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, and Roles, on page 1
- External Authentication Servers, on page 6
- Managing Administrators, on page 10
- Managing Passwords, on page 11
- Managing Groups, on page 11
- Managing Roles, on page 12
- Granular Administration, on page 13
- Centrally Managing Administrators, on page 17

Administrators, Groups, and Roles

The types of functions that network administrators can perform in Cisco Prime IP Express 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 IP Express 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.

Related Topics

How Administrators Relate to Groups and Roles, on page 2

Administrator Types, on page 2

Roles, Subroles, and Constraints, on page 2

Groups, on page 6

Managing Administrators, on page 10

Managing Passwords, on page 11

Managing Groups, on page 11

Managing Roles, on page 12

How Administrators Relate to Groups and Roles

There are three administrator objects in Cisco Prime IP Express—administrator, group, and role:

- **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 10.

- **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 IP Express provides map each role to a unique group.

  Adding groups is described in Managing Groups, on page 11.

- **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 12.

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 into the web UI.

- **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.

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 12.

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. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases, and reservations.
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.

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. • *snmp-management*: Manage the SNMP server configuration.
dhcp-admin	Core functionality: Manage DHCP scopes and templates, policies, clients, client-classes, options, leases, and reservations. • *server-management*: Manage the DHCP server configuration, failover pairs, LDAP servers, extensions, and statistics. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases, and reservations.
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.
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. • *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. • *byod-management*: Manage BYOD 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 prefixes, links, options, leases and reservations.
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 utilization data. • *ipv6-management*: Manage IPv6 prefixes, links, options, leases and reservations. • *byod-management*: Manage BYOD Server configuration.

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 IP Express, 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 IP Express 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 RADIUS servers are inaccessible or misconfigured, use the local.superusers file to create a temporary username and password. See Managing Administrators, on page 10 for more details.

Configuring an RADIUS External Authentication Server

Cisco Prime IP Express administrators must be assigned to one or more administrator groups to perform management functions. When using a RADIUS 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 IP Express 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

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

Adding an RADIUS External Configuration Server

To add an external configuration server, do the following:

Local Advanced and Regional 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 **enabled** check box of the ext-auth attribute in the Edit Authentication Server page, and then click **Save**.

Step 4 Change the auth-type attribute to RADIUS in the Manage Server page, click **Save**, and then restart Cisco Prime IP Express.

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 an RADIUS External Authentication Server

Local Advanced and Regional Web UI

To delete an 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 IP Express 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 IP Express 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 CPIPE and add the users 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 **CPIPE**, 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 **CPIPE** and click **OK**.

Step 4 In AD Server Object windows, select **CPIPE** 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 IP Express. You must use the AD server to perform this configuration.

Configuring Kerbero's Realm and KDC

For the Cisco Prime IP Express to communicate with the AD server, the Kerbero's Realm and KDC servers are required. To configure the Kerbero's Realm and KDC servers in Windows and Linux platforms follow the below examples.

If the Cisco Prime IP Express is running on Windows platform (ksetup), define a KDC entry for a realm by running the following command:

```
ksetup /AddKdc <RealmName> [KdcName]
```

For example, `Ksetup /AddKdc ECNR.COM tm-chn-ecnr-ad.ecnr.com`

To verify, run the following command:

```
ksetup /dumpstate
```

The result should be similar to the message below:

```
default realm = partnet.cisco.com (NT Domain)
ECNR.COM:
 kdc = tm-chn-ecnr-ad.ecnr.com
 Realm Flags = 0x0No Realm Flags
No user mappings defined.
```

If the Prime IP Express is running on Linux platform, 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 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, domain you want to configure as the external authentication server, and you can set the base domain, LDAP user attribute map, AD group name which will be used for communicating with this server in the Add Active Directory Server dialog box, and click **Add Active Directory Server**.

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

CLI Commands

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

Deleting an AD External Authentication Server

Local Advanced and Regional Web UI

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 Administrators

When you first log in, Cisco Prime IP Express 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.

Tip If you accidentally delete all the roles by which you can log into Cisco Prime IP Express (those having superuser, ccm-admin, or regional-admin privileges), you can recover by creating a username/password pair in the *install-path* /conf/priv/local.superusers file. You must create this file, have write access to it, and include a line in it with the format *username password*. Use this username and password for the next login session. Note, however, that 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.

Adding Administrators

To add a 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.

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.

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 into 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. Click **Cancel** in the confirmation window to cancel the deletion.

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 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 and enter a name 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).

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 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, 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 14

Prefix-Level Constraints, on page 15

Link-Level Constraints, on page 16

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 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 IP Express 9.0 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 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 Prefixes page.

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 Advanced 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

Related Topics

Pushing and Pulling Administrators, on page 18

Pushing and Pulling Groups, on page 22

Pushing and Pulling Roles, on page 23

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.

Related Topics

Pushing Administrators to Local Clusters, on page 18

Pushing Administrators Automatically to Local Clusters , on page 18

Pulling Administrators from the Replica Database, on page 19

Pushing Administrators to Local Clusters

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

Regional Basic and Advanced 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.

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 Basic and Advanced Web UI

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

Step 2 Click the **Local CCM Server** link on the Manage Servers pane to open the Edit 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 Basic and Advanced 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
```

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**.

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.

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.

Related Topics

Pushing Groups to Local Clusters, on page 22

Pulling Groups from the Replica Database, on page 23

Pushing Groups to Local Clusters

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

Regional Basic and Advanced 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.

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 Basic and Advanced 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.

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 17).

Related Topics

Pushing Roles to Local Clusters, on page 24

Pulling Roles from the Replica Database, 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.

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.