



Network Registrar User Interfaces

Cisco CNS Network Registrar provides two Web-based user interfaces (Web UIs) and a command line interface (CLI) to manage the DNS, DHCP, TFTP, and Central Configuration Management (CCM) servers:

- Web UI for the regional cluster to access local cluster servers
- Web UI for the local clusters
- CLI for the local clusters
- CCM servers that provide the infrastructure to support these interfaces

This chapter describes the Network Registrar user interfaces and the services that the CCM servers provide. Read this chapter before starting to configure the Network Registrar servers so that you become familiar with each user interface's capabilities.

Introduction to the Web-based User Interfaces

The Web UI provides granular access to configuration data through user roles and constraints. The Web UI granularity is described in the following section.

Supported Web Browsers

The minimum Web browsers supported in Network Registrar are Internet Explorer 5.5 and Netscape 6.2.

Access Security

At installation, you can choose to configure HTTPS to support secure client access to the Web UIs. To enable secure communication, you must have the Cisco CNS Network Registrar Communications Security Option Release 1.1 installed.

Logging In to the Web UIs

You can log in to the Network Registrar local or regional cluster Web UIs either by HTTPS secure or HTTP nonsecure login. After installing Network Registrar, open one of the supported Web browsers and specify the login location URL in the browser's address or netsite field. Login is convenient and provides some memory features to increase login speed.

You can log in using a nonsecure login in two ways:

- On Windows, from the Start menu, **Start > Programs > Network Registrar 6.1 > Network Registrar 6.1 {local | regional} Web UI**, which opens the local or regional cluster Web UI from your default Web browser.
- Open the Web browser and go to the website. For example, if default ports were used during the installation, the URLs would be **http://hostname:8080** for the local cluster Web UI, and **http://hostname:8090** for the regional cluster Web UI.

This opens the Login page. With a conventional login, the page indicates “Page is not secure” (see [Figure 3-1](#)); with an SSL-secured login, the page indicates “Page is SSL Secure.”



Note

To prepare for an HTTPS-secured login, see the *Network Registrar Installation Guide*.

Figure 3-1 Login Page

Enter your account name and password. The password is case sensitive. Depending on how your browser was set up, you might be able to abbreviate the account name and select it from the drop-down list. If the password is stored from a previous login, it might be entered automatically.

To log in, click **Login**. If this is the first login after installing Network Registrar, an Add Product License page appears first (see [Figure 3-2](#) for the local cluster page; the regional cluster page is essentially the same). Your license key is printed on the installation CD. Enter it, then click **Add License**. If the license key is valid, you immediately enter the Web UI application pages.

Figure 3-2 Add Product License Page

To re-enter a previously active session, click **Reuse current session**. (This option is only available if you did not remove the cookie for it in the Web browser.)

**Note**



If you log in again to a previously active session without clicking **Reuse current session**, you may have two active sessions open, which can cause erratic failures. For example, if your active session was the first one after an installation, when you had to enter the license key, you are prompted again for the license key indefinitely. To avoid this, either click **Reuse current session**, or close and re-open the browser to initiate a new session.

Navigating

The Web UI provides a hierarchy of pages based on the functionality you desire and the thread you are following as part of your administration tasks. The page hierarchy is never so deep that you can get lost in it.

**Caution**

Do not use the Back button of the browser. Always use the Primary or Secondary Navigation bar, or the **Cancel** button on the page to return to a previous page. Using the Back button can cause erratic failures.

An additional single sign-on feature is now available to connect between the regional and local cluster Web UIs. Many of the regional cluster Web UI pages include the Go Local icon () , which you can click to connect to the local cluster associated with the icon. If you have single sign-on privileges to the local cluster, the connection takes you to the related local server management page (or a related page for failover pair configurations). If you do not have these privileges, the connection takes you to the login page for the local cluster. To return to the regional cluster, local cluster pages have the Go Regional icon () at the top right corner of the page.


Waiting for Page Resolution Before Proceeding

Operations performed in the Web UI, such as resynchronizing or replicating data from server clusters, are synchronous operations that do not return control to the browser until the operation in Network Registrar is completed. These operations display confirmation messages in blue text when they are completed. Also, both the Netscape and IE browsers display a wait cursor while the operation is in progress. Unfortunately, the browsers do not prevent you from moving the mouse over another control icon and clicking it, in which case the browser session can be irrevocably impaired.

To prevent this, wait for each operation in the Web UI to finish before you begin a new operation. If the browser becomes impaired, close the browser, re-open it, then login back in again.

Committing Changes

**Tip**

You do not actually commit the page entries you make until you click **Add...** or **Modify...** on the page. You can delete items using the Delete icon () . To prevent unwanted deletions, a Confirm Delete page appears in many cases so that you have a chance to confirm or cancel the deletion.

Role and Attribute Visibility Settings

The Main Menu page shows the administrative roles assigned to the logged-in administrator. It also presents a selection of which visibility you want the configuration attributes to be in the Web UI:

- To view the roles for the administrator, expand the area of the page by clicking the plus sign (+) next to the “Show Roles for User” heading. The roles appear in S-expression format. For example, a host administrator might show this role:

```
name=boston-hostadmin-role, role=host-admin, unconstrained=false, read-only=false,
zones={boston.example.com.}, use-any-range=false, use-any-zone=false,
use-any-owner=false, edit-owners=false, access-secondary-zones=false,
access-reverse-zones=false
```

This means that this particular host administrator is constrained to the boston.example.com zone, has read-write privileges to that zone, cannot administer just any address ranges in it, cannot use just any owner or edit owners, and cannot access secondary zones or reverse zones. (For details on how to set up these administrator roles, see the [“Administrators, Roles, and Groups”](#) section on page 4-1)



Note Superuser privileges override any roles displayed for a superuser administrator.

- To set the attribute visibility settings for this user session only, expand the area of the page by clicking the plus sign (+) next to the “Session Attribute Visibility Setting” heading. You can then select Normal or Expert from the drop-down list:
 - Normal attribute visibility is appropriate under most conditions and is the default setting.
 - Expert attribute visibility exposes a set of attributes that are relevant for fine-tuning or troubleshooting the configuration. In most cases, you would accept the default values for these reserved attributes and not change them without guidance from the Cisco Technical Assistance Center (TAC). These reserved attributes are each marked with a warning icon (⚠) on the configuration pages.

Displaying and Modifying Attributes

Many of the Web UI pages, such as those for servers, zones, and scopes, include attribute settings that correspond to those you can set using the CLI. (When the Web UI attribute name differs from the CLI name equivalent, the CLI name appears as a secondary attribute name.) The attributes are categorized into groups by their function, with the more prominent attributes listed first and the ones less often used for configuration at the bottom of the page.

Modifying Attributes

You can modify these configuration attribute values and unset those for optional attributes. In many cases, these attributes have default values, which are listed under the Default column on the page. The explicit value overrides the default one, but the default one is always the fallback. If there is no default value, unsetting the explicit value removes all values for that attribute.

Displaying Attribute Help

For contextual help for an attribute, click the name of the attribute to open a help window. This help window is a separate browser window and you must close it when finished reading the description.

Attribute Visibility

You can select one of two visibility settings of these configuration attributes. Normal mode is for normal conditions and is the default. Expert mode is reserved for troubleshooting conditions under the guidance of the Cisco TAC. In most cases, you do not need to change the default Normal setting. If required, you can change the setting on the Main Menu page (see the [“Role and Attribute Visibility Settings”](#) section on page 3-4).

Help Pages

The Web UI provides a separate window that displays help text for each page. The Help page identifies the topic and the application page name. In many cases, you can access a summary page for the topic by clicking a **Top of Section** link at the bottom of the help page. You can navigate through the help pages, which provide many links to related topics. To exit the help window, click the **Close Window** link at the bottom.

You can also open a separate context-sensitive help window for many configuration attributes by clicking the attribute name. See the [“Displaying Attribute Help”](#) section on page 3-4.

Logging Out

You can log out of the Web UI by clicking the **Logout** link at the top right corner of any application page.

Local Cluster Web UI

The local cluster Web UI provides concurrent access to Network Registrar user and protocol server administration and configuration. It provides granular administration across servers with permissions you can set on a per element or feature basis. Once you log in to the application, the Main Menu page (see [Figure 3-3](#)).

Figure 3-3 Local Cluster Main Menu Page

Home | Administration | Zone | Host | Address Space | DHCP

Main Menu

[Administration](#)
Use these pages to manage licenses, administrators, administrator groups and roles, encryption keys and access control lists, manage protocol servers, and to view the datastore change logs.

[Zone](#)
Use these pages to manage the lists of zones, reverse zones and secondary zones, and their resource records. Also manage zone owners and templates, secondary servers, and the zone distribution.

[Host](#)
Use these pages to manage hosts, assigning them a DNS name and one or more IP addresses.

[Address Space](#)
Use these pages to view the unified address space tree, and to manage address blocks, subnets and static IP ranges, as well as owners and regions.

[DHCP](#)
Use these pages to manage the Cisco Network Registrar DHCP server. This includes management of scopes and associated ranges, reservations and leases, policies and associated options, and client and client-class entries.

- + Show Roles for User *admin*
- + Session Attribute Visibility Setting
- + WebUI Debug Settings
- + Server Debug Settings

84322

The full list of elements possible on the Main Menu page are:

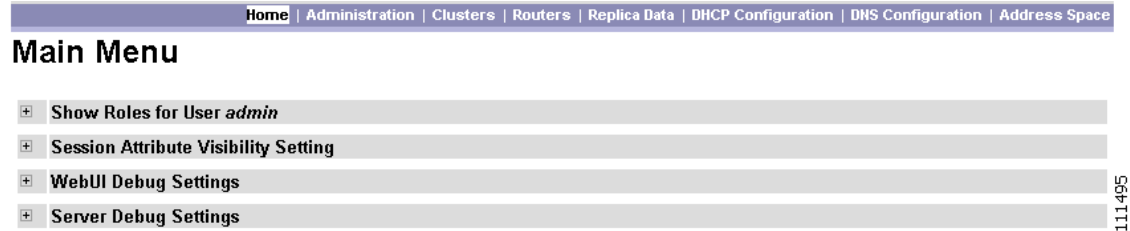
- Administration—Use these pages to manage administrators, groups and roles, encryption keys, access control lists, and protocol servers, and view the datastore change logs.
- Zone—Use these pages to manage the lists of forward, reverse, secondary zones, and their resource records; and manage zone owners and templates, secondary servers, and zone distributions.
- Host—Use these pages to manage hosts and their addresses.
- Address Space—Use these pages to view the unified address space tree, and manage address blocks, subnets and static IP ranges, owners, and regions.
- DHCP—Use these pages to manage the Network Registrar DHCP server. This includes managing scopes and associated ranges, reservations and leases, policies and associated options, and client and client-class entries.

Local cluster administration begins with [Chapter 6, “Maintaining Servers.”](#)

Regional Cluster Web UI

The regional cluster Web UI provides concurrent access to Network Registrar regional and central administration tasks. Like the local cluster Web UI, it provides granular administration across servers with permissions you can set on a per element or feature basis. Once you log in to the application, the Main Menu page (see [Figure 3-4](#)).

Figure 3-4 Regional Cluster Main Menu Page



The full list of elements possible on the regional cluster Main Menu page are:

- Administration—Use these pages to manage product licenses, administrators, groups and roles, owners, regions, and servers, and view the datastore change logs.
- Clusters—Use these pages to manage the local clusters.
- Routers—Use these pages to manage router interface configuration (RIC) servers.
- Replica Data—Use this page to view the replica data of the local clusters on the regional cluster.
- DHCP Configuration—Use these pages to manage virtual private networks (VPNs), DHCP scope templates, policies, client-classes, and failover server pairs.
- DNS Configuration—Use these pages to manage DNS zone distributions, forward zones, and reverse zones.
- Address Space—Use these pages to manage the address space, address blocks, subnets, address types, address destinations; and to check subnet utilization, lease history, and consistency rules.

Regional cluster administration is described in [Chapter 5, “Managing the Central Configuration.”](#)

Command Line Interface

Using the Network Registrar CLI (the **nrcmd** program), you can control your local cluster servers’ operations. You can set all configurable options, as well as start and stop the servers. The CLI provides for concurrent access, but you should not have more than one CLI session open, because these interfaces require a lock on the databases. See the *Network Registrar CLI Reference* for details.

The **nrcmd** program for the CLI is located on:

- Windows—In the *install-path\bin* directory.
- Solaris and Linux—In the *install-path/usrbin* directory.

On a local cluster, once you are in the appropriate directory, use the following command at the command prompt:

```
nrcmd -C localhost -N admin -P changeme
```

- **-C** is the cluster name
- **-N** is the username
- **-P** is the user password (it is advisable to change this default password right away)

(For additional command options, see the *Network Registrar CLI Reference*.)

To disconnect from the cluster, use the **exit** command:

```
nrcmd> exit
```

**Tip**

The CLI operates on a coordinated basis with multiple user logins. If you receive a cluster lock message, determine who has the lock and discuss the issue with them. You can override the lock using the **force-lock** command, but not unless you are absolutely sure you would thereby not adversely affect someone else's work.

Central Configuration Management Server

The Central Configuration Management (CCM) servers on the local and regional clusters provide the infrastructure for Network Registrar operation and user interfaces. The Web UIs operate with a combination of the legacy Network Registrar databases (MCD) and the additional CCM databases. The main purpose of the local cluster Web UI infrastructure is to store and propagate data from the user to the protocol servers, and from the servers back to the user.

The change set is the fundamental unit of change to a data store. It is used to send incremental changes to a replicating server, and it provides an audit log for changes to the data store. Change sets consist of lists of change entries that are groups of one or more changes to a single network object. The Web UI provides a view of the change sets for each data store.