CHAPTER 5

Using the Network Services Manager Administration UI

This chapter describes the Network Services Manager Administration UI and includes the following sections:

Getting Started with the Administration UI

To log into the Network Services Manager Administration UI:

Step 1 In your browser, enable popup windows for the Network Services Manager engine. If you do not enable popup windows, you cannot view confirmation dialog boxes or other messages that Network Services Manager displays.

Step 2 Enter the following URL:

`https://hostname:8443/`

where ***`hostname`*** is the name of the Network Services Manager engine.

Step 3 When prompted, accept the security certificate.

Step 4 In the login screen, enter the username and password. The default value is **`admin`** for both the username and password.

Note For security purposes, we recommend that you change the password. To change the login password, see Changing User Passwords, page 5-7.

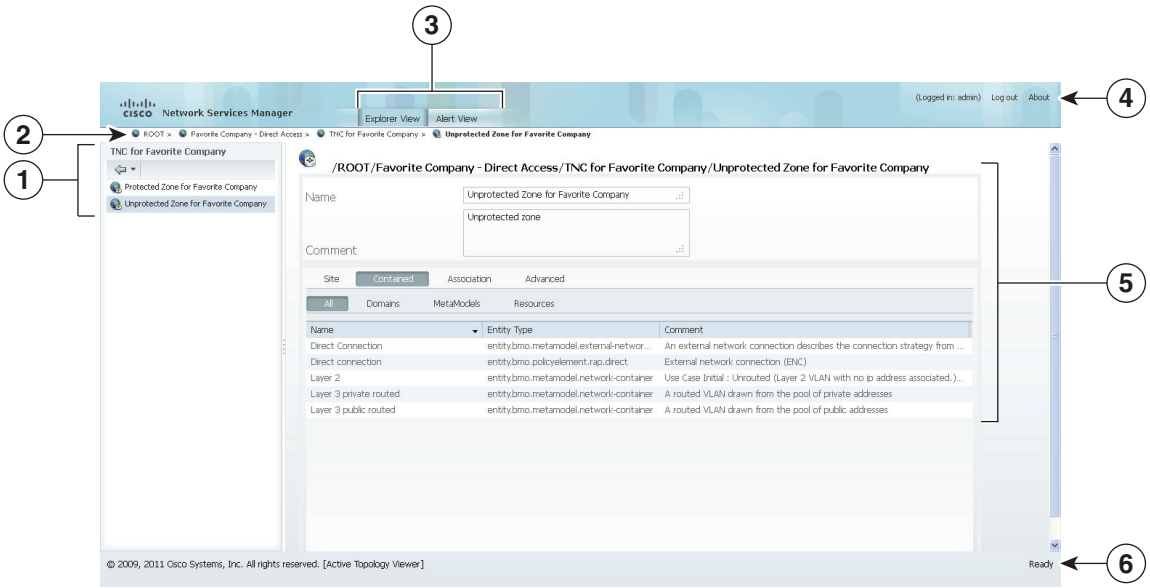
The main Administration screen is displayed with the ROOT domain selected.

Administration UI Features

When you log into Network Services Manager, the Administration UI is displayed as shown in Figure 5-1. The UI includes the following components:

- Explorer and Alert Views, page 5-2
- Domain Navigator, page 5-3
- Breadcrumb Trail, page 5-3
- Content Pane, page 5-3
- Status Bar, page 5-6
- Product Information, page 5-6

Figure 5-1 Administration UI



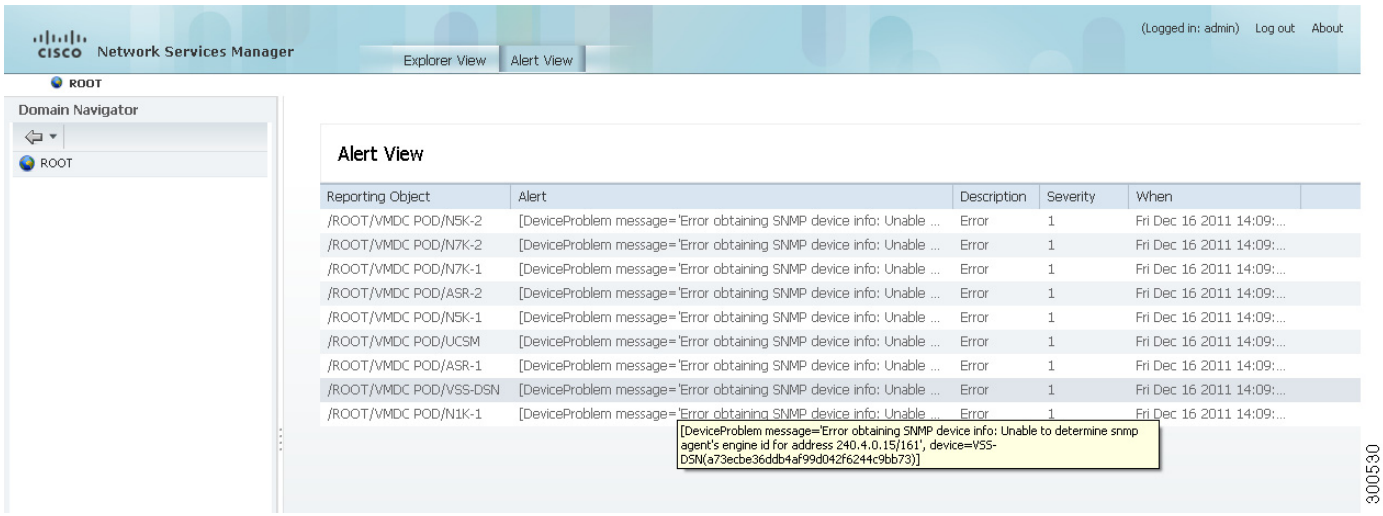
1	Domain Navigator	**4**	Product information
2	Breadcrumb trail	**5**	Content pane
3	Explorer View and Alert View tabs	**6**	Status bar

Explorer and Alert Views

The Administration UI includes the following views, each accessible via a tab at the top of the window:

- Explorer View—The Explorer View enables you to view objects, their properties, and their running configurations.
- Alert View—The Alert View (shown in Figure 5-2) displays a sortable list of system events, specific to the item selected in the Domain Navigator. You can resize the columns or hover your cursor over an entry in the table to see the complete text.

Figure 5-2 Alert View



Domain Navigator

The Domain Navigator displays the domain hierarchy in a dynamic view that allows you to view tenants and the associated objects.

When you log into Network Services Manager, the ROOT domain is selected by default. As you navigate the hierarchy, the breadcrumb trail is updated with the path, and the content pane is updated with the properties of the currently selected item.

The return arrow button at the top of the Domain Navigator pane enables you to return to a higher level in the domain hierarchy.

Tip Use the drop-down list next to the return arrow to select the level you want to return to.

Breadcrumb Trail

The breadcrumb trail identifies your recent navigation path and enables you to easily return to previously viewed screens. It also provides the currently displayed item's path, relative to the ROOT domain. If you select a new item in the Domain Navigator, the breadcrumb trail reflects the new path from ROOT to the selected item.

Content Pane

The content pane contains detailed information about the selected object. The top portion contains:

- The path from ROOT to the selected item.
- Name and Comment fields.

The lower portion of the content pane contains tabs with object-specific properties. The tabs that are displayed depend on the selected object and can contain subordinate tabs. Table 5-1 describes the tabs available for common objects.

Table 5-1 Content Pane Tabs

Tab	Description
ROOT, Tenant, and Tenant Network Container	
Contained	Contains the All, Subdomains, Sites, and Resources tabs. The All tab lists all contained entities, including the entity name, entity type, and a comment. The other tabs list the entities that fall into the identified category.
Metaproperties	Displayed for tenants and tenant network containers. Lists metaproperties associated with the selected object.
Advanced	Contains the Settings, Client Properties, and State tabs. The Advanced tab contains advanced settings for the selected object.
Pod	
Controller	Contains the username and password for the Network Services Manager controller for the selected device stack.
Assignments	Lists the local resources, VLANs, and zones that can be assigned to the device stack and those that are assigned.
Contained	Contains the All, Network Elements, and Interconnects tab. Identifies the network elements and interconnects associated with the selected object, including their entity type and any comments.
Advanced	Contains the Settings, Client Properties, and State tabs. The Advanced tab contains advanced settings for the selected object.
ENC	
General	Displays the ENC name and comment.
Settings	Identifies the start and end dates for the service, and any owned objects.
State Variables	Identifies any parameters defined for the ENC.
Metaproperties	Lists all metaproperties associated with the ENC.
Advanced	Contains the Settings, Client Properties, and State tabs. The Advanced tab contains advanced settings for the selected object.
Zone Network Container	
Site	Identifies the device stack assigned to the site.
Contained	Contains the All, Domains, Metamodels, and Resources tabs. The All tab lists all contained entities, including the entity name, the entity type, and a comment. Entity types can include created VLANs, network containers, and ENCs. The other tabs list the entities that fall into the identified category.

Table 5-1 Content Pane Tabs (continued)

Tab	Description
Association	Contains the Policy Elements and Groups tabs. The Policy Elements tab lists the available policy elements and those that are associated with the selected zone. The Groups tab lists the available groups and those that are associated with the selected zone.
Advanced	Contains the Settings, Client Properties, and State tabs. The Advanced tab contains advanced settings for the selected object.
VLAN	
General	Identifies whether or not an ACL enforcement policy is in effect, whether or not the VLAN is managed, the scope of the VLAN (for example, Layer 2 or Layer 3), and the device stack assigned to the site.
Subnet	Identifies the VLAN subnet and mask, the DHCP IP address if one is configured, the gateway IP address, and the type of IP address pool, such as private or public.
Association	Contains the Policy Elements and Groups tabs. The Policy Elements tab lists the available policy elements and those that are associated with the selected VLAN. The Groups tab lists the available groups and those that are associated with the selected VLAN.
Metaproperties	Lists metaproperties associated with the selected VLAN.
Advanced	Contains the Settings, Client Properties, and State tabs. The Advanced tab contains advanced settings for the selected object.
Group and Local Resource	
General	Displayed for local resources. Identifies the VLAN subnet with the subnet mask and the object that the local resource is associated with.
Members	Displayed for groups. Lists objects that are available to the group and those that participate in the group.
Association	Contains the Policy Elements and Groups tabs. The Policy Elements tab lists the available policy elements and those that are associated with the selected group or local resource. The Groups tab lists the available groups and those that are associated with the selected group or local resource.
Advanced	Contains the Settings, Client Properties, and State tabs. The Advanced tab contains advanced settings for the selected object.

Status Bar

The status bar indicates whether Network Services Manager is loading information or ready for your next selection.

Product Information

Product information is available at the top right of the window and includes:

Field	Description
Username	Account name of the person logged in.
Logout button	Logs you out of Network Services Manager after you confirm the logout request.
About button	Displays Network Services Manager version information.

Verifying Device Configurations

After you add a tenant network container and network containers, you can verify that the configuration on a device matches the information you entered by using the Run Commands feature.

To verify the device configuration in Network Services Manager:

Step 1 Navigate to the required device by choosing **ROOT > Contained > All**.

Step 2 Click **VMDC POD**.

Step 3 Choose **Contained > Network Elements**.

Step 4 Click the required device in the list of network elements.

Step 5 In the properties screen, click **Run Commands**.

Step 6 In the Run Command dialog box, choose the required Show option from the drop-down list and click **Run**.

The configuration is displayed in the dialog box (see Figure 5-3), allowing you to compare the information entered using Network Services Manager with the existing device configuration.

UI Example

Figure 5-3 shows an example device configuration in the Run Commands dialog box.

Figure 5-3 Device Configuration in Run Commands Dialog Box

Changing User Passwords

We recommend that you change user passwords for security purposes.

The following conventions apply when changing user passwords:

- The password must contain at least eight characters.
- The password must contain characters from three of the following groups:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Special characters

If your organization requires different password policy settings, review and edit the passwordpolicy.properties file on the engine in the following directory:

/usr/local/overdrive/engine/bin/UtilUpdateUserPassword

To change the password for the Network Services Manager Administration UI or apiclient account:

Step 1 Log into the Network Services Manager engine from the vSphere console window.

Step 2 To enter the root shell, enter **shell**.

Step 3 Navigate to the correct directory by entering:

```
cd /usr/local/overdrive/engine/bin/UtilUpdateUserPassword
```

Step 4 To change a password, do either or both of the following:

- Administration UI password—Enter the following command:

  `java -jar UtilUpdateUserPassword.jar` *`old-password new-password`*

- Apiclient account password—Enter the following command:

  `java -Dusername=apiclient -jar UtilUpdateUserPassword.jar` *`old-password new-password`*

  where:

  – *`old-password`* is the current apiclient account password.

  – *`new-password`* is the new apiclient account password.

Step 5 Leave the root shell by entering **`exit`**.

Step 6 To update affected clients, do one or both of the following:

- Administration UI password—Close any browser windows that are logged into Network Services Manager using the old password, and log in again using the new password.
- Apliclient account password—Update any application using the apiclient account with the new password.