute*=*value*] to create a group.

Use **group** *name* **delete** to delete a group.

When connected to a regional cluster, you can use the following pull, push, and reclaim commands. For push and reclaim, a list of clusters or "all" may be specified. The push operation will also push the related roles (using replace mode) and related owners and regions (using ensure mode) unless **-omitrelated** is specified to prevent this.

- **group** < *name* | **all** > **pull** < **ensure** | **replace** > *cluster-name* [**-report-only** | **-report**]
- **group** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-report-only** | **-report**]

- **group** *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

Managing Roles

A superuser, ccm-admin, or regional-admin administrator can create, edit, and delete administrator roles. Creating an administrator role involves:

- Adding its name.
- Choosing a base role.
- Possibly specifying if the role should be unconstrained, or read-only.
- Possibly adding constraints.
- Possibly assigning groups.

Adding Roles

To add a role, do the following:

Local Advanced and Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Roles** under the **User Access** submenu. This opens the List/Add Administrator Roles page.

Step 2 Click the **Add Role** icon in the Roles pane, enter a name, and choose a tenant and a base role in the Add Roles dialog box, and then click **Add Role**.

Step 3 On the List/Add Administrator Roles page, specify any role constraints, subrole restrictions, or group selections, then click **Save**.

Editing Roles

To edit a role, select the role in the Roles pane, then modify the name or any constraints, subrole restrictions, or group selections on the Edit Administrator Role page. The active subroles or groups should be in the Selected list. Click **Save**.

Deleting Roles

To delete a role, select the role in the Roles pane, click the **Delete Role** icon, and then confirm the deletion.

Note You cannot delete the default roles.

CLI Commands

To add and edit administrator roles, use **role** *name* **create** *base-role* [*attribute*=*value*] (see the **role** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions). The base roles have default groups associated with them. To add other groups, set the *groups* attribute (a comma-separated string value).

When connected to a regional cluster, you can use the following pull, push, and reclaim commands. The push and reclaim commands allow a list of clusters or "all". The push operation will also push the related groups (using replace mode) and related owners and regions (using ensure mode). The pull operation will pull the related owners and regions (using ensure mode). For either operation, specify **-omitrelated** to prevent this and just push or pull the role.

- **role** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**]
- **role** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-report-only** | **-report**]
- **role** *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

Granular Administration

Granular administration prevents unauthorized users from accidentally making a change on zones, address blocks, subnets, and router interfaces. It also ensures that only authorized users view or modify specific scopes, prefixes, and links. Granular administration constraints administrators to specific set of scopes, prefixes, and links. A constrained administrator can view or make changes to authorized scope, prefix, and link objects only. The CCM server uses owner and region constraints to authorize and filter IPv4 address space objects, and DNS zone related objects (CCMZone, CCMReverseZone, CCMSecondaryZone, CCMRRSet, and CCMHost). The zones are constrained by owners and regions. Owner or region attributes on the CCMSubnet control access to scopes. Also, owner or region attributes on the Prefix and Link objects control access to prefixes and links.

Local Advanced and Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Roles** to open the List/Add Administrator Roles page.

Step 2 Click the **Add Role** icon in the Roles pane, enter a name for the custom role, for example, my-dhcp, choose a tenant, and choose **dhcp-admin** from the Role drop-down list and click **Add Role**.

Step 3 Click **True** or **False** radio button as necessary, on the Add DHCP Administrator Role page.

Step 4 Choose the required sub roles in the Available field and move them to the Selected field.

Step 5 Click **Add Constraint**.

a) On the Add Role Constraint page, modify the fields as necessary.

b) Click **Add Constraint**. The constraint must have an index number of 1.

Step 6 Click **Save**.

The name of the custom role appears on the list of roles in the List/Add Administrator Roles page.

Related Topics

Scope-Level Constraints, on page 21

Prefix-Level Constraints, on page 22

Link-Level Constraints, on page 23

Scope-Level Constraints

A dhcp admin user can view or modify a scope if any of the following conditions is met:

- Owner of the subnet for the scope matches the dhcp-admin owner.
- Region of the subnet for the scope matches the region role constraints.
- Owner or region of the parent address block matches the dhcp-admin owner or region role constraints. Note that the most immediate parent address block that has owner or region defined takes precedence.

The following conditions are also valid:

- If the matching owner or region constraint is marked as read-only, you can only view the scope.
- If a scope has a primary network defined, the primary subnet and its parent address block owner or region constraints override secondary subnets.
- If no parent subnet or address block defines owner or region constraints, then you can access the scope.
- If you are an unconstrained dhcp-admin user, you can have access to all scopes.

Note These hierarchical authorization checks for dhcp-admin owner/region constraints are applicable to scopes, subnets, and parent address blocks. Identical hierarchical authorization checks for addrblock-admin owner/region constraints apply to address blocks and subnets. If you have dhcp-admin and the addrblock-admin privileges, you can access address blocks and subnets, if either of the roles allow access.

Examples of Scope-Level Constraints:

```
Parent CCMAddrBlock 10.0.0.0/8 has owner 'blue' set.
    Scope 'A' has subnet 10.0.0.0/24 has parent CCMSubnet with owner 'red'.
    Scope 'B' has subnet 10.0.1.0/24 has parent CCMSubnet with no owner set.
    Scope 'C' has subnet 10.10.0.0/24 has parent CCMSubnet with owner 'green' and
primary-subnet 10.0.0.0/24.
    Scope 'D' has subnet 100.10.0.0/24 has parent CCMSubnet with owner unset, and no parent
 block.

    Scope 'A' owner is 'red'.
    Scope 'B' owner is 'blue'.
    Scope 'C' owner is 'red'.
    Scope 'D' owner is unset. Only unconstrained users can access this scope.
```

Local Advanced Web UI

To add scopes, do the following:

Step 1 From the **Design** menu, choose **Scopes** under the **DHCPv4** submenu to open the List/Add DHCP Scopes.

Step 2 Click the **Add Scopes** icon in the Scopes pane, enter a name, subnet, primary subnet, choose policy, enter a selection-tag-list, and select the scope template in the Add DHCP Scope dialog box.

Step 3 Click **Add DHCP Scope**. The List/Add DHCP Scopes page appears.

Step 4 Enter values for the fields or attributes as necessary.

Step 5 To unset any attribute value, check the check box in the **Unset?** column, then click **Unset Fields** at the bottom of the page.

Step 6 Click **Save** to add scope or **Revert** to cancel the changes.

Tip If you add new scope values or edit existing ones, click **Save** to save the scope object.

Prefix-Level Constraints

You can view or modify a prefix, if you have either of the following:

- The ipv6-management subrole of the dhcp-admin, or addrblock-admin role on the local cluster.
- The central-cfg-admin, or regional-addr-admin role on the regional cluster.

You can view or modify a prefix if any of the following conditions is true:

- The owner or region of the parent link matches the owner or region role constraints defined for you.
- The owner or region of this prefix matches the owner or region role constraints defined for you.
- The owner or region of the parent prefix matches the owner or region role constraints defined for you.

You can view or modify a prefix if any of the following conditions is true:

- If the matching owner or region constraint for you is marked as read-only, then you can only view the prefix.
- If the prefix references a parent link, the link owner or region constraints is applicable if the link owner or region constraints set.
- If no parent link or prefix defines any owner or region constraints, then you can access this prefix only if owner or region role constraints are not defined for you.
- If you are an unconstrained user, then you have access to all.

Examples of Prefix-Level constraints:

```
Link 'BLUE' has owner 'blue' set.
    Parent Prefix 'GREEN' has owner 'green' set.
    Prefix 'A' has owner 'red' set, no parent prefix, and no parent link.
    Prefix 'B' has owner 'yellow' set, parent Prefix 'GREEN' and parent link 'BLUE'.
    Prefix 'C' has no owner set, parent prefix 'GREEN', and no parent link.
    Prefix 'C' has no owner set, no parent prefix, and no parent link.

    Prefix 'A' owner is 'red'.
    Prefix 'B' owner is 'blue'.
    Prefix 'C' owner is 'green'.
    Prefix 'D' owner is unset. Only unconstrained users can access this prefix.
```

Local Advanced and Regional Advanced Web UI

To view unified v6 address space, do the following:

Step 1 From the **Design** menu, choose **Address Tree** under the **DHCPv6** submenu to open the DHCP v6 Address Tree page.

Step 2 View a prefix by adding its name, address, and range, then choosing a DHCP type and possible template (see the *"Viewing IPv6 Address Space" section in Cisco Prime Network Registrar 11.2 DHCP User Guide*).

Step 3 Choose the owner from the owner drop-down list.

Step 4 Choose the region from the region drop-down list.

Step 5 Click **Add Prefix**. The newly added Prefix appears on the DHCP v6 Address Tree page.

Local Advanced and Regional Advanced Web UI

To list or add DHCP prefixes, do the following:

Step 1 From the **Design** menu, choose **Prefixes** under the **DHCPv6** submenu to open the List/Add DHCP v6 Prefixes page.

Step 2 Click the **Add Prefixes** icon in the Prefixes pane, enter a name, address, and range for the prefix, then choose the DHCP type and possible template.

Step 3 Choose the owner from the owner drop-down list.

Step 4 Choose the region from the region drop-down list.

Step 5 Click **Add IPv6 Prefix**. The newly added Prefix appears on the List/Add DHCP v6 Prefixes page and also under the Prefixes pane on the left.

Link-Level Constraints

You can view or modify a link if:

- You are authorized for the ipv6-management subrole of the dhcp-admin or addrblock-admin role on the local cluster, or the central-cfg-admin or regional-addr-admin role on the regional cluster.
- The owner or region of the link matches the owner or region role constraints defined for you.
- No owner or region is defined for the link, and only if no owner or region role constraints are defined for you.

If you are an unconstrained user, then you have access to all links.

The following is an example of Link Level Constraints:

```
Link 'BLUE' has owner 'blue' set.
    Link 'ORANGE' has owner unset.

    Link 'BLUE' owner is 'blue'.
    Link 'ORANGE' owner is unset. Only unconstrained users can access this link.
```

Local and Regional Web UI

To add links, do the following:

Step 1 From the **Design** menu, choose **Links** under the **DHCPv6** submenu to open the List/Add DHCP v6 Links page.

Step 2 Click the **Add Links** icon in the Links pane, enter a name, then choose the link type, and enter a group.

Step 3 Click **Add Link**. The newly added DHCPv6 Link appears on the List/Add DHCP v6 Links page.

Centrally Managing Administrators

As a regional or local CCM administrator, you can:

- Create and modify local and regional cluster administrators, groups, and roles.
- Push administrators, groups, and roles to local clusters.
- Pull local cluster administrators, groups, and roles to the central cluster.

Each of these functions involves having at least one regional CCM administrator subrole defined. The following table describes the subroles required for these operations.

Table 3: Subroles Required for Central Administrator Management

Central Administrator Management Action	Required Regional Subroles
Create, modify, push, pull, or delete administrators	authentication
Create, modify, push, pull, or delete groups or roles	authorization
Create, modify, push, pull, or delete groups or roles with associated owners or regions	authorization owner-region
Create, modify, push, pull, or delete external authentication servers	authentication
Create, modify, push, pull, or delete tenants	authentication

Pushing and Pulling Administrators

You can push administrators to, and pull administrators from local clusters on the List/Add Administrators page in the regional cluster web UI.

You can create administrators with both local and regional roles at the regional cluster. However, you can push or pull only associated local roles, because local clusters do not recognize regional roles.

Pushing Administrators to Local Clusters

Pushing administrators to local clusters involves choosing one or more clusters and a push mode.

Regional Web UI

Step 1 From the **Administration** menu, choose **Administrators**.

Step 2 On the List/Add Administrators Page, click the **Push All** icon in the Administrators pane to push all the administrators listed on the page. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode by clicking one of the Data Synchronization Mode radio buttons. If you are pushing all the administrators, you can choose Ensure, Replace, or Exact. If you are pushing a single administrator, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing administrator data at the local cluster. You would choose Exact only if you want to create an exact copy of the administrator database at the local cluster, thereby deleting all administrators that are not defined at the regional cluster.

Step 4 Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

Step 5 Click **Push Data to Clusters**.

Step 6 On the View Push Data Report dialog box, view the push details, then click **OK** to return to the List/Add Administrators page.

CLI Command

When connected to a regional cluster, you can use the **admin** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-report-only** | **-report**] command. A list of clusters or "all" may be specified. For push, unless **-omitrelated** is specified, associated roles and groups are also pushed (using replace mode).

Pushing Administrators Automatically to Local Clusters

You can automatically push the new user name and password changes from the regional cluster to the local cluster. To do this, you must enable the synchronous edit mode in the regional cluster. The edit mode is set for the current web UI session, or set as default for all users is set in the CCM Server configuration.

When synchronous mode is set, all the subsequent changes to user name and password are synchronized with local clusters. You can modify your password on the regional server, and this change is automatically propagated to local clusters.

If you are an admin user, you can make multiple changes to the user credentials on the regional cluster. All these changes are automatically pushed to local clusters.

Regional Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under **Servers** submenu to open the Manage Servers page.

Step 2 Click **CCM** in the Manage Servers pane to open the Edit Local CCM Server page.

Step 3 Choose the synchronous radio buttons for the regional edit mode values for admin, dhcp, and dns.

Step 4 Choose the webui mode value from the **webui-mode** drop-down list.

Step 5 Enter the idle-timeout value.

Step 6 To unset any attribute value, check the check box in the **Unset?** column, then click **Unset Fields** at the bottom of the page. To unset the attribute value or to change it, click **Save**, or **Cancel** to cancel the changes.

Note Enter values for the attributes marked with asterisks because they are required for CCM server operation. You can click the name of any attribute to open a description window for the attribute.

Connecting to CLI in Regional Mode

You must connect to the CLI in Regional Mode. The -R flag is required for regional mode. To set the synchronous edit mode:

```
nrcmd-R> session set admin-edit-mode=synchronous
```

Pulling Administrators from the Replica Database

Pulling administrators from the local clusters is mainly useful only in creating an initial list of administrators that can then be pushed to other local clusters. The local administrators are not effective at the regional cluster itself, because these administrators do not have regional roles assigned to them.

When you pull an administrator, you are actually pulling it from the regional cluster replica database. Creating the local cluster initially replicates the data, and periodic polling automatically updates the replication. However, to ensure that the replica data is absolutely current with the local cluster, you can force an update before pulling the data.

Regional Web UI

Step 1 From the **Administration** menu, choose **Administrators** under the **User Access** submenu.

Step 2 On the List/Add Administrators page, click **Pull Data** on the Administrators pane. This opens the Select Replica Admin Data to Pull dialog box.

Step 3 Click the **Replica** icon in the **Update Replica Data** column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data.)

Step 4 Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing administrator properties already defined at the regional cluster by choosing Ensure, or create an exact copy of the administrator database at the local cluster by choosing Exact (not recommended).

Step 5 Click **Pull Core Administrators** next to the cluster, or expand the cluster name and click **Pull Administrator** to pull an individual administrator in the cluster.

Step 6 On the Select Replica Admin Data to Pull dialog box, view the change set data, then click **OK**. You return to the List/Add Administrators page with the pulled administrators added to the list.

Note If you do not have a regional cluster and would like to copy administrators, roles, or groups from one local cluster to another, you can export them and then reimport them at the target cluster by using the cnr_exim tool (see the Using the cnr_exim Data Import and Export Tool). However, the tool does not preserve the administrator passwords, and you must manually reset them at the target cluster. It is implemented this way to maintain password security. The export command is:

```
cnr_exim -c admin -x -e outputfile.txt
```

CLI Command

When connected to a regional cluster, you can use the **admin** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] command.

Pushing and Pulling External Authentication Servers

You can push all external authentication servers to local cluster or pull the external authentication server data from the local cluster on the List/Add RADIUS Server page or List/Add Active Directory Server page in the regional web UI.

Pushing RADIUS External Authentication Servers

To push external authentication servers to the local cluster, do the following:

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Radius** under the **External Authentication** submenu to view the List/Add RADIUS Server page in the regional web UI.

Step 2 Click **Push All** icon in the Radius pane to push all the external authentication servers listed on the page, or **Push** to push an individual external authentication server. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons.

- If you are pushing all the external authentication servers, you can choose Ensure, Replace, or Exact.
- If you are pushing a single external authentication server, you can choose Ensure or Replace.

In both the above cases, Ensure is the default mode.

Choose Replace only if you want to replace the existing external authentication server data at the local cluster. Choose Exact only if you want to create an exact copy of the external authentication server data at the local cluster, thereby deleting all external authentication servers that are not defined at the regional cluster.

Step 4 Click **Push Data to Clusters**.

Pulling RADIUS External Authentication Servers

To pull the external authentication server data from the local cluster, do the following:

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Radius** under the **External Authentication** submenu to view the List/Add Radius Server page in the regional web UI.

Step 2 On the List/Add Radius Server page, click **Pull Data** on the Radius pane. This opens the Select Replica External Authentication Server Data to Pull dialog box.

Step 3 Click the **Replica** icon in the **Update Replica Data** column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data.)

Step 4 Choose a replication mode using one of the Mode radio buttons.

Leave the default Replace mode enabled, unless you want to preserve any existing external authentication server properties at the local cluster by choosing Ensure.

Note We do not recommend that you create an exact copy of the external authentication server data at the local cluster by choosing Exact.

Step 5 Click **Pull All External Authentication Servers** next to the cluster.

Step 6 On the Report Pull Replica Authentication servers page, view the pull details, then click **Run**.

On the Run Pull Replica Authentication servers page, view the change set data, then click **OK**. You return to the List/Add Authentication Server page with the pulled external authentication servers added to the list.

Pushing AD External Authentication Servers

To push external authentication servers to the local cluster, do the following:

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Active Directory** under the **External Authentication** submenu to view the List/Add Active Directory Server page in the regional web UI.

Step 2 Click **Push All** on the Active Directory pane to push the external authentication server. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons.

- If you are pushing all the external authentication servers, you can choose Ensure, Replace, or Exact.
- If you are pushing a single external authentication server, you can choose Ensure or Replace.

  In both the above cases, Ensure is the default mode.

Choose Replace only if you want to replace the existing external authentication server data at the local cluster. Choose Exact only if you want to create an exact copy of the external authentication server data at the local cluster, thereby deleting all external authentication servers that are not defined at the regional cluster.

Step 4 Click **Push Data to Clusters**.

CLI Command

When connected to a regional cluster, you can use the **auth-ad-server** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] command. A list of clusters or "all" may be specified.

Pulling AD External Authentication Servers

To pull the AD external authentication server data from the local cluster, do the following:

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Active Directory** under the **External Authentication** submenu to view the List/Add Active Directory Server page in the regional web UI.

Step 2 On the List/Add Active Directory Server page, click **Pull Data** on the Active Directory pane. This opens the Select Replica External Authentication Server Data to Pull dialog box.

Step 3 Click the **Replica** icon in the **Update Replica Data** column for the cluster (For the automatic replication interval, see the Replicating Local Cluster Data).

Step 4 Choose a replication mode using one of the Mode radio buttons.

Leave the default Replace mode enabled, unless you want to preserve any existing external authentication server properties at the local cluster by choosing Ensure.

Note We do not recommend that you create an exact copy of the external authentication server data at the local cluster by choosing Exact.

Step 5 Click **Pull All External Authentication Servers** next to the cluster.

Step 6 On the Report Pull Replica Authentication servers page, view the pull details, and then click **Run**.

On the Run Pull Replica Authentication servers page, view the change set data, and then click **OK**. You return to the List/Add Authentication Server page with the pulled external authentication servers added to the list.

CLI Command

When connected to a regional cluster, you can use the **auth-ad-server** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] command.

Pushing and Pulling Groups

Pushing and pulling groups is vital in associating administrators with a consistent set of roles at the local clusters. You can push groups to, and pull groups from, local clusters on the List/Add Administrator Groups page in the regional cluster web UI.

Pushing Groups to Local Clusters

Pushing groups to local clusters involves choosing one or more clusters and a push mode.

Regional Web UI

Step 1 From the **Administration** menu, choose **Groups** under the **User Access** submenu.

Step 2 On the List/Add Administrator Groups page, click the **Push All** icon on Groups pane to push all the groups listed on the page, or **Push** to push an individual group. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons. If you are pushing all the groups, you can choose Ensure, Replace, or Exact. If you are pushing a single group, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing group data at the local cluster. You would choose Exact only if you want to create an exact copy of the group data at the local cluster, thereby deleting all groups that are not defined at the regional cluster.

Step 4 By default, the associated roles and owners are pushed along with the group. Roles are pushed in Replace mode and owners in Ensure mode. To disable pushing the associated roles or owners, uncheck the respective check box.

Step 5 Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

Step 6 Click **Push Data to Clusters**.

Step 7 On the View Push Group Data Report page, view the push details, then click **OK** to return to the List/Add Administrator Groups page.

CLI Command

When connected to a regional cluster, you can use the **group** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-report-only** | **-report**] command. A list of clusters or "all" may be specified. This operation will also push the related roles (using replace mode) and related owners and regions (using ensure mode). To prevent this and to just push the group, specify **-omitrelated**.

Pulling Groups from the Replica Database

Pulling administrator groups from the local clusters is mainly useful only in creating an initial list of groups that can then be pushed to other local clusters. The local groups are not useful at the regional cluster itself, because these groups do not have regional roles assigned to them.

When you pull a group, you are actually pulling it from the regional cluster replica database. Creating the local cluster initially replicates the data, and periodic polling automatically updates the replication. However, to ensure that the replica data is absolutely current with the local cluster, you can force an update before pulling the data.

Regional Web UI

Step 1 From the **Administration** menu, choose **Groups** under the **User Access** submenu.

Step 2 On the List/Add Administrator Groups page, click the **Pull Data** icon on the Groups pane. This opens the Select Replica CCMAdminGroup Data to Pull dialog box.

Step 3 Click the **Replica** icon in the **Update Replica Data** column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data.)

Step 4 Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing group properties at the local cluster by choosing Ensure, or create an exact copy of the group data at the local cluster by choosing Exact (not recommended).

Step 5 Click **Pull Core Groups** next to the cluster, or expand the cluster name and click **Pull Group** to pull an individual group in the cluster.

Step 6 On the Report Pull Replica Groups page, view the pull details, then click **Run**.

Step 7 On the Run Pull Replica Groups page, view the change set data, then click **OK**. You return to the List/Add Administrator Groups page with the pulled groups added to the list.

CLI Command

When connected to a regional cluster, you can use the **group** < *name* | **all** > **pull** < **ensure** | **replace** > *cluster-name* [**-report-only** | **-report**] command.

Pushing and Pulling Roles

You can push roles to, and pull roles from, local clusters on the List/Add Administrator Roles page in the regional cluster web UI. You can also push associated groups and owners, and pull associated owners, depending on your subrole permissions (see Table 3: Subroles Required for Central Administrator Management , on page 24).

Pushing Roles to Local Clusters

Pushing administrator roles to local clusters involves choosing one or more clusters and a push mode.

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Roles** under the **User Access** submenu.

Step 2 On the List/Add Administrator Roles page, click the **Push All** icon in the Roles pane to push all the roles listed on the page, or **Push** to push an individual role. This opens the Push Data to Local Clusters dialog box.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons. If you are pushing all the roles, you can choose Ensure, Replace, or Exact. If you are pushing a single role, you can choose Ensure or Replace. In both cases, Ensure is the default mode. You would choose Replace only if you want to replace the existing role data at the local cluster. You would choose Exact only if you want to create an exact copy of the role data at the local cluster, thereby deleting all roles that are not defined at the regional cluster.

Step 4 By default, the associated groups and owners are pushed along with the role. Groups are pushed in Replace mode and owners in Ensure mode. To disable pushing the associated roles or owners, uncheck the respective check box:

- If you disable pushing associated groups and the group does not exist at the local cluster, a group based on the name of the role is created at the local cluster.
- If you disable pushing associated owners and the owner does not exist at the local cluster, the role will not be configured with its intended constraints. You must separately push the group to the local cluster, or ensure that the regional administrator assigned the owner-region subrole has pushed the group before pushing the role.

Step 5 Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

Step 6 Click **Push Data to Clusters**.

Step 7 On the View Push Role Data Report page, view the push details, then click **OK** to return to the List/Add Administrator Roles page.

CLI Command

When connected to a regional cluster, you can use the **role** < *name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-omitrelated**] [**-report-only** | **-report**] command. A list of clusters or "all" may be specified. This operation will also push the related groups (using replace mode) and related owners and regions (using ensure mode). To prevent this and to just push the role, specify **-omitrelated**.

Pulling Roles from the Replica Database

Pulling administrator roles from the local clusters is mainly useful only in creating an initial list of roles that can then be pushed to other local clusters. The local roles are not useful at the regional cluster itself.

When you pull a role, you are actually pulling it from the regional cluster replica database. Creating the local cluster initially replicates the data, and periodic polling automatically updates the replication. However, to ensure that the replica data is absolutely current with the local cluster, you can force an update before pulling the data.

Regional Advanced Web UI

Step 1 From the **Administration** menu, choose **Roles** under the **User Access** submenu.

Step 2 On the List/Add Administrator Roles page, click the **Pull Data** icon in the Roles pane. This opens the Select Replica Administrator Role Data to Pull dialog box.

Step 3 Click the **Replica** icon in the **Update Replica Data** column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data.)

Step 4 Choose a replication mode using one of the Mode radio buttons. In most cases, you would leave the default Replace mode enabled, unless you want to preserve any existing role properties at the local cluster by choosing Ensure, or create an exact copy of the role data at the local cluster by choosing Exact (not recommended).

Step 5 If you have the owner-region subrole permission, you can decide if you want to pull all the associated owners with the role, which is always in Ensure mode. This choice is enabled by default.

Step 6 Click **Pull Core Roles** next to the cluster, or expand the cluster name and click **Pull Role** to pull an individual role in the cluster.

Step 7 On the Report Pull Replica Roles page, view the pull details, then click **Run**.

Step 8 On the Run Pull Replica Roles page, view the change set data, then click **OK**. You return to the List/Add Administrator Roles page with the pulled roles added to the list.

CLI Command

When connected to a regional cluster, you can use the **role** < *name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] command. This operation will pull the related owners and regions (using ensure mode). To prevent this and to just pull the role, specify **-omitrelated**.

Pushing and Pulling Tenants

You can push all tenants to local cluster or pull the tenants data from the local cluster on the List/Add Tenants Page in the regional web UI.

Pushing Tenants to Local Clusters

To push tenants to the local cluster, do the following:

Regional Web UI

To add scopes, do the following:

Step 1 From the **Administration** menu, choose **Tenants** under the **User Access** submenu to view the List/Add Tenants page in the regional web UI.

Step 2 Click the **Push All** icon in the Tenants pane to push all the tenants listed on the page, or **Push** to push an individual tenant. This opens the Push Tenant Data to Local Clusters page.

Step 3 Choose a push mode using one of the Data Synchronization Mode radio buttons.

- If you are pushing all the tenant, you can choose Ensure, Replace, or Exact.
- If you are pushing a single tenant, you can choose Ensure or Replace.

  In both cases, Ensure is the default mode.

  Choose Replace only if you want to replace the tenant data at the local cluster. Choose Exact only if you want to create an exact copy of the tenant data at the local cluster, thereby deleting all tenants that are not defined at the regional cluster.

Step 4 Click **Push Data to Clusters**.

CLI Command

When connected to a regional cluster, you can use the **tenant** < *tag* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**] command. A list of clusters or "all" may be specified.

Pulling Tenants from the Replica Database

To pull tenants from the replica database, do the following:

Regional Web UI

Step 1 From the **Administration** menu, choose **Tenants** under the **User Access** submenu to view the List/Add Tenants page.

Step 2 On the List/Add Tenants page, click the **Pull Data** icon in the Tenants pane. This opens the Select Replica Tenant Data to Pull dialog box.

Step 3 Click the **Replica** icon in the **Update Replica Data** column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data.)

Step 4 Choose a replication mode using one of the Mode radio buttons.

Leave the default Replace mode enabled, unless you want to preserve any existing tenant data at the local cluster by choosing Ensure.

Note We do not recommend that you create an exact copy of the tenant data at the local cluster by choosing Exact.

Step 5 Click **Pull Replica**.

Step 6 On the Select Replica Tenant Data to Pull page, click **Pull all Tenants** to view the pull details, and then click **Run**.

On the Run Pull Replica Tenants page, view the change set data, then click **OK**. You return to the List/Add Tenants page with the pulled tenants added to the list.

CLI Command

When connected to a regional cluster, you can use the **tenant** < tag | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**] command.

Session Management

Cisco Prime Network Registrar provides administrator functions to monitor user sessions, manage system configuration for session management, and report login information for each user. Session events are added to provide login and logout details for each user.

User Sessions

You can find when and where your account has been used by clicking the gear icon (⚙) at the top right corner of the application page. The first login displays only the user name and host. The second login displays the last successful login with date and time. After failed login attempts, the next successful login displays the number of failed login attempts.

Superuser administrators can limit the number of concurrent sessions for one user, to discourage account sharing or excessive use. They can also limit the number of failed login attempts to protect against automated login attacks. When the retry limit is reached, the user account is suspended.

To set the session control attributes:

Local and Regional Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Server page.

Step 2 Click **CCM** in the Manage Servers pane on the left. The Edit Local CCM Server page appears. This page displays all the CCM server attributes.

Step 3 Enter the required value in the following fields:

- **admin-failed-login-limit**—Specifies the maximum number of failed user or token login attempts that are allowed before an administrator account is suspended. If set to 0, no limit is applied. A value of 1 or 2 is not recommended.
- **admin-user-session-limit**—Specifies the maximum number of concurrent user sessions for a single administrator. If set to 0, no limit is applied.
- **admin-token-session-limit**—Specifies the maximum number of concurrent token sessions for a single administrator. Single sign-on connections are the most common token sessions. The web UI may also open token sessions for resource monitoring and dashboard displays. If set to 0, no limit is applied. A value of 1 or 2 may result in unexpected web UI failures and is not recommended.
- **admin-suspended-timeout**—Specifies the length of time an administrator account should remain suspended if it has not been administratively reinstated. If set to 0, administrative action is required to reinstate the account. An additional delay of up to 30 minutes can occur when the account is automatically reinstated.

Step 4 Click **Save** to save the settings.

Step 5 Restart the server to see the changes.

CLI Commands

To suspend user accounts, use **admin** *name* **suspend**.

To reinstate user accounts, use **admin** *name* **reinstate**.

Active User Sessions

The list of active user sessions is shown in the CCM User Connections page. This report page is available only for superusers.

To view the CCM User Connections report:

Local and Regional Web UI

From the **Operate** menu, choose **CCM User Connections** under the **Reports** submenu to open the CCM User Connections page. All the active user sessions will be listed with admin name, type of authentication associated with the connection (admin auth type), connection start time, total requests, and client source details.

The **Client Source** column shows additional information about the connection when available and can be:

- The source address and port of the incoming HTTP/HTTPS connections (for web UI and REST sessions).
- The source address, port, and user information for the incoming CLI, tools, or SDK sessions. The addresses and ports for the initiating user's SSH connection may also be provided, if available (this is based on the user's SSH_CONNECTION environment variable).
- Other useful indications, such as:
  - "Regional-to-local management" or "Local-to-regional management" for CCM connections between the local and regional clusters.
  - "Local-to-local management" for failover or HA sync, or other CCM-to-CCM connections between the local clusters.
  - Other identifiers, enclosed in < and >, for server related connections that identify the server (and sometimes additional details).

Note As this information is supplied to CCM by the client, it may be subject to spoofing and should be treated as informational, but not authoritative.

Note CCM User Connection supports two types of authentication (Admin Auth Type): 1) user and 2) token.

- Cisco Prime Network Registrar runs couple of application level threads to operate dashboard and resource monitor. These are displayed as token type connections. So, even though you log out, these connections will still exist and the number of requests for the token type connection will get incremented as these keep running in the background. If you want to clear all the connections (mainly the token type), then you must restart Cisco Prime Network Registrar.
- If you close the browser without logging out of Cisco Prime Network Registrar, the user type connection remains for 2 hrs (default session timeout).

CLI Command

To view the active user sessions, use **ccm listConnections**.

Logs for Session Events

Superuser administrators can monitor session activity by viewing the log entries for session events, or by viewing the session events by clicking the Alarms icon at the top of the web UI.

To view the logs for session events:

Local and Regional Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Server page.

Step 2 Click **CCM** in the Manage Servers pane on the left. The Edit Local CCM Server page appears.

Step 3 Click the **Monitor Logs** tab to view the logs for session events.

CCM will log the additional client supplied source information (see Active User Sessions, on page 34 for more details) when a user authenticates to CCM. Also, it will log the information when the connection is closed, if the information is supplied. This information will also appear in the change log entries related to the user login (User Preference) information.

Note This information is only supplied starting with Cisco Prime Network Registrar 10.1 CLI and SDKs (Cisco Prime Network Registrar 10.0 and earlier clients will not report this additional information and hence CCM will not log it).

Note Starting with Cisco Prime Network Registrar 11.1, for admins logged in through web UI and REST API, the actual client details (IP and port) are logged for each SCP operations.