



Network Infrastructure Manager User Guide

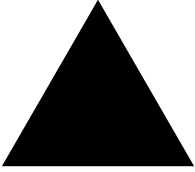
Infrastructure Client for ISM Provision

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
<http://www.extremenetworks.com>

Published: April, 2002
Part number:100120-00 rev01

©2002 Extreme Networks, Inc. All rights reserved. Extreme Networks and BlackDiamond are registered trademarks of Extreme Networks, Inc. in the United States and certain other jurisdictions. ExtremeWare, ExtremeWare Vista, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Alpine, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS, and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodriven logo is a service mark of Extreme Networks, which may be registered or pending registration in certain jurisdictions. Specifications are subject to change without notice.

All other registered trademarks and service marks are property of their respective owners.



Contents

Preface	
Introduction	ix
Terminology	x
Conventions	x
Related Publications	xii
1 Infrastructure and Services Management Provision Overview	
Overview	1-1
Summary of Features	1-2
How ISM Provision works	1-3
Your Network Devices	1-4
ISM Provision Server	1-4
Device Communicators	1-4
Network Infrastructure Manager Client	1-5
IP Service Manager Client	1-5
2 Starting Network Infrastructure Manager	
Overview	2-1
Starting Network Infrastructure Manager	2-1
3 Network Infrastructure Manager Overview	

Network Infrastructure Manager Overview	3-1
Summary of Features	3-1
NIM Views	3-2
Selecting NIM Views	3-2
Network Provision View	3-5
Network Inventory View	3-6
Providers Administration View	3-7
Server Administration View	3-8
Change Control View	3-9
NIM Icons	3-9
Open Changes	3-10
Save Changes	3-10
Modify Object	3-10
Copy	3-10
Paste	3-10
Delete	3-10
Move Device	3-11
Verify Configuration	3-11
Synchronize	3-11
Commit Changes	3-11
Revert Changes	3-11
Help	3-11

4 Network Provisioning

Overview	4-1
Network Provision View Panels	4-3
Network Panel	4-4
Templates Panel	4-5
Verification Panel	4-5
Properties Panel	4-5
Configuration Objects	4-5
Key Information	4-6
Unsupported Configuration Commands	4-6
Managed and Unmanaged Devices	4-7
View Device Configurations	4-8
View a Single Configuration Object	4-8

View Multiple Configuration Objects	4-15
Modify Visible Configuration Options	4-18
Modify View Options	4-20
Create and Modify Network Device Configurations	4-20
Add a New Device	4-21
Add a Configuration Object	4-22
Modify a Configuration Object	4-26
Copy a Device or other Object	4-29
Save Changes Without Changing Network Configuration	4-34
Remove Changes (Revert to Server State)	4-34
Change an Unmanaged Device into a Managed Device	4-35
Access Extreme Devices Directly	4-39
Use Telnet to access a device	4-39
Use Extreme WebVista to access a device	4-40

5 Managing the Network Inventory

Overview	5-1
Manage the Network Inventory List	5-2
Add a Device to the Network Inventory	5-2
Modify a Network Inventory Device Listing	5-10
Delete a Device from the Network Inventory	5-11
Import Inventory File	5-11
Export Inventory File	5-15
Manage the Network Inventory Devices	5-16
Upload Devices	5-16
Save Running Configurations	5-18

6 Managing Providers

Overview	6-1
The Infrastructure Provider	6-2
Device Access	6-2
Managing Providers	6-2
Create a Provider and Provider Accounts	6-2
Limit Provider Device Access	6-5

7 Managing the ISM Provision Server

Overview	7-1
Communicators Tab	7-2
Logs Tab	7-3
Control Tab	7-4
Manage Device Communicators	7-4
Add a Device Communicator	7-5
Modify a Device Communicator	7-5
Delete a Device Communicator	7-6
View Device Communicator Logs	7-7
Manage ISM Provision Server	7-8
View Other Connected Users	7-8
Send Broadcast Message	7-9
Stop Server	7-10
View Server Log	7-11

8 Change Control

Overview	8-1
Jobs	8-2
Configuration Versions	8-2
Change Control Tasks	8-3
View Current Job Changes	8-3
View Committed, Scheduled, or Saved Jobs	8-4
Delete Scheduled or Saved Jobs	8-7
Create Configuration Version	8-7
Rollback to a Configuration Version	8-9
	8-10

A ISM Provision Devices, Images, and Modules

Supported Devices, Images and Modules	A-1
---------------------------------------	-----

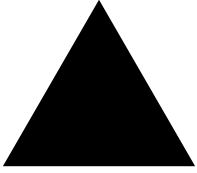
B ISM Provision Rules

Overview	B-1
----------	-----

C ISM Provision Server Maintenance

Overview	C-1
Database Backup Utility	C-1
Database Backup Utility Location	C-2
Using the Database Backup Utility	C-2
Installing a Backup Database	C-3
Adding a License Key	C-3

Index



Preface

This Preface provides an overview of this guide, describes guide conventions, and lists other publications that may be useful.

Introduction

This guide provides the required information to manage a network using Extreme Networks' Network Infrastructure Manager (NIM) client as the interface for Extreme Networks' Infrastructure and Services Management Provision (ISM Provision).

This guide is intended for use by network administrators who are responsible for configuring network equipment. It assumes a basic working knowledge of:

- Local area networks (LANs).
- Ethernet concepts.
- Ethernet switching and bridging concepts.
- Routing concepts.
- Internet Protocol (IP) concepts.
- Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
- Simple Network Management Protocol (SNMP).

Additionally, this guide assumes a familiarity with the features and functionality of ExtremeWare Software and with Extreme Networks' hardware. See the section, "Related Publications", for documents covering Extreme Networks' Software and Hardware.



If the information in the release notes shipped with your software differs from the information in this guide, follow the release notes.

Terminology

When features, functionality, or operation is specific to the Summit, Alpine, or BlackDiamond switch family, the family name is used. Explanations about features and operations that are the same across all Extreme switch product families simply refer to the product as the “Extreme device” or “Extreme switch.” Explanations about features that are the same for all devices managed by Network Infrastructure Manager (both Extreme devices and others) simply refer to “devices.”

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1: Notice Icons




Icon	Notice Type	Alerts you to...
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.

Table 2: Text Conventions

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
Screen displays bold	This typeface indicates how you would type a particular command.

Table 2: Text Conventions (continued)

Convention	Description
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Words in Bold type	GUI elements are written in bold type. Example: menu items, buttons, field names
Words in <i>italicized</i> type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used to denote variables, such as VLAN names, or user account names.

Related Publications

The publications related to this one are:

- *ISM Provision Installation Guide*
- *IP Service Manager User Guide*
- *ExtremeWare Software User Guide*

Documentation for Extreme Networks products is available on the World Wide Web at the following location:

<http://www.extremenetworks.com/>



1

Infrastructure and Services Management Provision Overview

Overview

Extreme Networks' Infrastructure and Services Management Provision (ISM Provision) is a tightly connected collection of components for delivering services to customers and for managing your network. ISM Provision allows you to easily extend services to your network users by defining and provisioning bundles of IP services. Services are managed as simple objects that are easy to apply to customers, but the configuration changes required to support the delivery of services is managed by ISM Provision. ISM Provision also allows you to control all or a portion of your network, by controlling the configurations of the devices in the network.

ISM Provision is designed to make it much easier to roll out changes to the network. You can add devices and make configuration changes offline and apply them to your network later. Planned changes are verified against a comprehensive set of rules to assure that the changes can be applied to your network and will not conflict with existing configurations. Incomplete sessions can be saved to be completed later.

Services provided across a group of customers can be easily modified. Once a service is updated, the change is applied to all customers using the service. ISM Provision manages all the configuration changes to make the modifications.

Network Infrastructure Manager (NIM) is the GUI client portion of ISM Provision that controls and manages the infrastructure of your network, the configurations of your network devices. NIM works closely with IP Service Manager (IPSM), the GUI client portion of ISM Provision that allows a provider to manage customers, service bundles, and policy based services.

Summary of Features

- Version Control of Network Configuration
- Staging of Network Configuration Changes
- Configuration rules checking
- Helps Manage the VLANs, Access Lists, and QoS Profiles Required to Support Subscribers
- Provides Service-Level Abstractions to Manage Subscribers
- Client/Server Java architecture - platform independent and scalable
- Offline and on-line tool - used in both green field and existing network environments
- Co-exists with other management tools using CLI or SNMP
- Version control for configurations and deployment module for system rollouts
- Provides an abstraction model that simplifies and automates both infrastructure and subscriber provisioning life-cycles
- Distributed device communication infrastructure for redundancy and scaling

How ISM Provision works

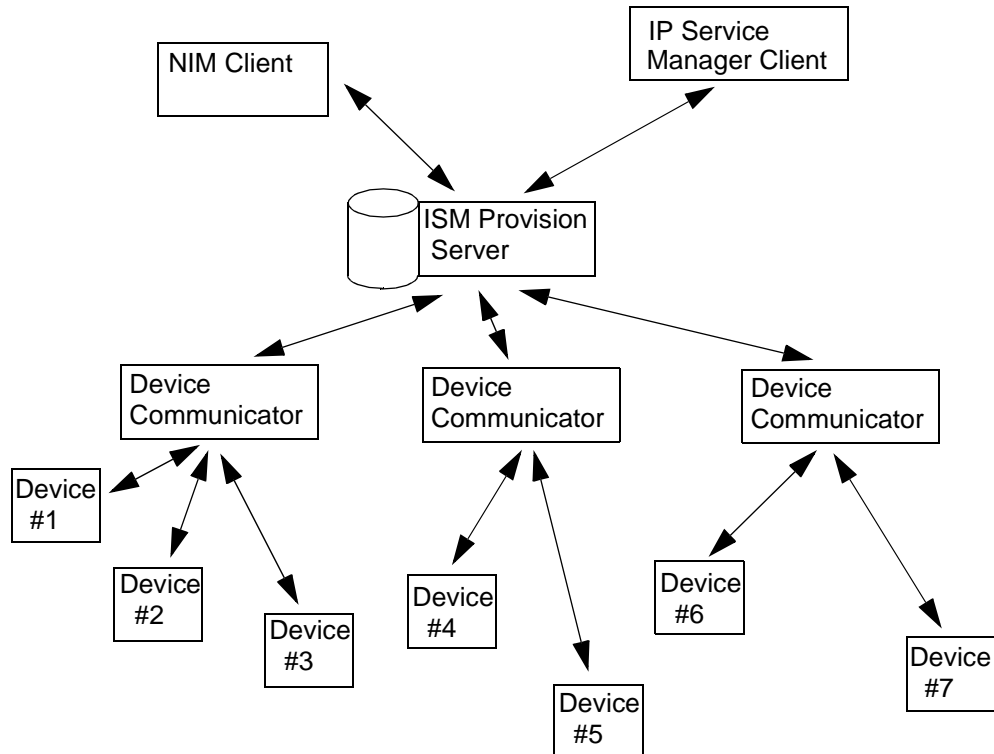


Figure 1-1: ISM Provision Components

ISM Provision consists of several different components:

- ISM Provision Server
- Device Communicators
- Network Infrastructure Manager Client
- IP Service Manager Client

These components work together to manage another important component:

- Your Network Devices

The following sections describe these components and how they interact in more detail.

Your Network Devices

The network managed by ISM Provision consists of your current existing network of Extreme Network devices, or a subset of your devices. Many devices can be managed by ISM Provision simultaneously. The devices are managed by querying them for their configurations, and by sending new configuration commands to them. Once ISM Provision manages a device, it will periodically check that the device configuration for changes.

ISM Provision Server

The ISM Provision server is the heart of ISM Provision. You may have more than one instance of the other components, but only one server. The server contains the information about the configurations of the managed devices, configurations that are scheduled to be applied to the network at a later time, and previous configurations. An ISM Provision server can contain the configurations of a large number of devices, but does not communicate with the devices directly. Instead, it uses device communicators to handle this task.

The ISM Provision server also contains the saved configuration changes that have not yet been applied to the network. These changes may be saved to edit later, or may be applied at a future time to the network.

Device Communicators

The device communicators control the communication between the network devices and the ISM Provision server. All queries to devices from the ISM Provision server and all commands from the ISM Provision server to the devices are handled by the device communicators. To spread the processing load across hosts, there can be more than one device communicator in an ISM Provision installation, but only one per host.

For example, in a network of 100 devices all managed with the same ISM Provision server, you might have five different device communicators, each talking with twenty devices. Any one managed device can only be managed by one device communicator, otherwise conflicts will occur.

Typically, you will install one device communicator on the same host as the ISM Provision server, and then add other device communicators on other hosts as needed to manage the processing load of communicating with your devices.

Network Infrastructure Manager Client

The Network Infrastructure Manager (NIM) client is used to manage changes to the network infrastructure. With NIM you can prepare and commit changes to the current network configuration, and add new devices to be provisioned. Before changes are rolled out to your network, NIM tests your proposed changes against a set of rules designed to spot and help you correct errors (for example, duplicate IP addresses assigned to different VLANs).

The NIM client also manages the providers, provider accounts, and provider access to network resources. With NIM you can define a provider and restrict that provider's control to a specific set of ports on a specific set of devices. You can also restrict the allowable VLAN IDs and IP addresses that the provider can assign.

The NIM client also manages the ISM Provision server and device communicators. You can see the status of the server and communicators and examine their logs. You can also see who is currently connected to the ISM Provision server and send a broadcast message to them. You can shutdown the ISM Provision server from within NIM.

Finally, you can review the current changes in your session, review committed, saved and scheduled jobs, and perform configuration versioning.

IP Service Manager Client

The IP Service Manager client allows providers to manage subscribers (subscribers consist of a VLAN and a single port in your network). IP Service Manager also allows you to configure service bundles (these correspond to QoS profiles) and policy based services (these correspond to access control lists) for these subscribers.

2

Starting Network Infrastructure Manager

Overview

Since the Network Infrastructure Manager (NIM) client is part of ISM Provision, NIM relies on a running ISM Provision server and device communicator. This chapter assumes that you already have a functioning ISM Provision server and device communicator. For information about installing and starting an ISM Provision server and device communicator, see the document, *ISM Provision Installation Guide*, available as a PDF file, “install-1-0.pdf” on your ISM Provision CDROM.

Starting Network Infrastructure Manager

The following is a short summary of the steps to start Network Infrastructure Manager

Summary Steps. To start Network Infrastructure Manager you must:

- 1 **Launch the NIM Client**
- 2 **Specify the ISM Provision Server**
- 3 **Enter a User Account Name**
- 4 **Enter the Password for the Account**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To start Network Infrastructure Manager you must:

1 Launch the NIM Client

Launch the NIM client as you would launch other applications on your host. For example, Windows users can select **Network Infrastructure Manager** from the **Start>Programs>Extreme Networks>ISM Provision>Applications** menu. Solaris users can launch the **nim** executable file from the **/opt/extreme/ismprov/bin** directory by using a graphical file manager application to double-click on its icon, or by typing:

```
/opt/extreme/ismprov/bin/nim
```

Once the application starts, you will see the login screen similar to the one shown in Figure 2-1.

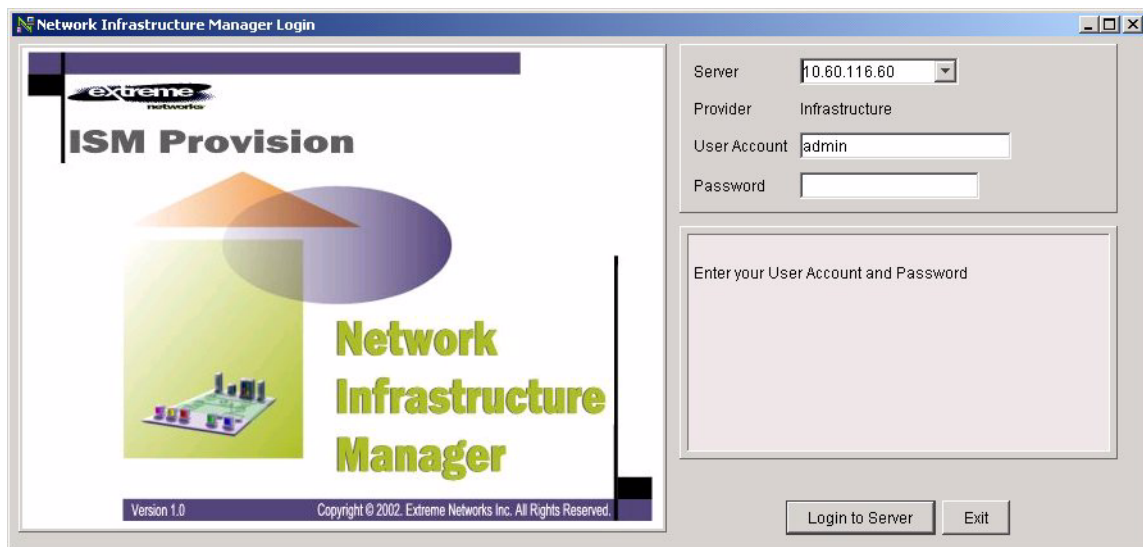


Figure 2-1: Network Infrastructure Manager Login Screen

2 Specify the ISM Provision Server

Once the login screen appears, you will specify the ISM Provision server. Specify the IP address of the server or the hostname by typing it into the server field. Figure 2-2 shows the login screen and server field in more detail (if the server is on the same host as the NIM client, you can also specify “localhost”).

NIM will store the IP addresses and names that you have specified in previous sessions, so you may find your server already specified, or you may be able to select

it from the drop-down list in the server field. Click on the down-arrow on the right side of the field and select the server.



Server 10.60.116.60

Provider Infrastructure

User Account admin

Password

Enter your User Account and Password

Login to Server Exit

Figure 2-2: NIM Login Screen Detail

3 Enter a User Account Name

In the **User Account** field, enter your user account name. The previously accessed account name is displayed in the field, so you may not need to enter a name.

4 Enter the Password for the Account

Enter the account password. The account passwords are not saved and will need to be entered every session.

Once the information has been entered, click the **Login to Server** button, then the NIM client will attempt to connect with the ISM Provision server. While it is connecting you will see messages similar to those in Figure 2-3.

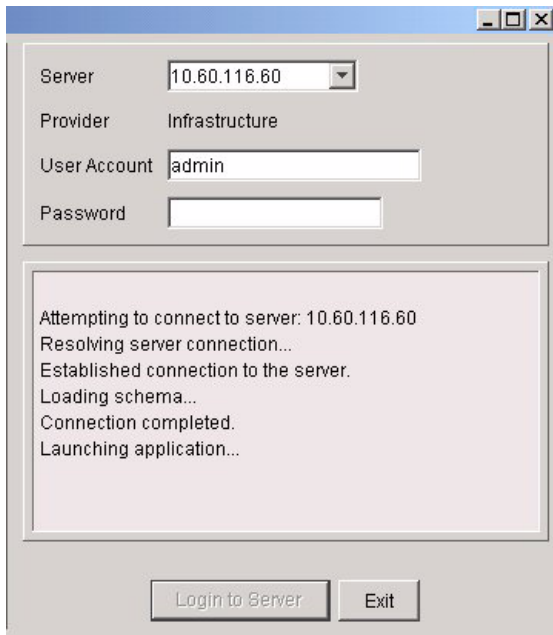


Figure 2-3: The NIM Client Connecting to the ISM Provision Server

Once the NIM client is launched, you will see the **Network Provision** view.

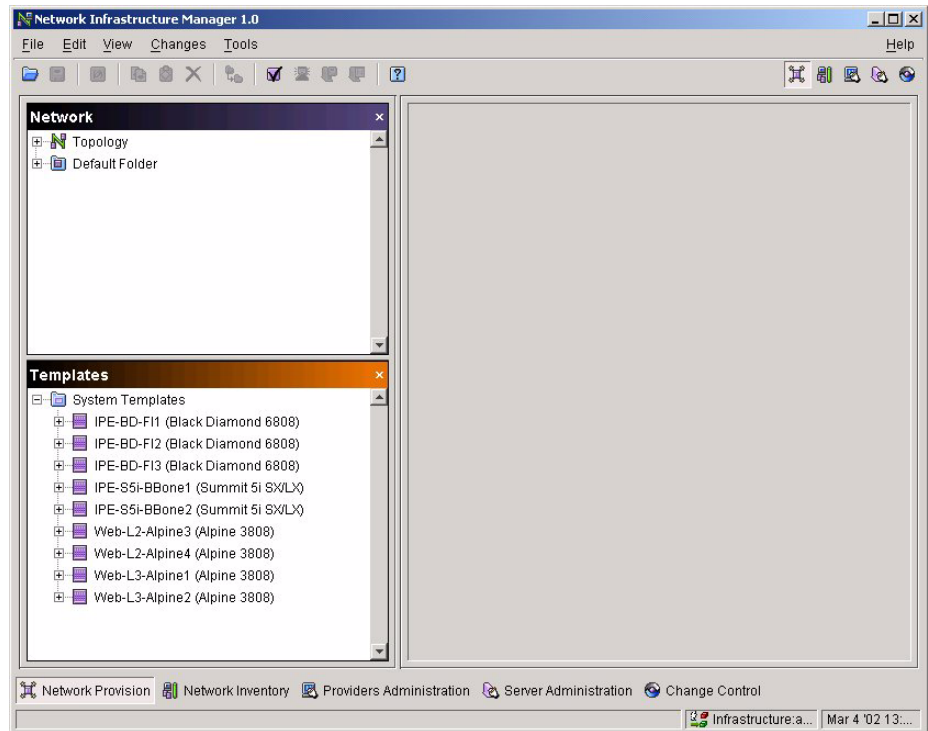


Figure 2-4: NIM Initial Screen

When NIM launches, the **Network Provision** view is initially displayed. You are now ready to use NIM. See Chapter 3, *Network Infrastructure Manager Overview*, for more information about NIM.

3

Network Infrastructure Manager Overview

Network Infrastructure Manager Overview

Network Infrastructure Manager (NIM) is composed of a number of views that are organized to complement your workflow. The different views allow you to manage different functional areas controlled by NIM. They are:

- Network Provision View
- Network Inventory View
- Providers Administration View
- Server Administration View
- Change Control View

NIM also has a number of icons and menus that are available from all of the views.

Summary of Features

- Layer 1 to 4 configuration: ports, trunks, VLANs, IP addressing, routing protocols, ACLs
- Extreme Networks-only device support: BlackDiamond, Alpine, and Summit (*i* chipset and 24e3 only)
- Service Provider Administration (wholesale model support)
- ISM Provision Server Administration (device communicators, utilities)
- Configuration Versioning (change histories, checkpoints)

- Configuration and topology import from devices and input files

NIM Views

When NIM is first launched you will be presented with the Network Provision view, as shown in Figure 3-1. The different views are described below.

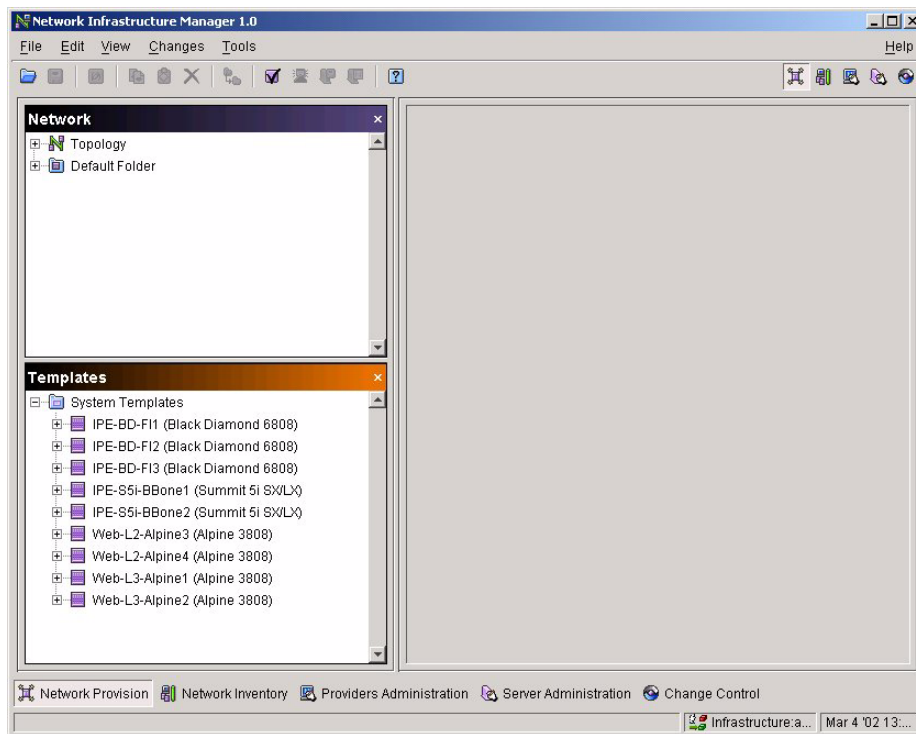


Figure 3-1: Initial NIM Network Provision View

Selecting NIM Views

There are four ways to select a particular view. One way is to select the desired view from the icons near the upper right side of the NIM client screen, as shown in Figure 3-2. From left to right the icons represent the views Network Provision, Network

Inventory, Providers Administration, Server Administration, and Change Control. Select the icon to display the view.

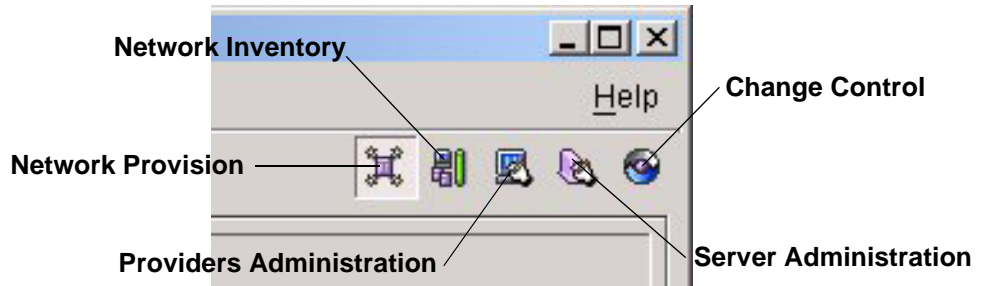


Figure 3-2: Selecting a NIM View Using Icons

A second way is to select the View menu and choose the view, as shown in Figure 3-3. A third way is to use the shortcut keys also shown in Figure 3-3. Press the [ALT] key

and a number key at the same time to use the shortcuts. For example, press [ALT]+3 to choose the **Providers Administration** view.

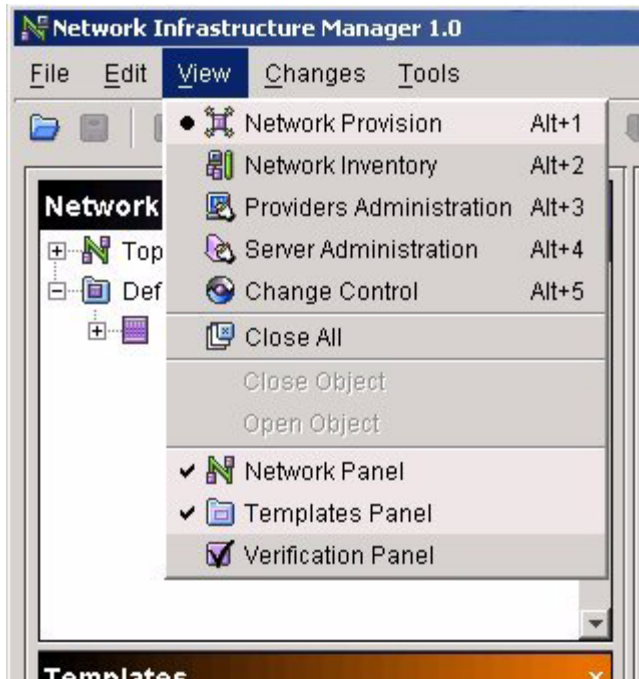


Figure 3-3: Selecting a NIM View Using the Menu

A fourth way is to select the view from the named icons near the bottom of the NIM client screen, just above the status line, as shown in Figure 3-4.



Figure 3-4: Selecting a NIM View Using Named Icons

Network Provision View

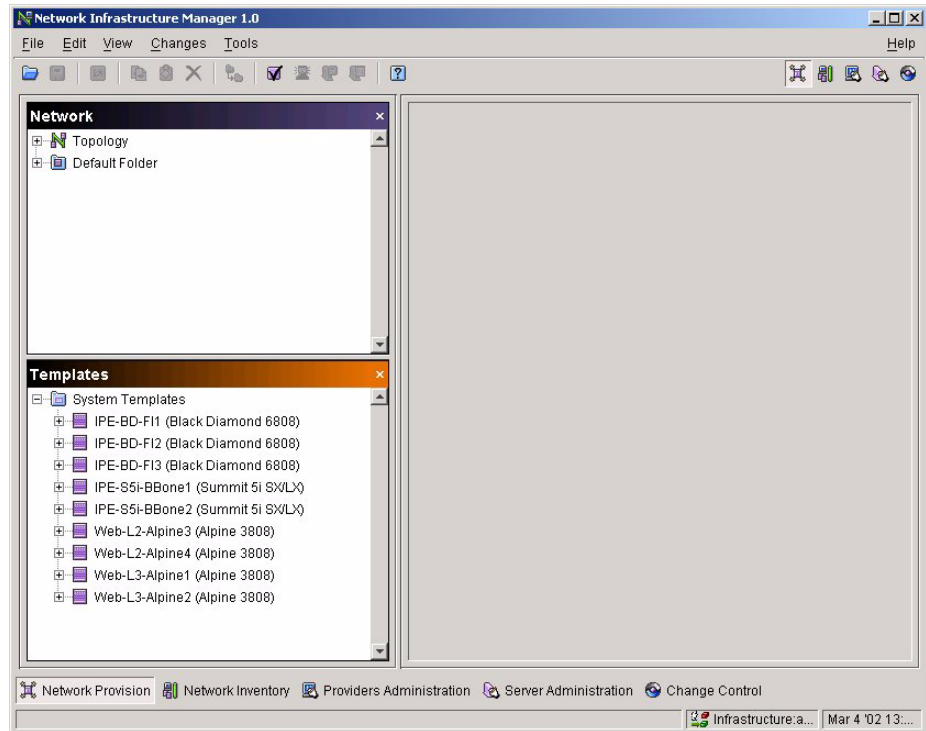


Figure 3-5: NIM Network Provision View

The **Network Provision** view is used to stage changes to your network before actually committing them to your devices. From this view, you build configurations for new devices, modify configurations for existing devices, and view the current configurations of existing devices. Once you have made changes, you will either commit the changes to the network, save the changes without affecting the network, or throw away the changes by reverting to the current server state.

Saved changes are not saved on the local client host, but on the ISM Provision server, so they are accessible from other NIM clients, and can be viewed and reviewed by other NIM users. Saved changes can also be scheduled to be committed to your network at a later time.

Committed changes are also saved on the ISM Provision server, but they are also pushed out to your network devices. Committed changes become part of the current configurations of your devices.

At any time you may test your modified configurations against a number of rules derived from Extreme Network devices, ExtremeWare, and good networking practices. For example, if you attempt to re-issue an IP address that would conflict with your current configurations, you will be warned and the error will be identified so you can take action. You will also be warned if you select an incompatible set of modules for an Extreme Networks chassis.

Network Inventory View

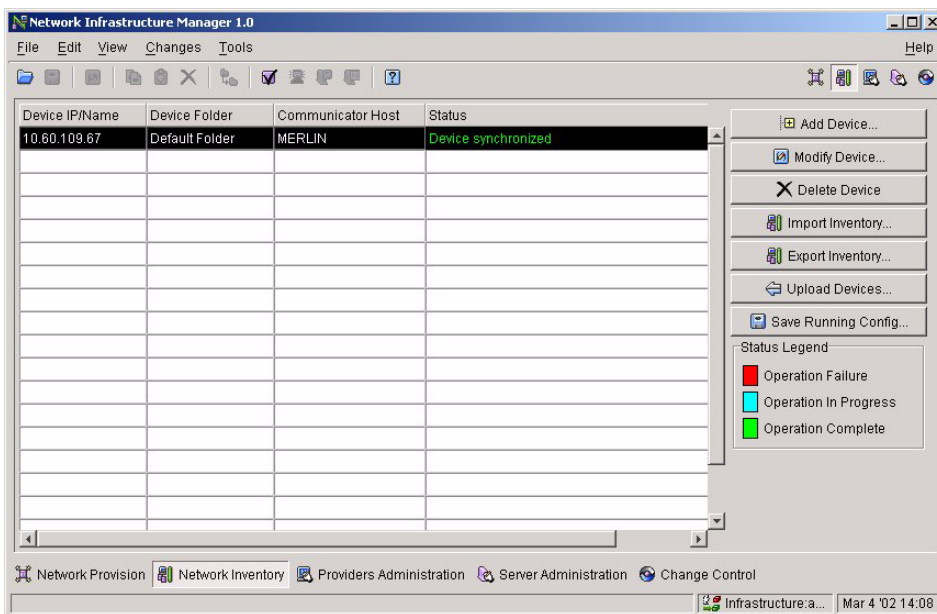


Figure 3-6: Network Inventory View

The **Network Inventory** view shows you the managed devices in your network. Managed devices are specified by their network name or IP address. ISM Provision manages the devices through the administrator account of each device. From this view you can add and remove managed devices, select which device communicator talks to each of the managed network devices, upload device configurations to the server, save device configurations to the device's NVRAM, and view the current status of the device.

If you have an existing network, this is likely the first view you will use. To capture the current state of your network you will add your devices to the inventory. By adding

your devices to the inventory, ISM Provision will read the current configurations and store them in the ISM Provision server.

From this view you can also export and import inventory files (you can also do this from the **File** menu). These files contain the administrator access information for devices. If you plan to add a large number of devices to the network inventory, you will likely create an inventory file and import it.

Providers Administration View

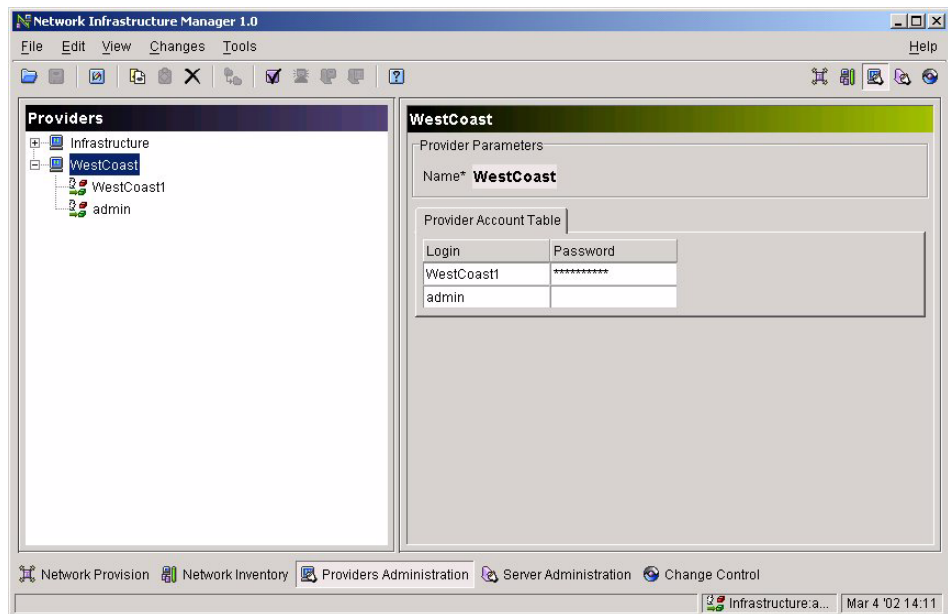


Figure 3-7: Providers Administration View

The **Providers Administration** view manages the providers, the provider user accounts and passwords, and provider resources that are accessible from the other ISM Provision client, IP Service Manager. From this view you can add, modify, and delete provider user accounts and passwords for IP Service Manager, and you can control provider access to devices, device ports, VLAN IDs, and IP addresses.

The **Providers Administration** view also manages the login accounts for NIM itself. In this view you can change passwords and add and delete accounts. The special provider name “Infrastructure” represents all of the user accounts for NIM. (That is why the NIM login screen has a read-only entry of “Infrastructure” for the **Provider** field.)

From this view there is a conversion tool to help you setup existing NIM objects to use in the IP Service Manager client.

Server Administration View

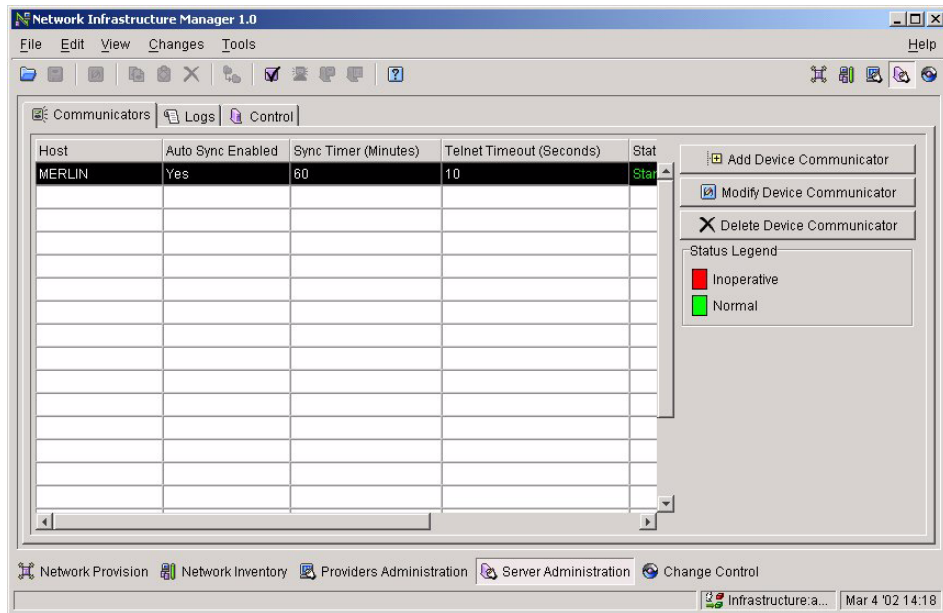


Figure 3-8: Server Administration View

The **Server Administration** view allows you to manage the ISM Provision server and device communicator servers. From this view you can add, modify, and delete device communicators, and verify their status. You can examine who is connected to the ISM Provision server, send a broadcast message to all connected users, and shut down the ISM Provision server. You can also examine the device communicator and ISM Provision server logs.

Change Control View

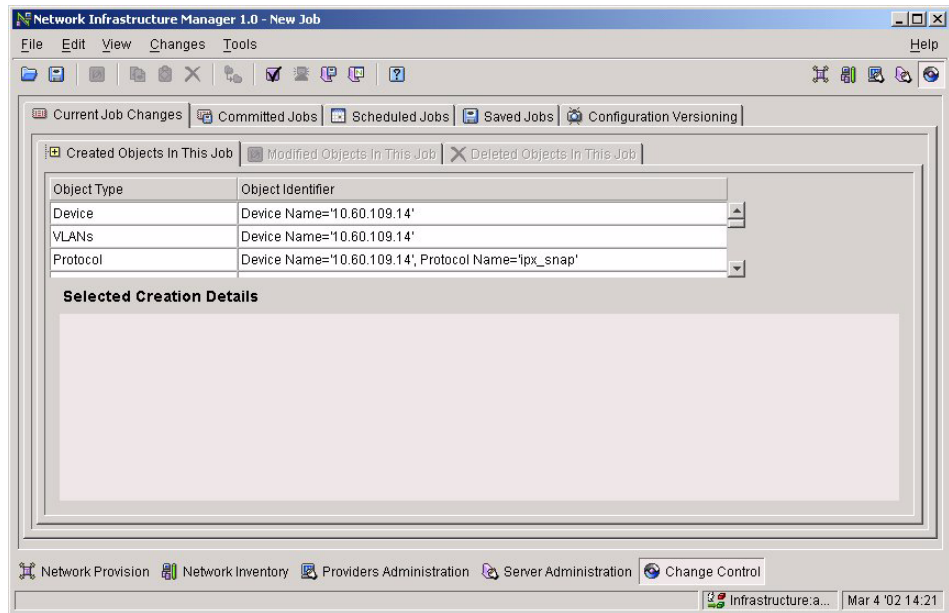


Figure 3-9: Change Control View

From the **Change Control** view you can manage the changes you create with NIM. For your current session, you can see the changes that you have made and not yet saved or committed to the network. There is a record of changes committed to the network and changes scheduled to be committed to the network.

You can also create network configuration versions; a collection of configurations for your entire managed network. This allows you to rollback all your device configurations to a known state.

NIM Icons

There are a number of icons visible from all of the NIM views. When the function associated with an icon is available, the icon is in color. When the icon function is not available, the icon is greyed out.



Figure 3-10: NIM Icons: Open Changes, Save Changes, Modify Object, Copy, Paste, Delete, Move Device, Verify Configuration, Synchronize, Commit Changes, Revert Changes, Help



Open Changes

Select this icon to open changes that you have previously saved to the ISM Provision server. The changes will be incorporated into your **Network Provision** view. Once opened, you can further modify the **Network Provision** view, or commit the changes to the network.



Save Changes

Select this icon to save changes that you have made. Saved changes are not pushed out to the network devices, but are saved on the ISM Provision server for further work, or to be viewed by others.



Modify Object

Select this icon to modify the currently selected object. In general, an object-specific wizard will open to allow you to change the object properties.



Copy

Select this icon to copy the currently selected object.



Paste

Select this icon to paste the previously copied object.



Delete

Select this icon to delete the currently selected object.



Move Device

Select this icon to move the currently selected device from one folder to another.



Verify Configuration

Select this icon to check your changes against the ISM Provision rules. If errors or warnings are found, they will be identified, and you can change them.



Synchronize

Select this icon to merge the changes from the server into your view, if you did not update your view when you were first notified.

When the network configuration changes because of the actions of another user, the state of the ISM Provision server changes. Your current view is now out of sync with the server. When the ISM Provision server changes, it notifies the NIM client and displays the **Server Update Notification** dialog box (if this option is set). From this box you can either select **Update Now** or **Update Later**. By selecting **Update Now**, the server changes are merged into your view. If you select **Update Later**, the **Synchronize** icon becomes available. At a later time you can then select the icon, and merge the sever changes into your view.



Commit Changes

Select this icon to commit your changes to ISM Provision. The changes are incorporated into the ISM Provision server and the device configurations are changed.



Revert Changes

Select this icon to discard changes you have made in NIM. Your changes will be removed and your view will be refreshed from the server.



Help

Select this icon to open a browser and display this document.

4

Network Provisioning

Overview

From the **Network Provision** view of Network Infrastructure Manager you can display and modify device configurations. These configurations may represent the actual configurations on your network, modified configurations that you intend to deploy to your network, or configurations for devices that do not currently exist in your network. You can copy the configuration of an existing device and modify it, and you can save typical configurations that you use in your network as a template to aid in adding additional devices.

At any time during the process of modifying the network configurations in **Network Provision** view, you may save your work without affecting the current network, to continue modifying later, or to allow others to review the changes before they are implemented. You can also back out the changes by reverting to the server state, so the **Network Provision** view only shows what is currently committed to the server.

Once you have modified the configurations in the view, you can apply the changes nearly simultaneously to the devices in your network by committing the changes to the ISM Provision server. Before changes are committed, or at any time you choose during the editing process, the changes are checked against a set of rules to detect errors like duplicate IP addresses, or unsupported module combinations.

This chapter explains the following concepts about the **Network Provision** view of Network Infrastructure Manager:

- Network Provision View Panels

- Configuration Objects
- Key Information
- Unsupported Configuration Commands
- Managed and Unmanaged Devices

This chapter also explains how to perform a number of tasks in the **Network Provision** view. The first set of tasks primarily deal with displaying the configurations in the system. The following tasks are documented in this first section:

- View Device Configurations
 - View a Single Configuration Object
 - View Multiple Configuration Objects
 - Modify Visible Configuration Options
 - Modify View Options

The next set of tasks deal with adding and modifying configuration objects. Here you would find information about adding a new device configuration or creating a new configuration object. The following tasks are documented in the section:

- Create and Modify Network Device Configurations
 - Add a New Device
 - Add a Configuration Object
 - Modify a Configuration Object
 - Copy a Device or other Object
 - Save Changes Without Changing Network Configuration
 - Remove Changes (Revert to Server State)
 - Change an Unmanaged Device into a Managed Device

The last set of tasks explains how to directly access a device in your network to manually modify its configuration. Since ISM Provision cannot directly support some commands, you may need to set some commands manually, either from the command line or from the web interface. The following tasks are documented in the section:

- Access Extreme Devices Directly
 - Use Telnet to access a device
 - Use Extreme WebVista to access a device

Network Provision View Panels

When you select the **Network Provision** view of NIM you will see a screen similar to that in Figure 4-1. This figure shows a single device in the default device folder, *10.60.109.67 (Alpine 3808)*. To create this example, an existing network device was added to the **Network Inventory**, as described in Chapter 5, “Managing the Network Inventory”. If you have not already added an existing device you can display a device configuration by adding a new device or copying a template to the **Network** panel in the **Network Provision** view. See the section, “Add a New Device”, or the section, “Copy a Device or other Object”, for instructions.

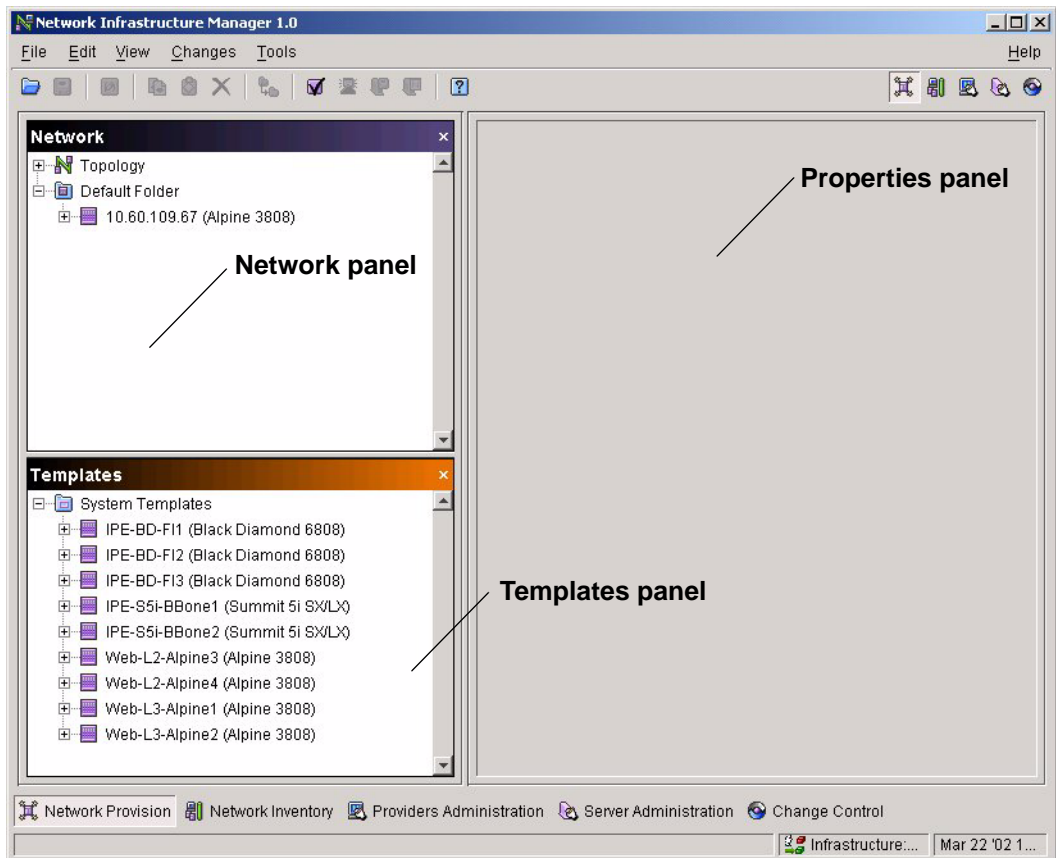


Figure 4-1: Network Provision View with One Device

The **Network Provision** view can show three named panels: **Network**, **Templates**, and **Verification** (The **Verification** panel is not visible in Figure 4-1). Additionally, there is a fourth, unnamed panel that is always visible in **Network Provision** view. For convenience, this document will refer to that panel as the **Properties** panel. Initially, NIM will show the **Network**, **Templates**, and **Properties** panel, and will show the **Verification** panel when a verification is performed. You can show the panels at any time from the **View** menu (see Figure 4-2).

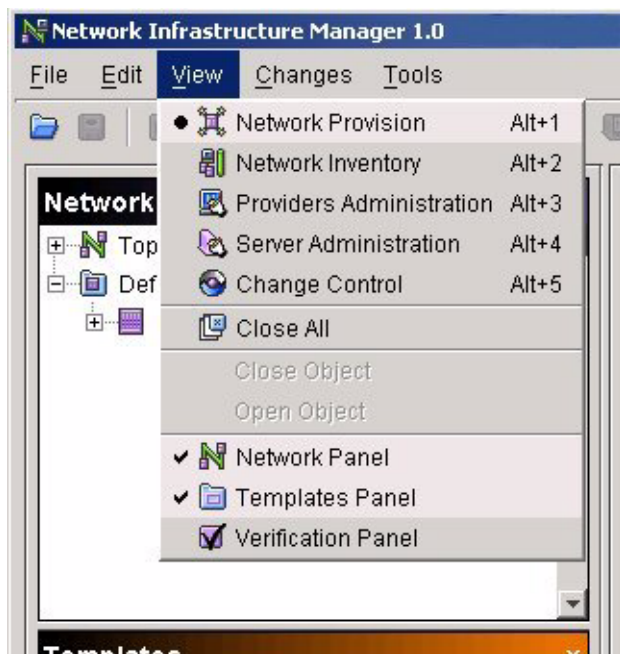


Figure 4-2: Selecting Network Provision Panels

To show a panel, select the **View** menu item for that panel. If the panel is visible, selecting its **View** menu item will close the panel.

Network Panel

The **Network** panel displays the configurations of any network devices that are in the network inventory (existing devices), any unmanaged device that you have created, and any configuration changes that you have made. Any object in the **Network** panel that has a plus (+) sign next to it can be expanded by clicking it. For example, if you click on

the plus sign next to a device name, the objects that make up that device will be displayed, like modules and VLANs. You can further expand any object displayed with the plus sign.

Templates Panel

The **Templates** panel displays device templates that were part of the initial installation and any that you have added. Like the **Network** panel, you can expand the objects in the **Templates** panel by clicking on the plus sign. You can also modify the templates in the **Templates** panel as you do the devices in the **Network** panel.

You can copy and paste a device from the **Network** panel into the **Templates** panel to be used as a template for later devices. Choose a device that has a typical configuration and use it for a template for adding similar devices. When ready to add a new device, copy and paste from the **Templates** panel to the **Network** panel, and modify its parameters.

Verification Panel

The **Verification** panel displays the results of verifying your device configurations against the ISM Provision rule set. From here you are alerted to any warnings or errors, and given an opportunity to correct them. You will also find suggested corrections for the error and warnings issued by ISM Provision. When you select an error or warning, the object causing the message is highlighted in the **Network** panel. You can then select and modify the object to correct the problem.

Properties Panel

The **Properties** panel shows information about the object selected in the **Network** panel. When you expand the objects in the **Network** panel you can display finer levels of detail about the configuration of your devices.

Configuration Objects

The **Network Provision** view displays the configuration objects that make up your network. Objects are an abstraction, a way to think about groups of commands that make up the configurations in your network. Here are some example objects: VLANs, an IP access list, a Qos profile, the SNMP parameters for your device, or even the entire

device configuration itself. Objects can be displayed, modified, copied, and pasted, so it is easy to add new objects with similar properties to your network configuration.

Objects can contain other objects. For example, a device object contains VLANs, modules, connections, access profiles, and other objects. A device's VLANs object contains objects named for all the VLANs on the device. A device folder object contains objects for all the devices in the folder. The object that contains other objects is called the parent of the other objects and the contained objects are the child objects. Whenever you create new objects you will specify the parent object that will contain the new object. For example, if you create a new device object, you will need to specify which device folder to place the new device. The device folder is the parent object of the device. Another example is the management access object. This object contains, among other things, the device user accounts. When you add a new user account to a device, you will first select the parent object, the management access object and then add the account information.

Key Information

A configuration object managed by ISM Provision is tracked by its object type and its key information. No other object of that type can use the same key information. When you create an object you supply its key information, denoted by a field that ends with an asterisk (*). For example, when you create a VLAN, you type the VLAN name into the **Name*** field. No other VLAN on this particular device can use this name. Since ISM Provision tracks an object by its key information, you cannot modify key information for objects. You can modify other parameters for objects, but not the key. If you want to have an object with the same parameters but different key information, you will need to copy the object, and provide the new key information when you paste it. The **Finish** button on any of the **Create** wizards will not be enabled unless the key information is entered.

Unsupported Configuration Commands

There are some ExtremeWare configuration commands that are unsupported by NIM and do not appear as GUI objects. These configuration commands fall into two categories: commands that are not appropriate to manage with NIM and commands that are not yet implemented in the current ISM Provision version. For example, the command `cli paging` (CLI paging) is unsupported.

However, commands classed as unsupported can still be managed by ISM Provision. These commands are added as CLI commands to the device configurations. The **Unsupported Configuration** object displays a list of commands that have been added to the managed device. If you upgrade your devices to a later version of ExtremeWare, ISM Provision can still track the new features through the Unsupported Configuration command list.

To add commands to the device configuration, you can use the Telnet or Extreme WebVista tool within NIM to access the device. See the tasks described in the section, “Access Extreme Devices Directly”, for more information.

Managed and Unmanaged Devices

The **Network Provision** view displays both managed and unmanaged devices. The **Network Inventory** view displays only the managed devices.

Managed devices correspond to actual devices in the network. The configurations of managed devices are stored on the ISM Provision server and kept in synchronization with the actual device configurations. If a change is committed to the configuration on the server, that change is made to the device's configuration. If a change is made to the device, that change is added to the server when the device communicator next synchronizes with the device. An unmanaged device will also have its configuration stored in the ISM Provision server, but will not be synchronized with a network device. Any changes to the configuration of an unmanaged device remain in the server database.

To synchronize the device to the server, the ISM Provision server uses a device communicator to monitor the device. Any changes to the device are added to the server and any changes to the server are moved to the device. Each managed device is assigned to a device communicator that is responsible for periodically checking the device's configuration and updating any changes to the database, and to take committed changes from the database and implement them on the device.

Unmanaged devices, in contrast, need not actually exist. Unmanaged device configurations are saved or committed in the ISM Provision server database like managed devices, but the configuration is never compared with an existing device. There is no device communicator assigned to the unmanaged device, and the unmanaged device's configuration, seen in the **Network Provision** view, is not synchronized with an actual device.

You will likely create an unmanaged device in preparation to adding an actual device to your network. Once you have created the configuration, you can then change the unmanaged device to a managed device, and ISM Provision will load the configuration onto the actual network device, overwriting any existing configuration on the device.

View Device Configurations

The **Network** panel in the **Network Provision** view of NIM displays device configurations. Rather than displaying the configuration as a text file listing all the configuration commands, NIM displays the configuration as a set of objects and properties. You can fine tune the display of information to just those objects that interest you, and select how much information to display.

In this section you will find instructions how to:

- View a Single Configuration Object
- View Multiple Configuration Objects

Additionally, you can change how configuration information is displayed by using the following procedures:

- Modify Visible Configuration Options
- Modify View Options

View a Single Configuration Object

If you want to view one of the configuration objects of a device, select the object and the object properties will be displayed in the **Properties** panel. Some objects are collections of other objects. You may need to expand an object to display one of its constituent objects. Click an object's plus sign (+) to expand it.

Summary Steps. To view a single configuration object:

- 1 **Select the object**
- 2 **View the object in the Properties panel**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To view a single configuration object:

1 Select the object

You may need to expand an object in the **Network** panel to select one of its constituent objects. In the following example, to display the properties of the VLAN *v1* on device *10.60.109.67* we will do a combination of expanding and selecting objects to display the final properties.

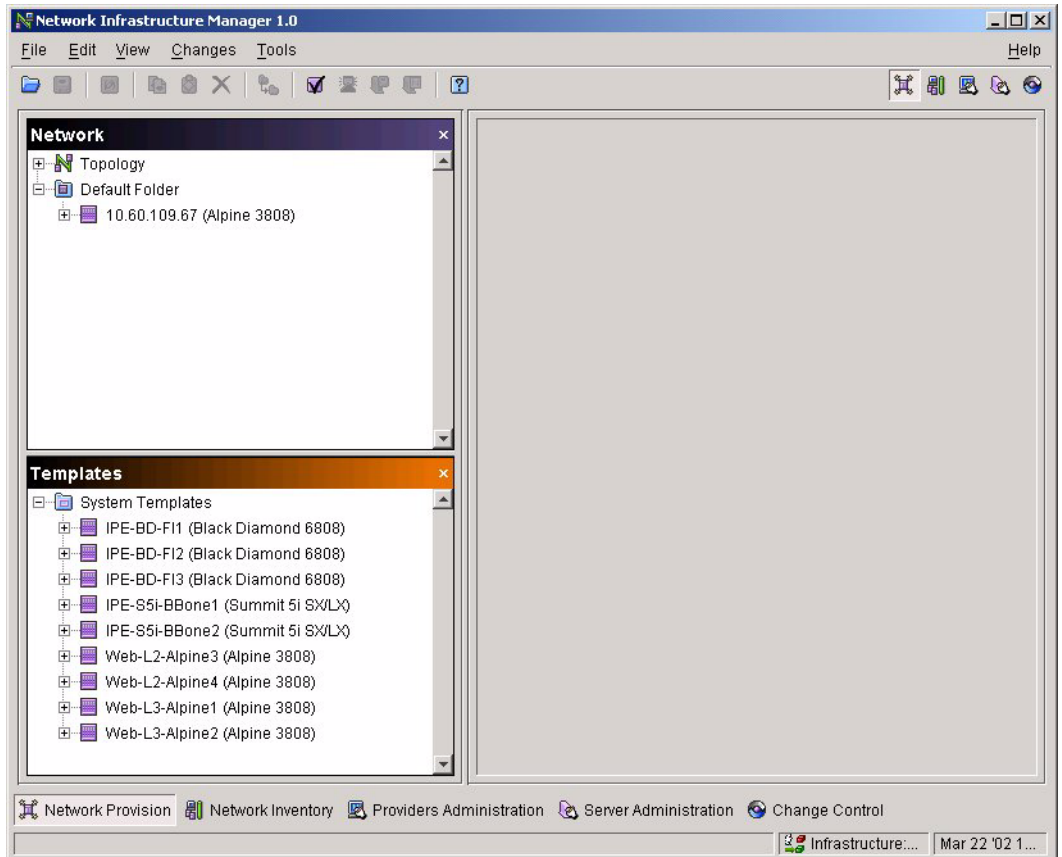


Figure 4-3: Single, Unexpanded Device

In the example (Figure 4-3) we start with a single, unexpanded device. By clicking the plus sign (+) to the left of the device name *10.60.109.67*, the device object expands to show the next level of objects (Figure 4-4).

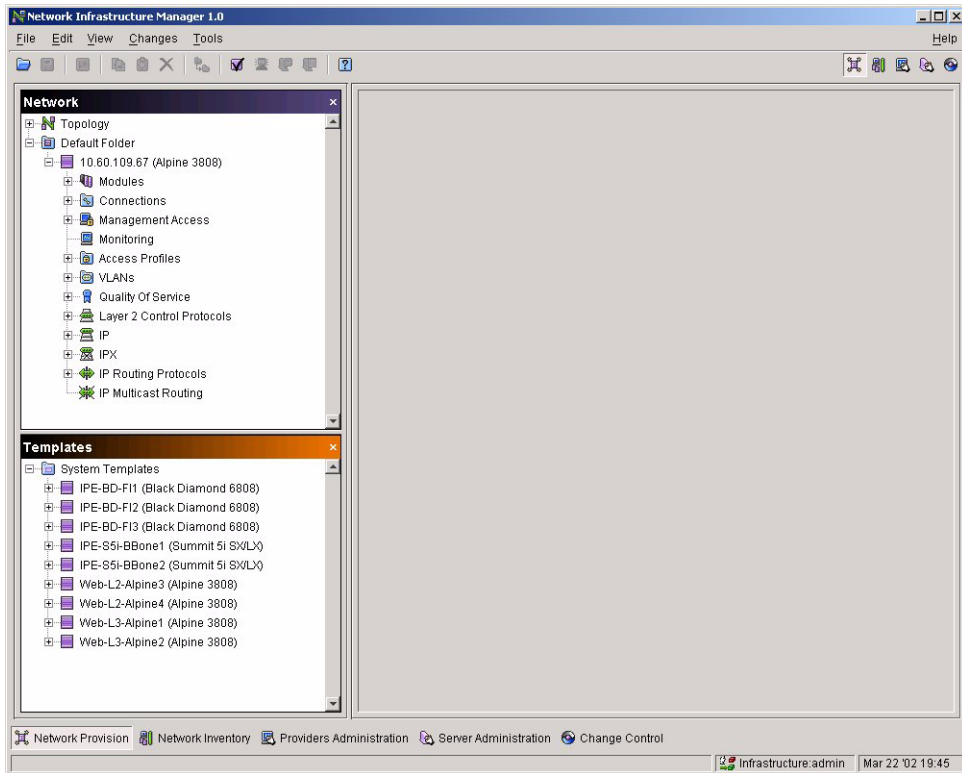


Figure 4-4: Device Expanded to Show Next Level of Objects

The following figure (Figure 4-5) is a detail view of the **Network** panel from Figure 4-4.

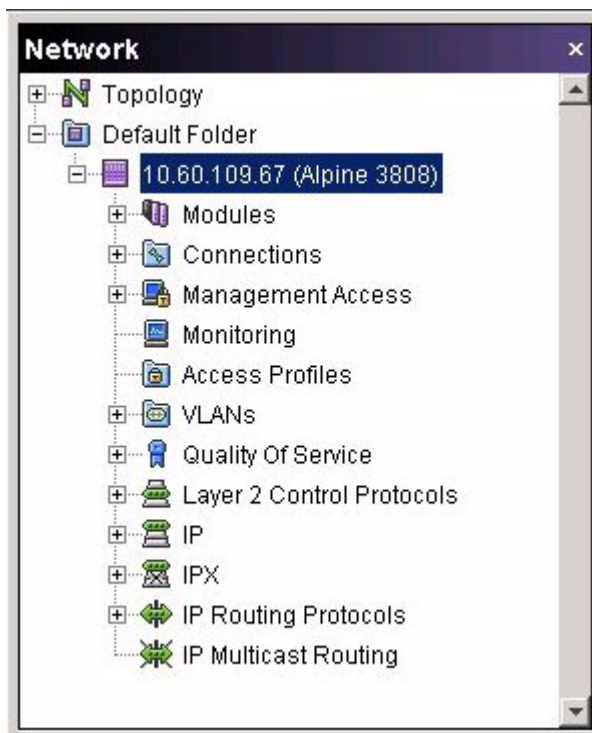


Figure 4-5: Network Panel Detail of Figure 4-4

The objects that make up device *10.60.109.67* are now displayed in the **Network** panel (To control which of these device objects are displayed, see the section “Modify Visible Configuration Options”). To display the properties of VLAN *v1*, click the plus sign (+) next to the **VLANs** object in the **Network** panel. Figure 4-6 shows the **Network** panel with the **VLANs** object expanded. Now the VLANs on this device are visible as separate objects.

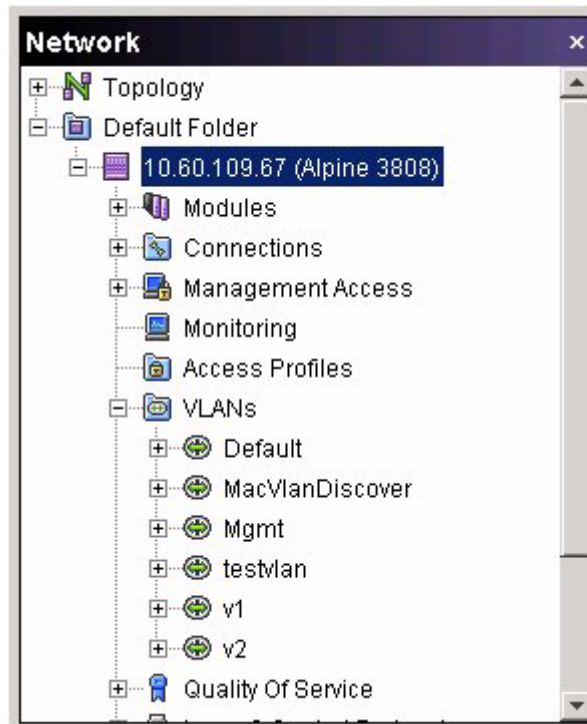


Figure 4-6: Network Panel with **VLANs** Expanded

Now that the VLAN object **v1** is visible, click on the object name to display the object properties in the **Properties** panel.

2 View the object in the Properties panel

Figure 4-7 shows the VLAN object **v1** selected and its properties displayed in the **Properties** panel.

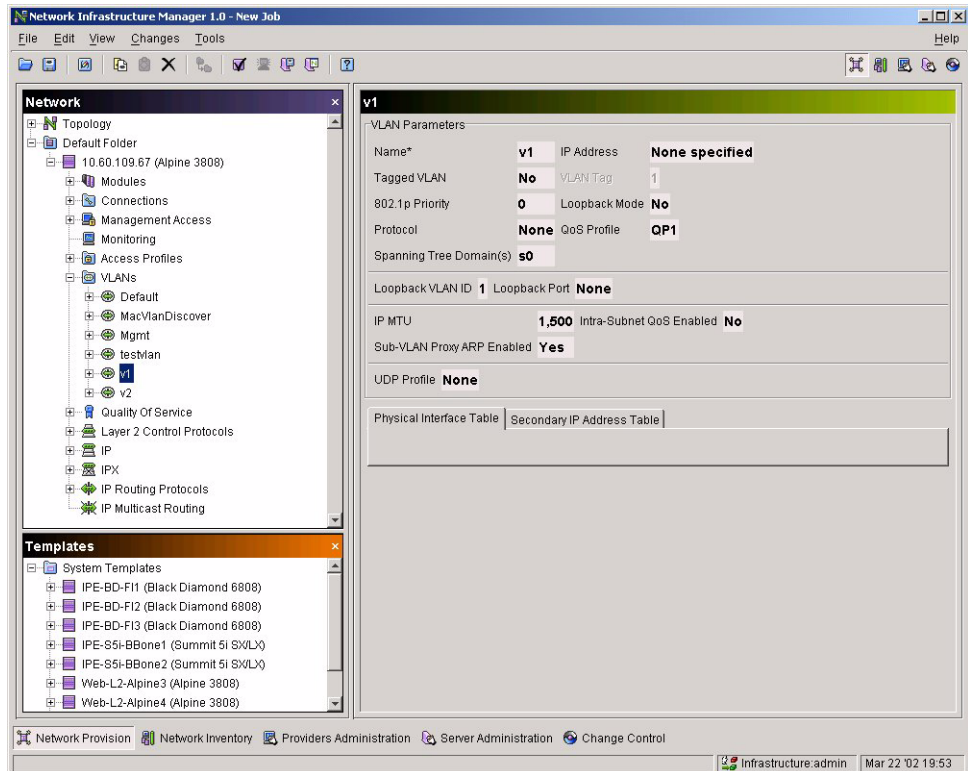


Figure 4-7: VLAN v1 Properties

Figure 4-8 shows the **Properties** panel for the VLAN v1 properties in more detail. Properties such as the VLAN name, IP address, VLAN Tag (if a tagged VLAN), and others are shown in this panel.

v1

VLAN Parameters

Name*	v1	IP Address	None specified
Tagged VLAN	No	VLAN Tag	1
802.1p Priority	0	Loopback Mode	No
Protocol	IP	QoS Profile	QP1
Spanning Tree Domain(s)	None		
Loopback VLAN ID	1	Loopback Port	None
IP MTU	1,500	Intra-Subnet QoS Enabled	No
Sub-VLAN Proxy ARP Enabled	Yes		
UDP Profile	None		
Secondary IP Address Table			

Figure 4-8: VLAN *v1* Properties Detail of Figure 4-7

Some of the properties that you might expect to see of the VLAN *v1* are not displayed in the panel, for example, the ports that belong to this VLAN, or whether OSPF is enabled for this VLAN. To see additional properties, notice that the VLAN object *v1* has a plus sign (+) next to it in the **Network** panel. This indicates that this VLAN object consists of other objects. Expand the VLAN object and select the sub-object to display its properties. For example, select the **OSPF** object shown in Figure 4-9 to display the OSPF properties of the VLAN *v1*.

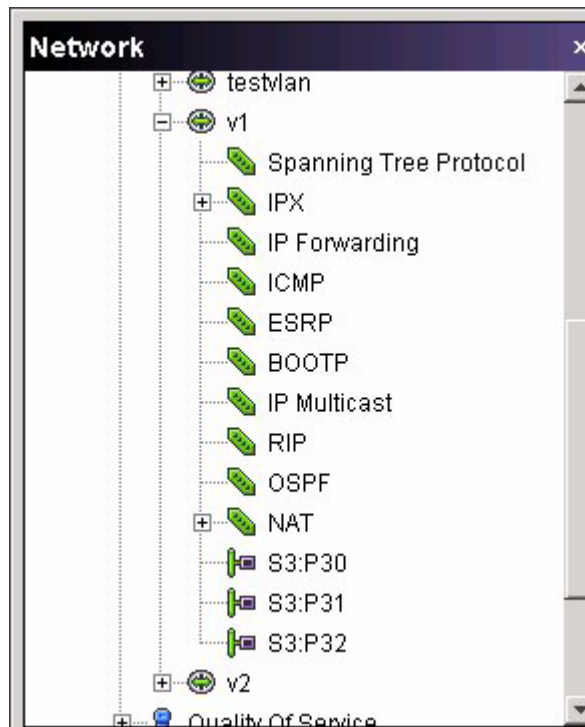


Figure 4-9: Expanded VLAN v1 Object

View Multiple Configuration Objects

You may need to view multiple configuration objects at the same time. For example, if you want to compare the settings for ports on two different devices, you will want to view the two objects at the same time. The **Properties** panel shows one object at a time, but you can open an object in its own window for viewing.

Summary Steps. To view multiple configuration objects:

- 1 Select the object to open**
- 2 Select View>Open Object**
- 3 Repeat steps 1 and 2**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To view multiple configuration objects:

1 Select the object to open

Selecting an object is covered in the detailed first step, “Select the object”, in the section, “View a Single Configuration Object”. Once the object is selected, it is displayed in the **Properties** panel.

2 Select View>Open Object

To open the object, select **Open Object** from the **View** menu, or by right-clicking on the object or the **Properties** panel and choosing **Open Object** from the pop-up menu (Figure 4-10).

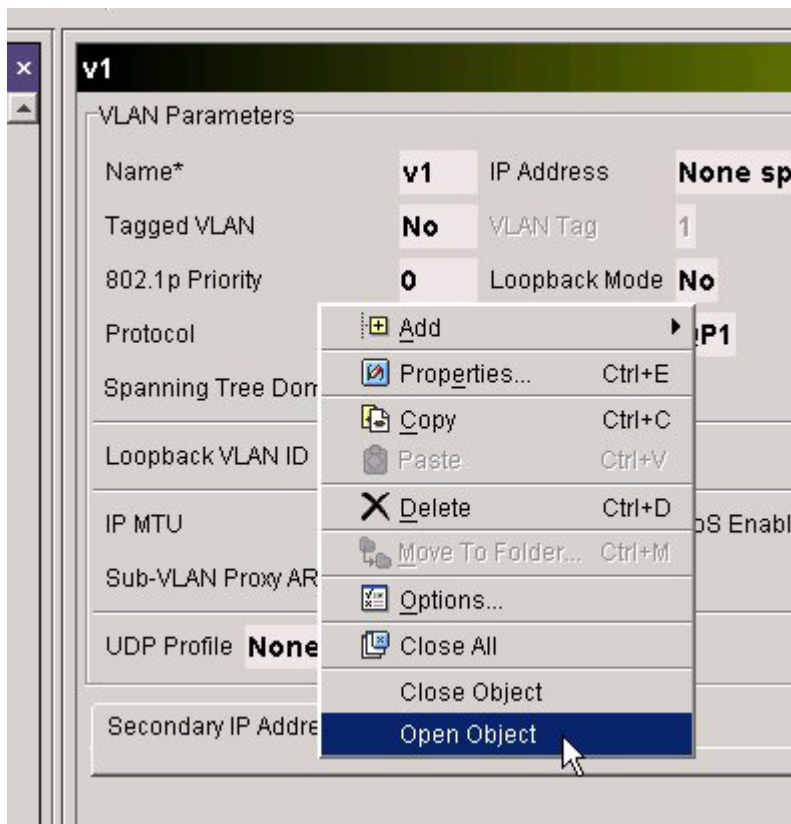


Figure 4-10: Selecting Open Object from a Pop-Up Menu in the Properties Panel

Once you have selected **Open Object**, a separate window will open to display the properties of that object. This window can only display object properties; you cannot modify the object parameters or launch a wizard from this window.

The screenshot shows a window titled 'v1' with a close button in the top right corner. The window displays the following properties for VLAN v1:

VLAN Parameters			
Name*	v1	IP Address	None specified
Tagged VLAN	No	VLAN Tag	1
802.1p Priority	0	Loopback Mode	No
Protocol	IP	QoS Profile	QP1
Spanning Tree Domain(s)	None		
Loopback VLAN ID	1	Loopback Port	None
IP MTU	1,500	Intra-Subnet QoS Enabled	No
Sub-VLAN Proxy ARP Enabled	Yes		
UDP Profile	None		
Secondary IP Address Table			

Figure 4-11: VLAN v1 Properties Displayed in New Window

3 Repeat steps 1 and 2

Select other objects to open, then choose **Open Object** to display each in its own window. Figure 4-12 shows VLANs v1 and v2 displayed in separate windows, with the **Properties** panel showing the general VLAN properties of the **VLANs** object.

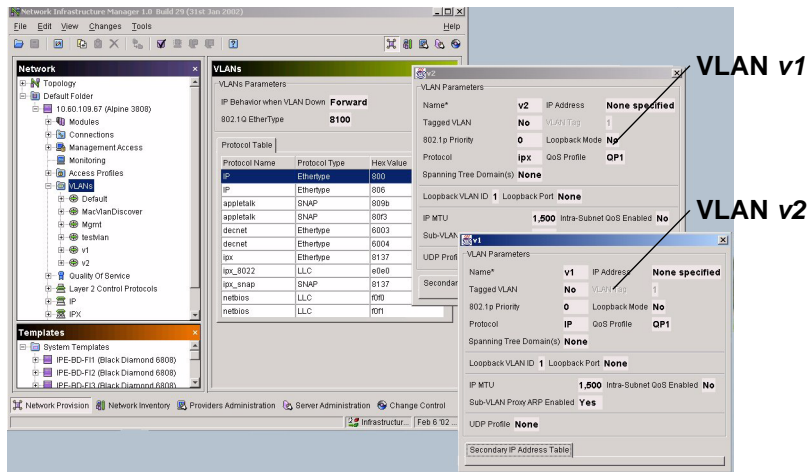


Figure 4-12: VLANs v1 and v1 Displayed in Separate Windows

Modify Visible Configuration Options

By default, NIM displays all the device configuration objects when the device is expanded. You may not need to change the configuration of some of the objects for your network, or you may wish to suppress display of some of the objects for your session. For example, you can suppress display of IPX configuration options if you don't support IPX in your network, or perhaps you only want to see the access profile information for a number of devices because you are only modifying them for your current session.

Changing the display of the objects does not affect the ISM Provision server, and only applies to the client you are currently running.

Summary Steps. To modify visible configuration options:

- 1 Open the Options dialog box
- 2 Select the Visible Configuration Options tab (if not already visible))
- 3 Select the options to display
- 4 Select Close

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To modify visible configuration options:

1 Open the Options dialog box

Right-click the **Network** or **Properties** panel to display a pop-up menu and select **Options** (see Figure 4-13), or select the **Tools>Options** menu item to open the **Options** dialog box.

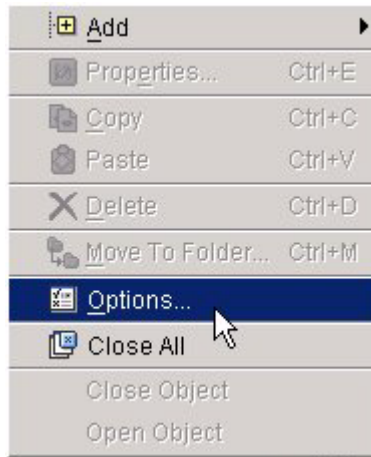


Figure 4-13: Selecting Options from Pop-Up Menu

2 Select the Visible Configuration Options tab (if not already visible)

The **Visible Configuration Options** tab of the **Options** dialog box should be visible. If not, select it to bring the options forward (Figure 4-14).

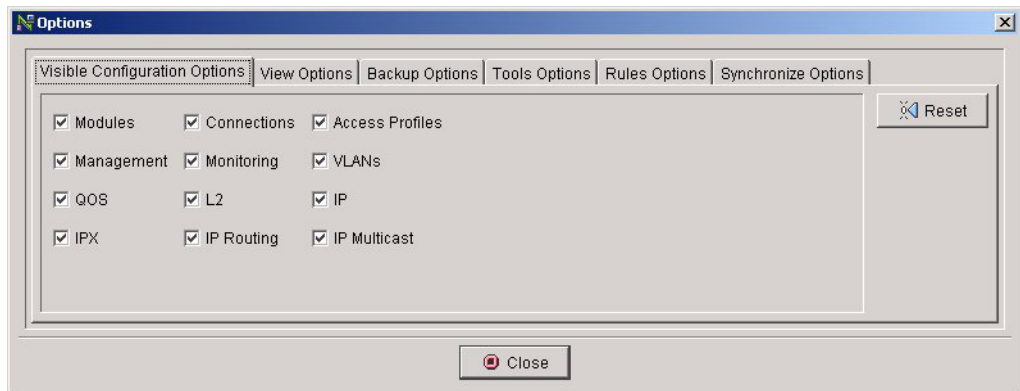


Figure 4-14: Visible Configuration Options Tab of the Options Dialog Box

3 Select the options to display

Check the boxes to display the objects. Uncheck the boxes to hide the objects. The object display in the **Network** panel changes as you check or uncheck the boxes, so you see your changes immediately.

4 Select Close

Select **Close** to return to NIM. Since you have not changed any of the configuration, merely suppressed its display, there will be no change to the server icons.

Modify View Options

The two view options that can be modified are **Use Tabs for Object Panels** and **Track Window Dimensions**.

Use Tabs for Object Panels controls object display in the **Properties** panel. With tabs enabled, each time you select an object to view, a tab is created in the **Properties** panel so you can quickly return to that object without having to select it in the **Network** panel. However, the **Properties** panel can become cluttered if you select a large number of different objects during a session.

Track Window Dimensions allows the client to track you as you resize client windows. The next time the client opens a window, it will use the latest size you chose. If **Track Windows Dimensions** is not selected, you can choose the default window size from the **View Options** tab of the **Options** dialog box

Steps. To modify view options:

1 Open the Options dialog box

For details, see the step, “Open the Options dialog box”, in the task, “Modify Visible Configuration Options”.

2 Select the View Options Tab

3 Modify settings

Create and Modify Network Device Configurations

The heart of ISM Provision is the ability to roll out network changes in a controlled manner. The powerful provisioning functions allow you to take existing device

configurations and modify them for new devices, create templates for typical device configurations, and coordinate changes across many devices.

In this section you will find instructions how to:

- Add a New Device
- Add a Configuration Object
- Modify a Configuration Object
- Copy a Device or other Object
- Save Changes Without Changing Network Configuration
- Change an Unmanaged Device into a Managed Device
- Change an Unmanaged Device into a Managed Device

Add a New Device

You can add a new device configuration into the **Network** panel of the **Network Provision** view. The device you add will have a configuration similar to an unconfigured device. Once the device is added you can make, save, and/or commit changes to the configuration. Typically, you would add a device this way if you are planning to add a new device that will have a very simple configuration, or whose configuration will be very different from any other devices in your network.

If you have an existing device in NIM whose configuration is similar to the new device configuration, you will want to copy the device and modify it for the new device. See the section, “Copy a Device or other Object” for more information.

If you have an existing device in your network and you want to add that device and its current configuration into ISM Provision, see the section, “Add a Device to the Network Inventory” in Chapter 5, “Managing the Network Inventory”.

Summary steps. To add a new device:

- 1 Select a folder in the Network panel**
- 2 Launch the Create Device wizard**
- 3 Enter a device name (or IP address)**
- 4 Modify the other properties**
- 5 Select Finish**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add a new device:

1 Select a folder in the Network panel

If the **Network** panel is not open, select it from the **View** menu. Once the panel is open, click the device folder into which you will add the new device.

2 Launch the Create Device wizard

To launch the **Create Device** wizard, select **Edit>Add>Device** from the menu, or right-click in either the **Network** or **Properties** panels and select **Add>Device** from the pop-up menu. The **Create Device** wizard will appear.

3 Enter a device name (or IP address)

Enter the device name into the **Create Device** wizard. You must give the device a unique name to identify it for ISM Provision. Use the name or IP address that you plan to use when the device will be deployed, otherwise use a temporary name.

If possible, do not use a temporary name. Since ISM Provision uses the name as a unique key for the device, device names cannot be directly changed. To change the name at a later time you will need to copy the device, paste it back into the Network panel and give it a new name, then delete the original device entry.

4 Modify the other properties

Use the drop-down list to choose the type of device and the image you plan to use. As you make your choices, the wizard may allow other choices based on your selections. Use the **Next** button to advance through the wizard choices.

*If you select the **Managed Device** checkbox in the **Create Device** wizard, and fill in the other administrative access information, the configuration you create in NIM will overwrite the existing device configuration when changes are committed to the server. See the section, "Change an Unmanaged Device into a Managed Device", for more information.*

5 Select Finish

When you have made all the selections for the new device, select **Finish** to close the wizard.

Add a Configuration Object

Anytime you wish to add a configuration object, you will select the parent object that you want to add the object to. For example, when you add a device, you select the

device folder you want to add the device to. When you add a VLAN, you select the VLANs object in the device you want to add the VLAN to.

Summary Steps. To add a configuration object:

- 1 Select the parent object that will contain the new object**
- 2 Launch the Create wizard (Edit>Add)**
- 3 Enter the key information**
- 4 Enter additional information**
- 5 Select Finish**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add a configuration object:

- 1 Select the parent object that will contain the new object**

For example, to add a VLAN select the VLANs object (see Figure 4-15).

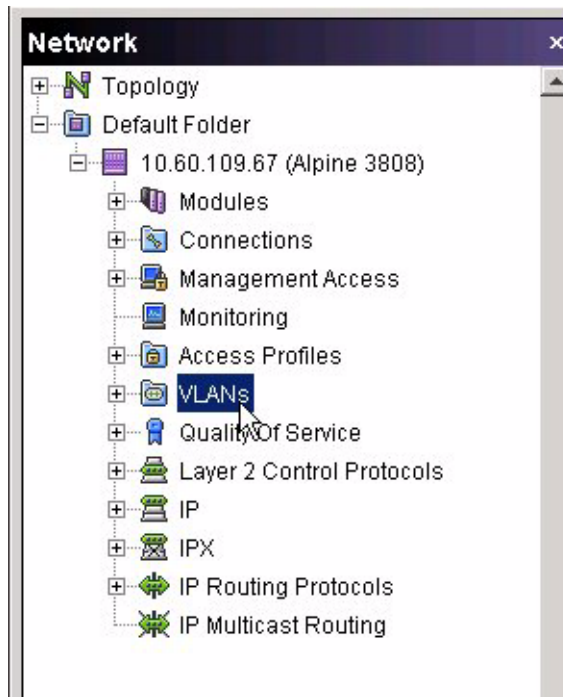


Figure 4-15: Selecting the VLANs Object

2 Launch the Create wizard (Edit>Add)

To launch the **Create** wizard, select the menu item **Edit>Add** and the object you wish to add. The object choices available to choose vary, depending on the objects that are appropriate to add to the parent object you selected. You can also launch the **Create** wizard by right-clicking on the parent object. The **Create** wizard that appears is dependent on the object you are adding. For example, if you are adding a VLAN, the **Create VLAN** wizard appears. If you are adding a device, the **Create Device** wizard appears (see Figure 4-16).

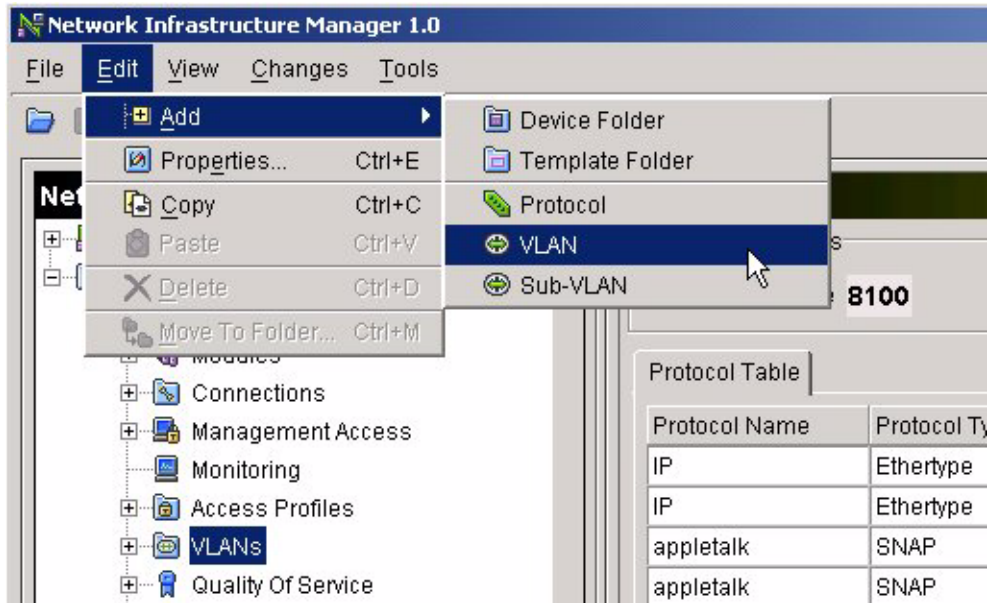


Figure 4-16: Launch the Create VLAN Wizard

3 Enter the key information

The field that ends with an asterisk (*) signifies the key information for the newly created object. This is the only information required to create the object, as the other object parameters are set to default values (see Figure 4-17).

Figure 4-17: Create VLAN Wizard

4 Enter additional information

Enter any other parameters that you wish to set. In Figure 4-17, the **Create VLAN** wizard shows a panel titled **Config Areas**. The **Config Areas** panel of the wizard represents additional pages of parameters available for you to set. Select the **Next** button or select the entry in the **Config Areas** panel to move to another page of parameters. The different wizards have different parameters and differing numbers of additional pages.

5 Select Finish

When you finish setting parameters for the object, select **Finish**.

Modify a Configuration Object

Any configuration object displayed in the **Network** panel can be modified. For example, you can modify the parameters of a QoS profile, or you can add or remove ports from a VLAN. The one exception is that key information cannot be modified. See the section, “Key Information”, for more information.

Summary Steps. To modify a configuration object:

- 1 **Select the object to modify**
- 2 **Launch the Modify wizard (Edit>Properties)**
- 3 **Edit the object properties**
- 4 **Select Finish**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To modify a configuration object:

- 1 **Select the object to modify**

Display the object you wish to modify and select it by left-clicking. See the section “View a Single Configuration Object” for detailed information on displaying (viewing) an object. For some objects, you may need to select its parent object instead. For example, to change which modules are configured in a device, you might try to select the **Modules** object and modify it. However, you cannot modify which module is configured from this object. You will need to select the parent device object to modify which module is present in a slot.

- 2 **Launch the Modify wizard (Edit>Properties)**

To launch the **Modify** wizard, select the menu item **Edit>Properties**. You can also launch the **Modify** wizard by right-clicking on the object and selecting **Properties** from the pop-up menu, or you can launch it by typing [CTRL]+E. The **Modify** wizard that appears is dependent on the object you are modifying. For example, if you are modifying a VLAN, the **Modify VLAN** wizard appears. If you are modifying a device, the **Modify Device** wizard appears (see Figure 4-18).

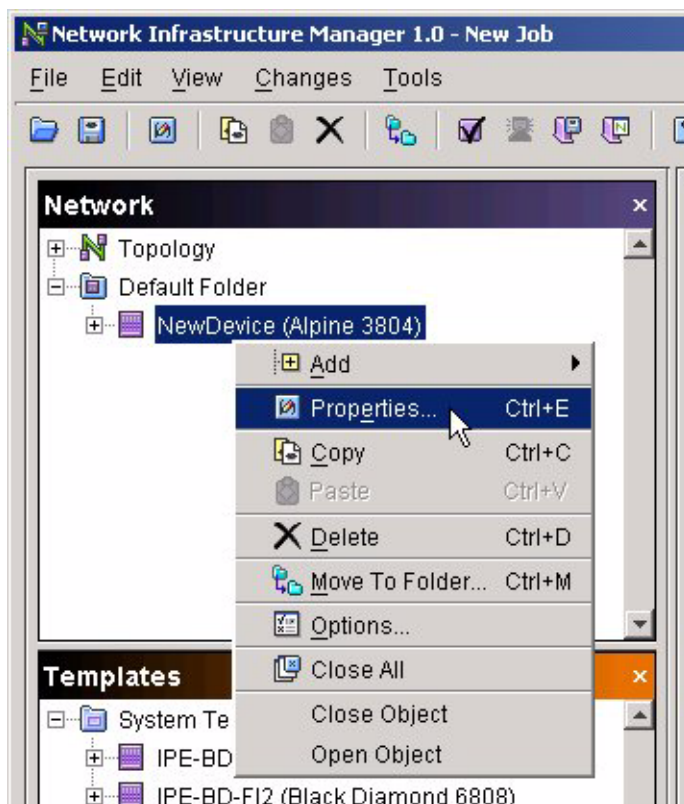


Figure 4-18: Launching the Modify Device Wizard

3 Edit the object properties

Edit any object parameters that you wish to set. In Figure 4-19, the **Modify Device** wizard shows a panel titled **Config Areas**. The **Config Areas** panel of the wizard represents additional pages of parameters available for you to set. Select the **Next** button or select the entry in the **Config Areas** panel to move to another page of parameters. The different wizards have different parameters and differing numbers of additional pages.

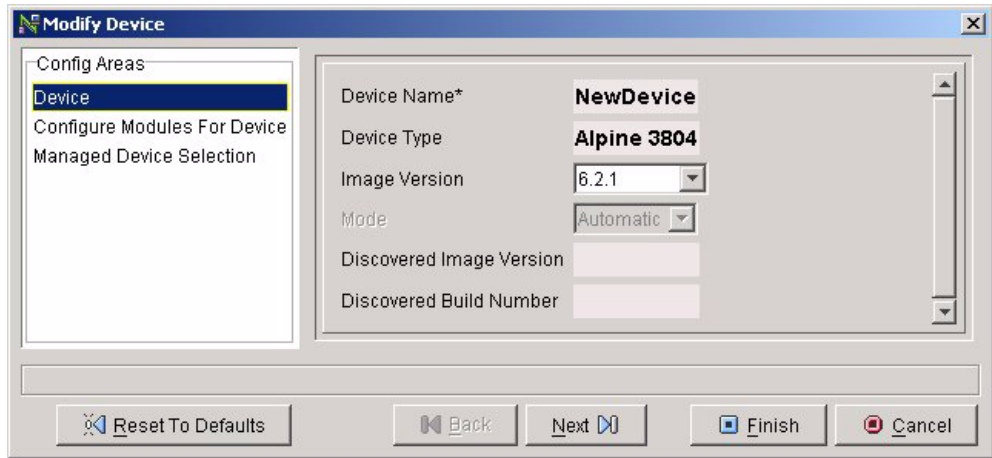


Figure 4-19: Modify Device Wizard

4 Select Finish

When you finish setting parameters for the object, select **Finish**.

Copy a Device or other Object

You can copy an existing device to simplify adding a device to your network. Typically, you will copy a device that has a similar configuration to the configuration you will use for the new device. Once the device has been copied, you can modify it.

Summary steps. The following is a short summary of the steps to copy an existing device.

To copy a device or other object:

- 1 **Select the object to copy**
- 2 **Select Copy**
- 3 **Select the paste location**
- 4 **Select Paste**
- 5 **Enter a device name (or IP address)**
- 6 **Select Finish, or modify the other properties**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To copy a device or other object:

1 Select the object to copy

Open the **Network** panel from the **View** menu if it is not visible. If the object to copy is not visible, open its parent object by clicking its plus sign, and/or scroll until the object is visible. Once the object to copy is visible, select it by clicking it.

2 Select Copy

You can select **Copy** by clicking the copy icon, by selecting the **Edit>Copy** menu item, by right-clicking and selecting **Copy**, or by pressing [CTRL]+C.

3 Select the paste location

For example, if you copy a device, you will paste it into a device folder. Your device will be added to the folder you select when you paste it (see Figure 4-20). If you copy a VLAN, you would paste it into the **VLANs** object, the parent of the VLANs on your device. If you attempt to paste an object to a location that is not applicable for that object, the **Paste** command will be grayed out, and you will not be able to paste until you select an appropriate location. If you attempt to paste an object onto an identical kind of object, you will be notified that you will overwrite the object's parameters. For example, if you paste a VLAN onto another VLAN, you will overwrite the parameters of that VLAN.

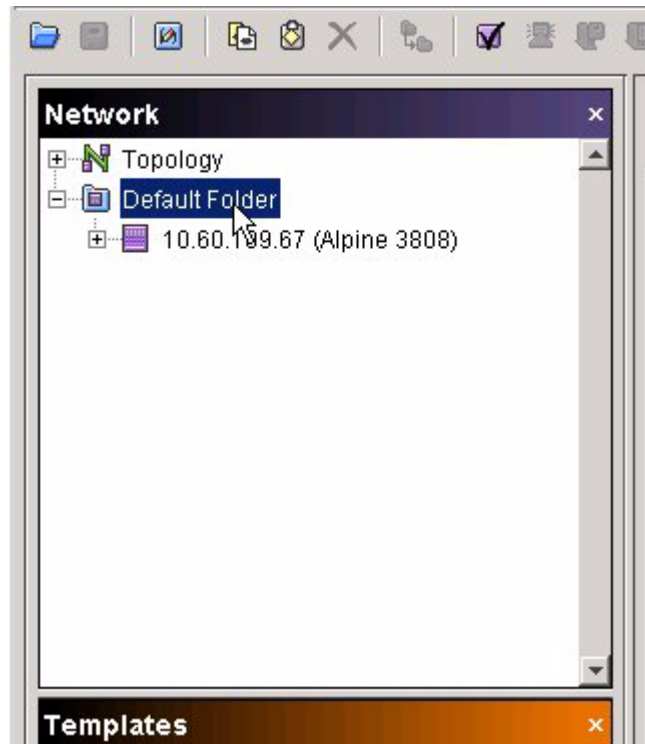


Figure 4-20: Select the Network Device Folder

4 Select Paste

You can select **Paste** by clicking the paste icon, by selecting the **Edit>Paste** menu item, by right-clicking and selecting **Paste**, or by pressing [CTRL]+V (see Figure 4-21). The **Modify Device** wizard will appear.

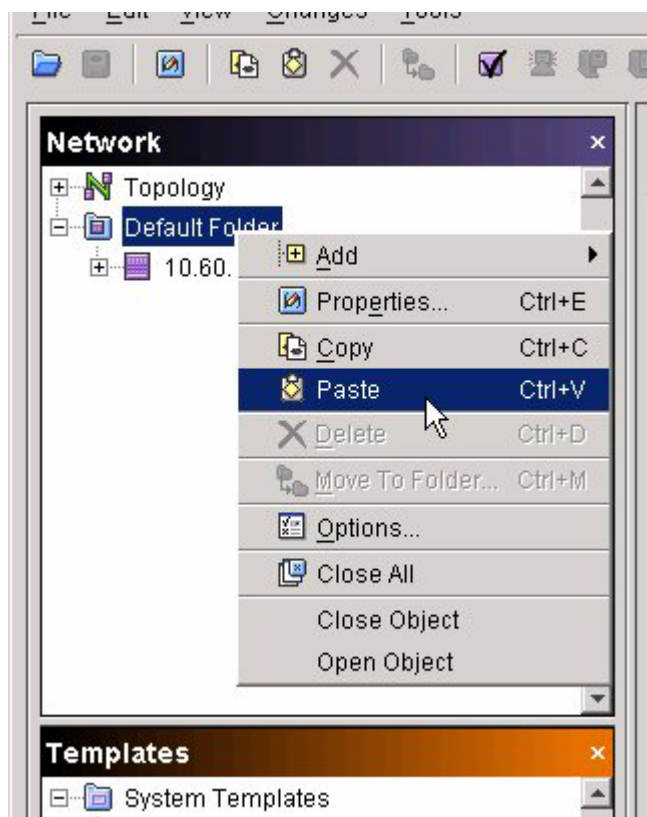


Figure 4-21: Paste the Device

5 Enter a device name (or IP address)

Enter the device name into the **Modify Device** wizard (see Figure 4-22). You must give the device a unique name to identify it for ISM Provision. Use the name or IP address that you plan to use when the device will be deployed, otherwise use a temporary name.

If possible, do not use a temporary name. Since ISM Provision uses the name as a unique key for the device, device names cannot be directly changed. To change the name at a later time you will need to copy the device, paste it back into the Network panel and give it a new name, then delete the original device entry.

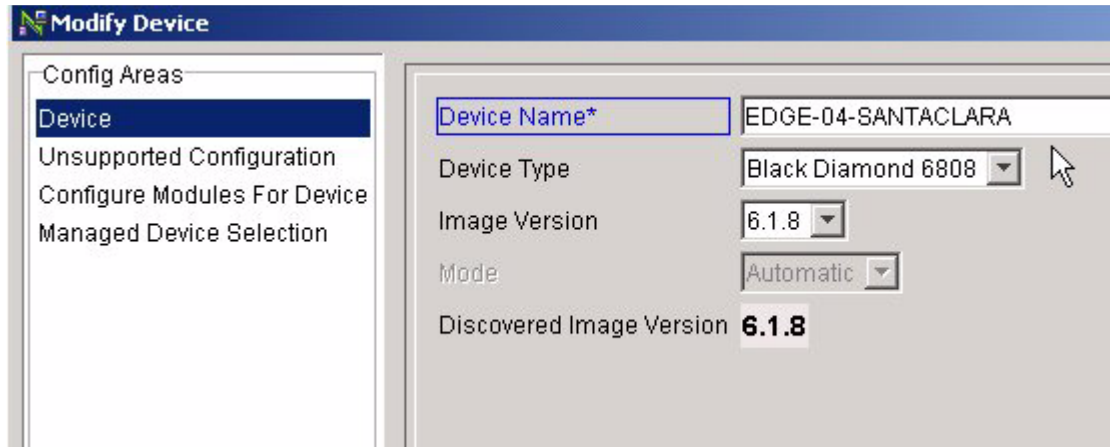


Figure 4-22: Enter Device Name

6 Select Finish, or modify the other properties

Once you have entered the device name, you may modify the other properties of the device now by selecting **Next**, or select **Finish** to copy the device now. All of the properties of the newly copied device, except for the device name, can be modified later.

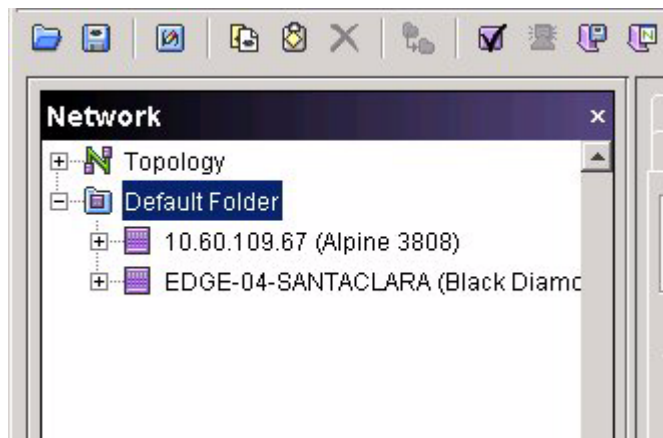


Figure 4-23: Device Added to Network Panel

Save Changes Without Changing Network Configuration

If you have made changes to the configurations displayed in the **Network Provision** view, you can save the changes without changing the configuration on your devices. For example, you would save your changes if you wanted someone to review them before committing them to the network. You would also do this if you have not completed making changes, but want to save them to complete later.

Steps. To save changes without changing network configuration:

1 Select **File>Save Changes...** or **File>Save As Changes...**

If you haven't saved changes yet, you can supply a name for the saved changes. If you have previously saved, the **Save Changes...** item will save the new changes to the previously saved changes. To save to a different name, use **Save As Changes....**

2 Enter a Job Name and Job Description

The time and date are used for the default name.

3 Select Next

The changes are saved, and can be opened at a later time.

4 Select Finish

The changes you have made are still displayed in the **Network Provision** view, so you can continue to work with the changes, saving periodically.

Remove Changes (Revert to Server State)

Changes that have not yet been committed to the ISM Provision server can be removed. If you wish to save the changes for use later, save the changes as described in the task, "Save Changes Without Changing Network Configuration". When you revert the server state, any uncommitted changes are removed from the **Network Provision** view, so this view will correspond to the state of the server.

Steps. To revert to server state:

1 Launch the Revert Changes window

To launch the **Revert Changes** window, select the **Revert** icon, select the **Changes>Revert...** menu item, or press [CTRL]+Z. The **Revert Changes** window will appear and ask, "Do you really want to revert and lose all changes you made to this configuration?". This question is asked regardless of whether you have recently saved your changes.

2 Select Yes

The changes are removed. At this point the **Network** panel of the **Network Provision** view displays the current state of the server.

Change an Unmanaged Device into a Managed Device

You should understand the section “Managed and Unmanaged Devices,” before performing this task. The unmanaged device configuration will be loaded onto the physical device that you specify and overwrite any existing configuration present on the device.

Be sure that the image version and the device type specified in the unmanaged configuration matches that of the device. Also be sure that the configuration that you set on the device will allow the device communicator to remain connected to the device. Since the device communicator uses Telnet to connect to the device and enter the configuration commands, if you unconfigure a necessary route, or remove a critical IP address, you will not be able to continue communicating with the device. The situation is identical to the case of manually connecting to the device with Telnet. If you unconfigure your access, the session will end.

If the physical device already contains an extensive configuration, there may be some errors caused by conflicts between the configuration that is moved to the device and its current configuration. See the last step in this task, “Correct errors (if any), then Commit and Upload”, for information about resolving conflicts.

Summary Steps. To change an unmanaged device into a managed device:

- 1 **Select the device to change**
- 2 **Launch the Modify Device wizard (Edit>Properties)**
- 3 **Select the Managed Device Selection wizard entry**
- 4 **Select Managed Device checkbox**
- 5 **Enter Device Address**
- 6 **Enter Administrator Login and Password**
- 7 **Select Communication Host**
- 8 **Select Finish**
- 9 **Commit changes to ISM Provision server**
- 10 **Correct errors (if any), then Commit and Upload**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To change an unmanaged device into a managed device:

1 Select the device to change

Select the device in the **Network** panel of the **Network Provision** view. You may need to open the device folder containing the device in order to select it. To open the folder, click on the plus sign (+) next to the device folder.

2 Launch the Modify Device wizard (Edit>Properties)

To launch the **Modify Device** wizard, you can either select the menu item **Edit>Properties**, select the **Modify** icon, right-click on the device name and select **Properties** from the drop-down menu, or type [CTRL]+E (see Figure 4-24). The **Modify Device** wizard should appear with the **Device Name** displayed (see Figure 4-25).

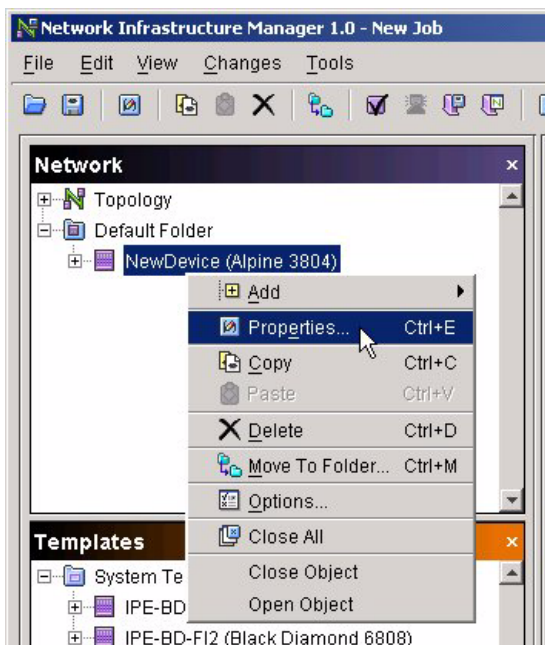
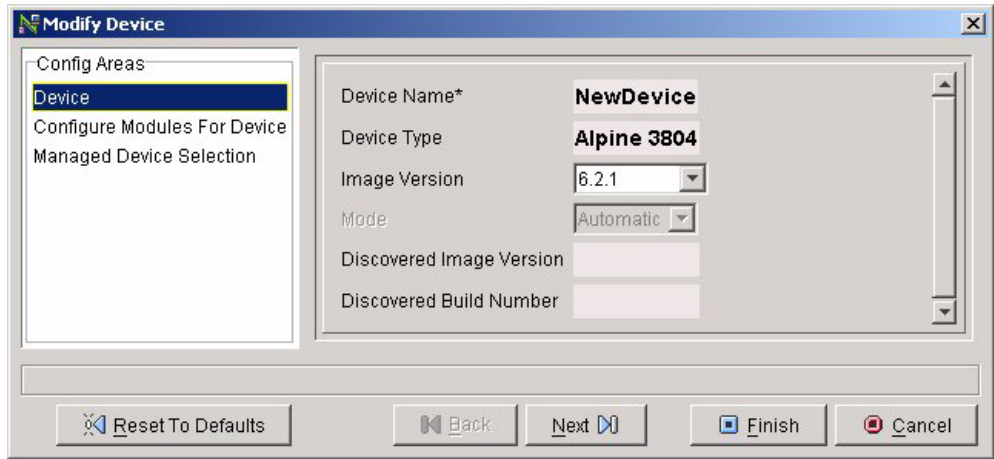


Figure 4-24: Launching the Modify Device Wizard

Figure 4-25: Modify Device Wizard Showing the Entry for NewDevice

3 Select the Managed Device Selection wizard entry



In the left-hand box titled **Config Areas**, select the **Managed Device Selection** entry. You will see the current setting for **Managed Device** is unchecked, and the other fields in the wizard are grayed out (see Figure 4-26).

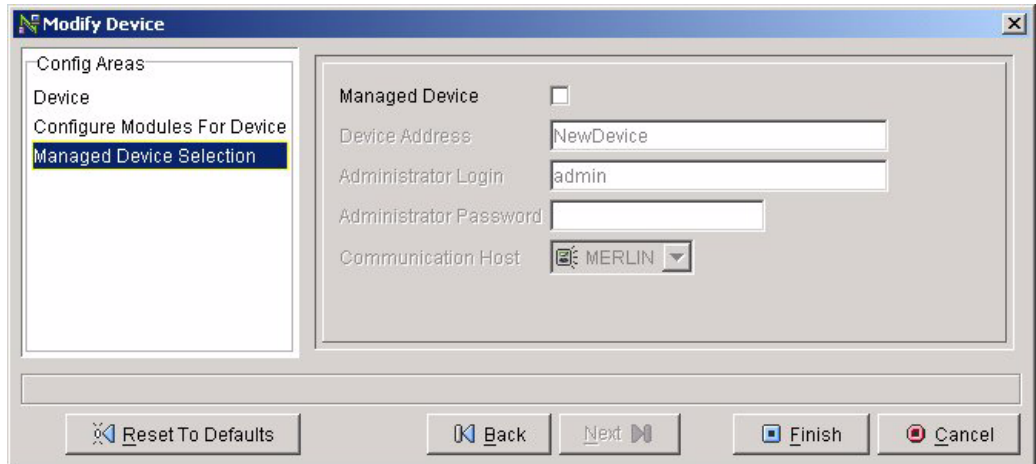


Figure 4-26: Modify Device Wizard for Unmanaged Device

4 Select Managed Device checkbox

Once you have selected the **Managed Device** checkbox, the other fields can be edited (see Figure 4-27).

Figure 4-27: Modify Device Wizard for Managed Device

5 Enter Device Address

The **Device Address** field is used to inform ISM Provision of the IP address for administrative access to the device. This will be an IP address or a name that your network DNS service resolves to an IP address.

6 Enter Administrator Login and Password

Enter the information into the fields.

7 Select Communication Host

From the drop-down list, select the device communicator to manage this device.

8 Select Finish

Select **Finish** to save the information and close the **Modify Device** wizard.

9 Commit changes to ISM Provision server

For details about this step, refer to the task, “View Current Job Changes”, in Chapter 8, “Change Control”. If the commit completes without error, select the **Finish** button to close the **Commit Changes** wizard.

10 Correct errors (if any), then Commit and Upload

Occasionally, as the new configuration commands are sent down to the device, an error will occur. For example, if there is a VLAN named *marketing* already configured on the device and the configuration being sent down also contains a VLAN named *marketing*, the device will report an error when the device communicator tries to create the second *marketing* VLAN. As the error is reported, the device communicator stops sending commands.

If this happens, examine the errors displayed in the **Results** panel of the **Commit Changes** wizard. Fix the errors by going to the **Network Provision** view and modify the device configuration. Once you have made the new changes, commit them to the server.

Finally, you must select the **Upload Devices...** button in the **Network Inventory** view, select the device, and select **Upload**. The changes committed to the server are now moved to the device.



In this special case of encountering an error upon changing an unmanaged device to a managed device, you must use the **Upload Devices...** button to move the configuration to the device. This is opposite to the normal action of the **Upload Devices...** button, normally used to move configuration information from the device to the server.

Access Extreme Devices Directly

When you access Extreme devices directly, you can modify the device configurations manually, either by Telnet or WebVista. This allows you to set configuration options that are not currently supported by ISM Provision. For example, if you load a new version of ExtremeWare onto your device, you can still manage new features by manually adding the commands to the device. Those commands that are not directly supported in your current version of ISM Provision, are contained in the **Unsupported Configuration** panel of the device object. These text versions of configuration commands are still saved and monitored by ISM Provision.

Use Telnet to access a device

You would use your system Telnet application to access the device CLI to manually enter commands.

Steps. To use Telnet to access a device:

1 Select device

Select the device to access in the **Network** panel of the **Network Provision** view of NIM.

2 Select the **Tools>Telnet** menu item

Select **Tools>Telnet** from the menu. This will launch your system Telnet application. (Specify the system Telnet application by selecting **Tools>Options** from the menu,

and then selecting the **Tools Options** tab in the **Options** window. Either type in the system Telnet command, or use the **Browse** button to find the application.)

3 Login to the device using the Telnet application

When the system Telnet application opens, login to the device. You will probably use the same username and password that you specified in NIM for administrative access to this device.

4 Use the CLI to examine or modify the device configuration

Once you access the device, you can issue commands to the CLI. When finished, exit your Telnet application.

Use Extreme WebVista to access a device

You would use Extreme WebVista to manually change the device configuration.

Steps. To use Extreme WebVista to access a device:

1 Select device

Select the device to access in the **Network** panel of the **Network Provision** view of NIM.

2 Select the **Tools>Extreme WebVista** menu item

Select **Tools>Extreme WebVista** from the menu. This will launch your system browser. (Specify the system browser application by selecting **Tools>Options** from the menu, and then selecting the **Tools Options** tab in the **Options** window. Either type in the system browser command, or use the **Browse** button to find the application.)

3 Login to the device

When the system browser opens, login to the device. You will probably use the same username and password that you specified in NIM for administrative access to this device.

4 Use Extreme WebVista to examine or modify the device configuration

Once you access the device, you can examine and modify the configuration. When finished, logoff WebVista.

5

Managing the Network Inventory

Overview

The **Network Inventory** view of NIM lists the managed devices in ISM Provision. Managed devices are the devices that exist in your network and whose configurations are synchronized with the configurations stored in the ISM Provision server. See the section, “Managed and Unmanaged Devices”, in Chapter 4, “Network Provisioning”, for more information.

From the **Network Inventory** view you can add existing devices into the inventory and begin managing them. You can modify the parameters of the devices in the inventory, and delete devices from the inventory, thereby making them into unmanaged devices (their configuration, displayed in the **Network Provision** view, is no longer synchronized with the actual configuration on the device). You can also export and import device inventory information from files.

In many cases, the first thing you will do with ISM Provision is to capture the configuration of your existing network and begin managing it. This group of devices managed by ISM Provision is referred to as the network inventory. Once a device is added to the network inventory, it appears as an entry in the list of managed devices shown in the **Network Inventory** view.

When a device is newly added to the network inventory, ISM Provision queries the device, loads its configuration into the server, and can display the configuration in the **Network Provision** view of NIM. Since the **Network Provision** view allows you to plan and test configuration changes and new device configurations, the devices displayed in the Network Provision view do not necessarily exist in your network. In contrast, the

Network Inventory view displays only those devices currently managed by ISM Provision.

This chapter explains how to perform a number of tasks in the **Network Inventory** view. The first set of tasks allow you to manage which devices make up the network inventory. The second set of tasks allow you to synchronize the ISM Provision server with the devices, and control how the managed configuration is stored on the device. The following tasks are documented in this chapter:

- Manage the Network Inventory List
 - Add a Device to the Network Inventory
 - Modify a Network Inventory Device Listing
 - Delete a Device from the Network Inventory
 - Import Inventory File
 - Export Inventory File
- Manage the Network Inventory Devices
 - Upload Devices
 - Save Running Configurations

Manage the Network Inventory List

Within the **Network Inventory** view, you manage the network inventory (the managed devices of ISM Provision). You can add devices one by one, see the section, “Add a Device to the Network Inventory”, or add a collection of devices by importing an inventory file. You can also save your network inventory by exporting an inventory file. You can also modify the network inventory entry for a device, or remove a device from the network inventory.

Add a Device to the Network Inventory

When you add a device to the network inventory you will specify an IP address or network name to reach the device, and the account and password for access to the device. The ISM Provision server will then use a device communicator to access the device and upload its configuration into the server. As the configuration loads, the device configuration will be added to the ISM Provision server and the device name and status will be displayed in the **Network Inventory** view. Finally, you will be given

an opportunity to synchronize the ISM Provision server with your NIM client and display the device configuration in the **Network Provision** view.

Summary Steps. To add a device to the network inventory:

- 1 Select the Network Inventory view of NIM**
- 2 Select the Add Device button**
- 3 Fill in the Device Name (or IP address)**
- 4 Enter the Administrator Login, and Administrator Password, Device Folder, and Communicator Host**
- 5 Select Finish to close the wizard**
- 6 Choose Update Now, or choose Update Later and later use the Synchronize icon to update**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To add a device to the network inventory:

- 1 Select the Network Inventory view of NIM**

You may either select the **View>Network Inventory** menu, the **Network Inventory** icon at the top right of the NIM screen, the **Network Inventory** icon near the bottom of the screen, or press [ALT]+2 to select the **Network Inventory** view. You will see the screen in Figure 5-1.

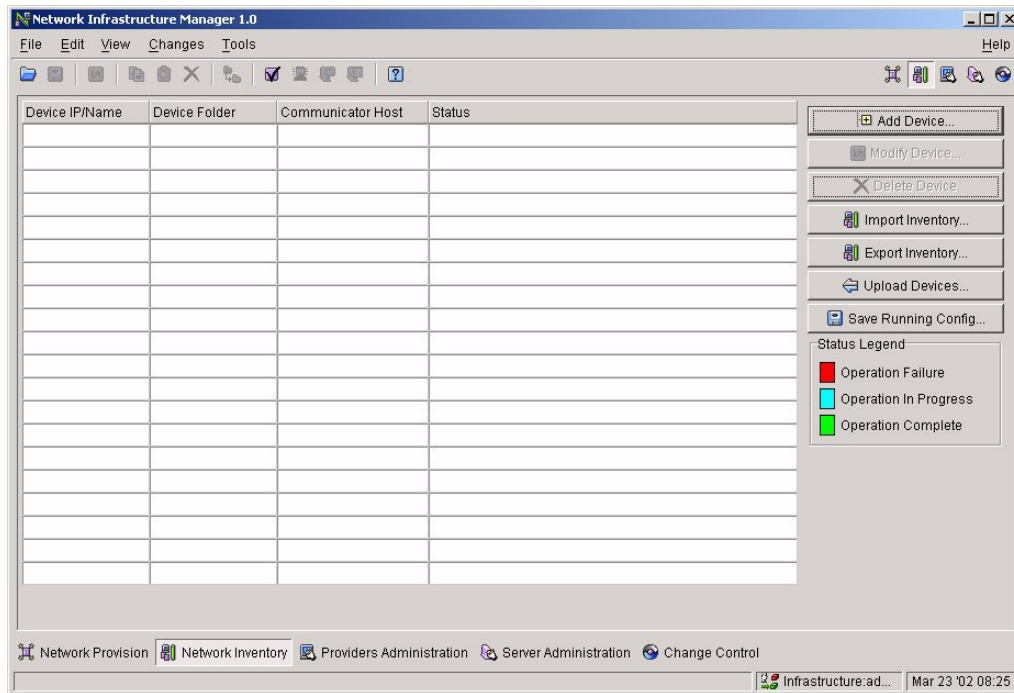


Figure 5-1: Network Inventory View—No Devices

2 Select the Add Device button

From the **Network Inventory** view, select the **Add Device** button, which launches the **Create Device Entry** wizard shown in Figure 5-2.

Figure 5-2: Create Device Entry Wizard

3 Fill in the Device Name (or IP address)

Fill in the first field shown in Figure 5-3.

Figure 5-3: Detail of Add Device Wizard

The first field is the key information for the device. This information cannot be modified once the device is added.

- **Device Name (or IP address).** This field specifies the name or IP address of the network connection that you use for administrative access for the device. Since NIM will be modifying device configurations, you must use administrative access to the device. Use the name of the device as recognized by the DNS service on your network, or use the IP address of the administrative network connection.

4 Enter the Administrator Login, and Administrator Password, Device Folder, and Communicator Host

Fill in the next two fields shown in Figure 5-3.

- **Administrator Login.** Enter the administrative account name used for this device
- **Administrator Password** Enter the password for this account.

The next two pieces of information are selected from drop-down lists. The drop-down lists consist of the following:

- **Device Folder.** NIM starts with one default folder. You may organize your devices into folders of related devices, or put them all into the default folder. Select the folder that the device will be added to.
- **Communicator Host.** Specify the host where the device communicator that will talk to this device is located. An ISM Provision server may have a number of Device Communicators to spread out the processing load, each servicing a number of devices.

5 Select Finish to close the wizard

Once the fields are completed, select **Finish**. NIM will add a device entry to the ISM Provision server, and the device communicator you specified will attempt to connect to the device and download its configuration. The status of the device is reported on the **Network Inventory** page in the status field. The device configuration is read from the device and added to the server, and you are notified that the server configuration has changed.

6 Choose Update Now, or choose Update Later and later use the Synchronize icon to update

Whenever the server configuration changes, NIM is notified, and you are provided an opportunity to synchronize the server configuration with that displayed on the **Network Provision** view (if the notification option is set). You will see the dialog box shown in Figure 5-4, **Server Update Notification**.

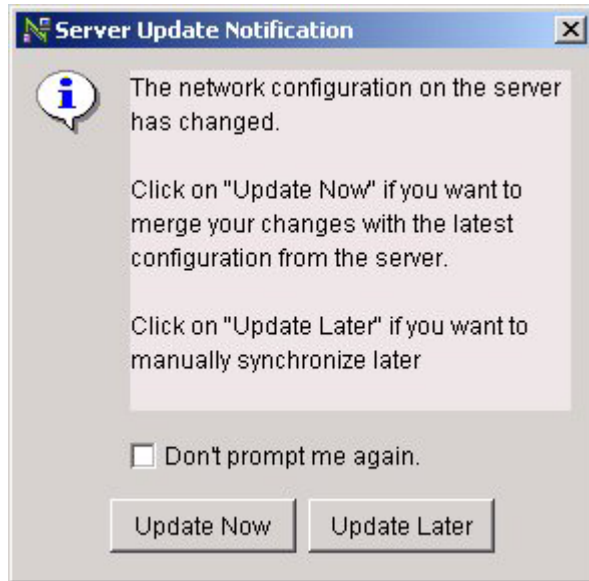


Figure 5-4: Server Update Notification

If you choose **Update Now**, the **Network Provision** view in NIM will update to reflect the new device you have added to the network inventory. If you choose **Update Later**, you will not see this new device in the **Network Provision** view. With either choice, you will see the device and its status displayed in the **Network Inventory** view, as shown in Figure 5-5.

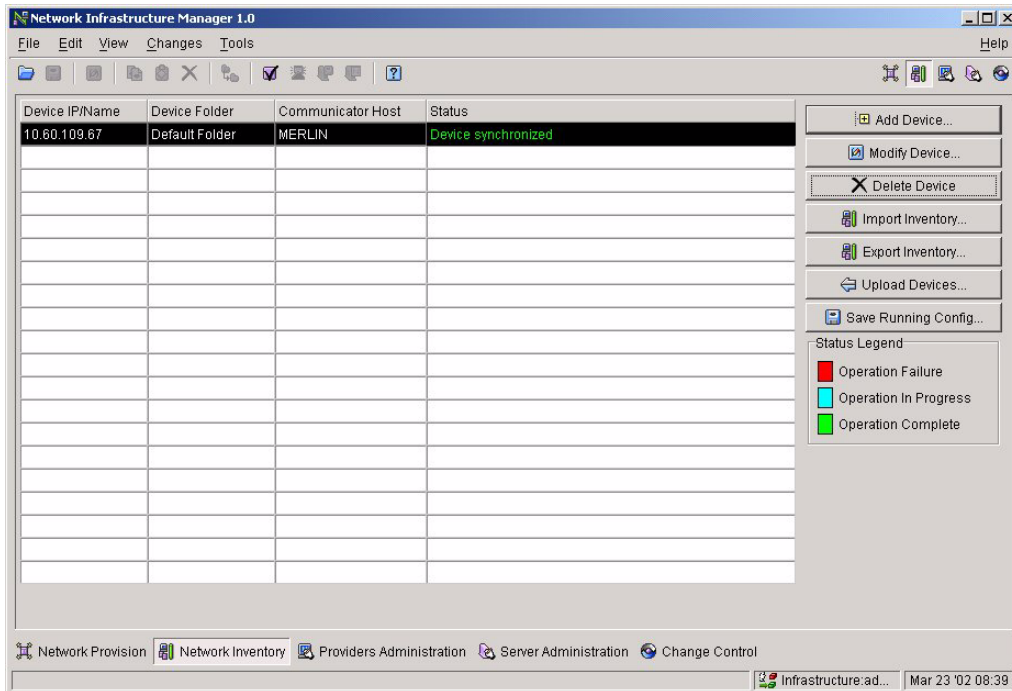


Figure 5-5: New Device Displayed in Network Inventory View

If you choose **Update Later**, use the **Synchronize** icon later, when you update (see “Synchronize” in Chapter 3, “Network Infrastructure Manager Overview”). When you update, a window will inform you of the update progress (Figure 5-6).

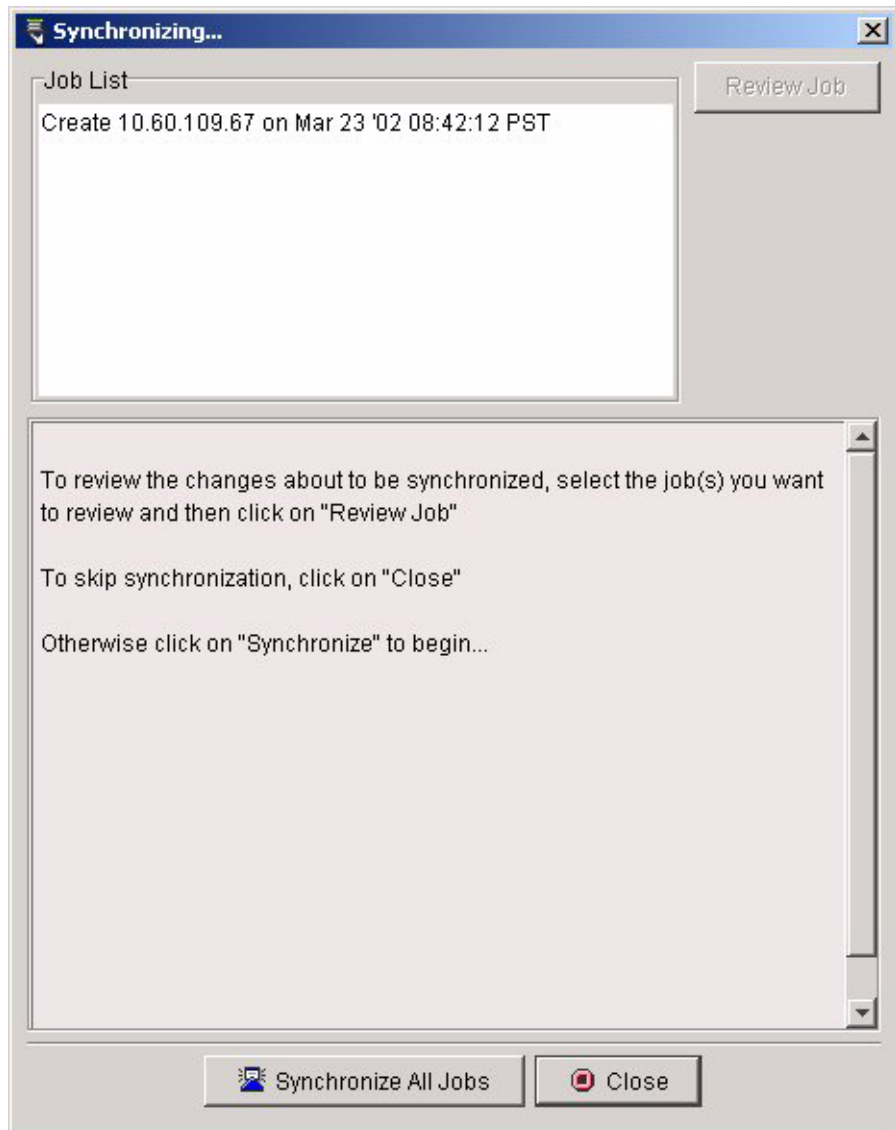


Figure 5-6: Synchronizing the View to the Server

Once the view is synchronized, you will see the new device displayed in the Network Provision view.

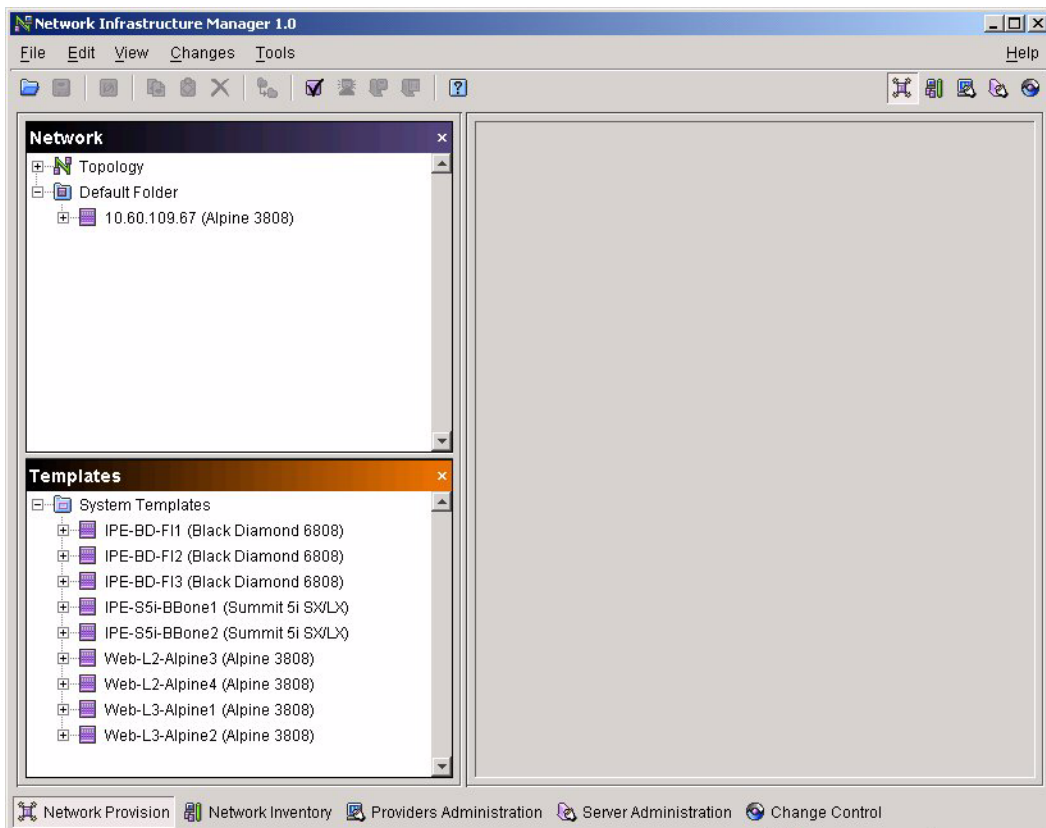


Figure 5-7: New Device Displayed in Network Provision View

Modify a Network Inventory Device Listing

Once a device is in the network inventory, you will typically not modify the device listing. However, if you modify the administrative access account or password, you will need to modify the device listing. Also, for performance reasons, you may wish to install other device communicators in your network or change which communicator manages which device to spread out the processing load in the system. You can modify which device communicator manages a device by modifying the device listing.

Steps. To modify the device listing:

- 1 From the Network Inventory view, select the device listing to modify**
- 2 Select the Modify Device... button to launch the Modify wizard**
- 3 Make changes to the listing**

For details about the fields in this **Modify** wizard, see the step, “Enter the Administrator Login, and Administrator Password, Device Folder, and Communicator Host”, from the task, “Add a Device to the Network Inventory”.

- 4 Select Finish**

Delete a Device from the Network Inventory

Deleting a device from the network inventory does not remove the device from ISM Provision. When you delete a device from the network inventory, you are unmanaging the device. ISM Provision stops synchronizing the device and the device configuration stored in the ISM Provision server. If you delete a device from the network inventory, you will still see the device in the **Network Provision** view of NIM. See the section, “Managed and Unmanaged Devices”, in Chapter 4, “Network Provisioning”, for more information about managed and unmanaged devices.

Steps. To delete a device from the network inventory:

- 1 From the Network Inventory view, select the device to delete**
- 2 Select the Delete Device button**

When you select the Delete Device button, a window appears and asks, “Are you sure you want to delete...”

- 3 Select Delete**

Import Inventory File

An inventory file contains information about a list of devices. The information is similar to that which you specify when performing the task, “Add a Device to the Network Inventory”. The inventory file contains: the device name, IP address, administrator account, and administrator password. This file contains only the information necessary to manage a device, and not configuration information.

If you have a large number of existing devices, it may be more efficient to create an inventory file containing this information for your network, rather than adding the devices individually. The recommended way to create an inventory file is to add two

devices to the network inventory, export an inventory file, and use a text editor to add entries to the file.

Summary Steps. To import an inventory file:

- 1 Launch the Import Inventory wizard**
- 2 Specify the file to import**
- 3 Select the folder to place the devices**
- 4 Select the devices to import**
- 5 Select Import**
- 6 Select Close**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To import an inventory file:

- 1 Launch the Import Inventory wizard**

Select the **Import Inventory...** button in **Network Inventory** view, or select **File>Import>Inventory...** from the menu. The **Import Inventory** wizard will appear (see Figure 5-8).

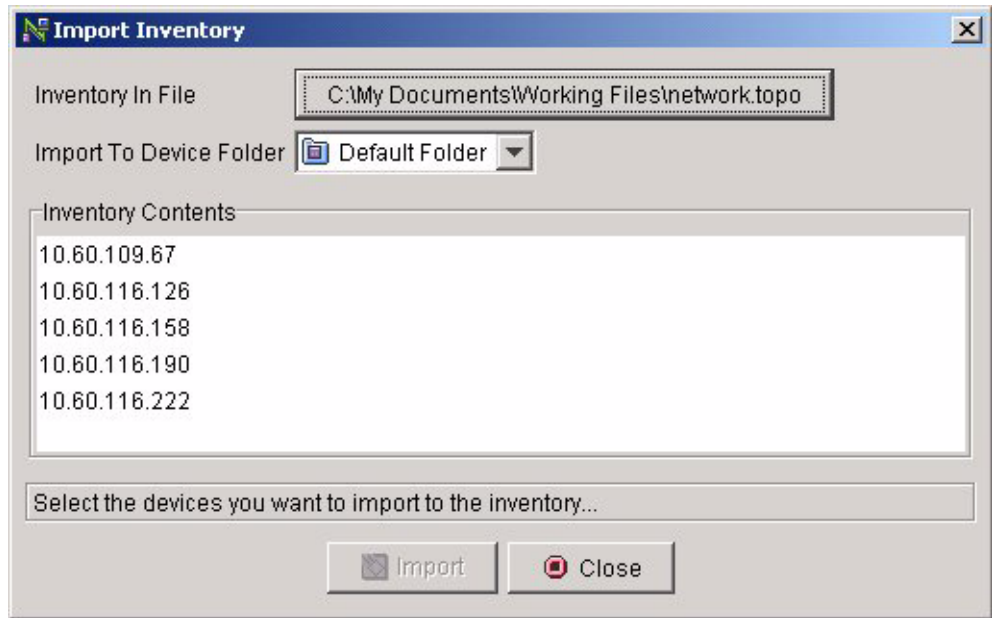


Figure 5-8: Import Inventory Wizard

2 Specify the file to import

The **Inventory In File** button on the **Import Inventory** wizard is labeled with the currently selected inventory file, or if no file has been selected, the button will be labeled **Choose....** To change the import file, select this button, and a **Select Inventory File** wizard will appear (see Figure 5-9).

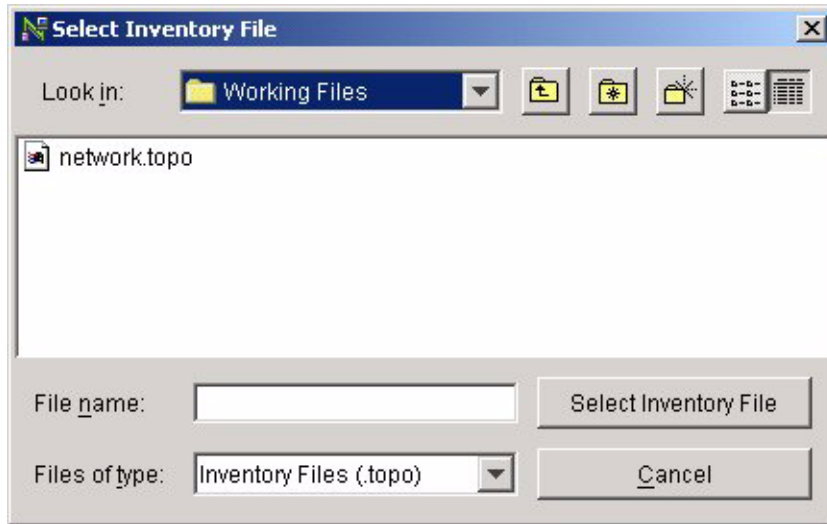


Figure 5-9: Select Inventory File

Select the file name from the file listing by clicking it or type it into the **File name** field, then select the button labeled **Select Inventory File** to return to the **Import Inventory** wizard.

3 Select the folder to place the devices

Use the **Import To Device Folder** drop-down list to select the device folder (see Figure 5-8).

4 Select the devices to import

The devices contained in the currently selected inventory file are listed in the **Inventory Contents** panel. Select which device you want to import, clicking on an individual device, or use the multiple select of your window manager (commonly [SHIFT]-click to select the whole list, [CTRL]-click to add items to a list).

5 Select Import

Select **Import** to add the devices to the inventory.

6 Select Close

You may wish to select other devices and import them into another folder, so the **Import Inventory** wizard will remain open until you select **Close**.

Export Inventory File

You would export an inventory file to save the administrative access information for devices managed by ISM Provision.

To export an inventory file:

1 Launch the Export Inventory wizard

Select the **Export Inventory...** button in **Network Inventory** view, or select **File>Export>Inventory...** from the menu. The **Export Inventory** wizard will appear

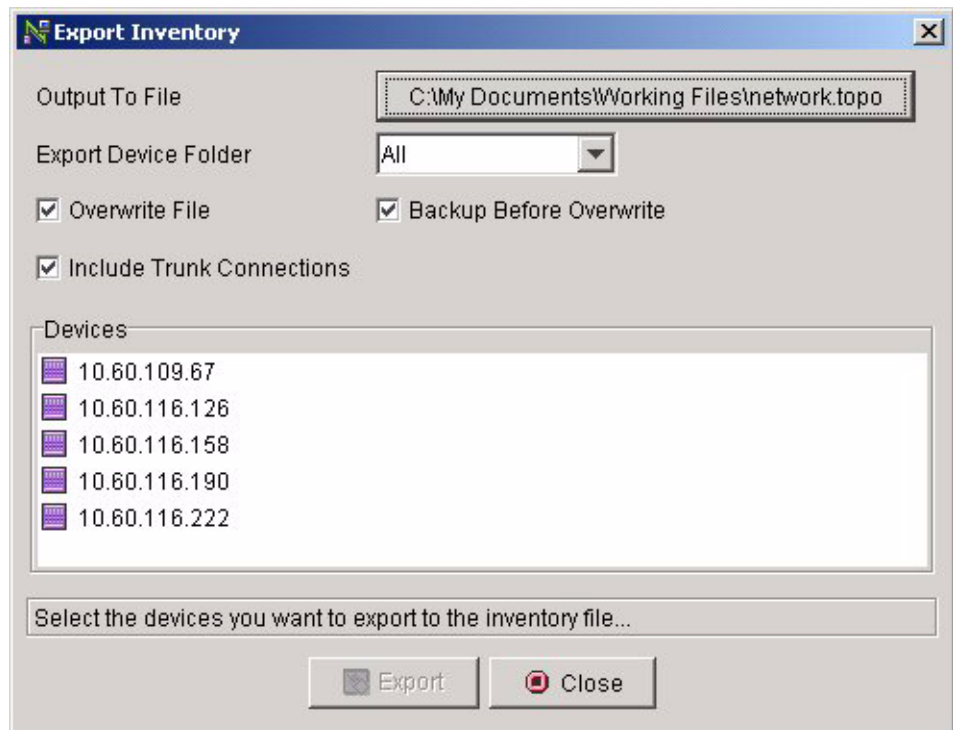


Figure 5-10: Export Inventory Wizard

2 Specify the output file

The **Output To File** button on the **Export Inventory** wizard is labeled with the currently selected inventory file, or if no file has been selected, the button will be labeled **Choose...** To change the export file, select this button, and a **Select Inventory File** wizard will appear (see Figure 5-9). The default extension for

inventory (and topology) files is “.topo”. If you do not specify an extension, the default will be appended to your file name.

3 Specify the folder that contains the devices to export

Use the **Export Device Folder** drop-down list to display the devices from a single folder, or select **All** to display all the devices. The **Devices** panel will display the devices to select from.

4 Specify the export options

Select the options for saving the file. If you select **Overwrite**, the save will overwrite an identically named file, if any, in that directory. **Backup Before Overwrite** will append the extension “.bak” to an existing, identically named file. **Include Trunk Connections** will also export the connection topology information to the file.

5 Select the devices to export

The devices contained in the currently selected device folder are listed in the **Devices** panel. Select which device you want to export, clicking on an individual device, or use the multiple select of your window manager (commonly [SHIFT]-click to select the whole list, [CTRL]-click to add items to a list).

6 Select Export

Select **Export** to export the devices to the file.

7 Select Close

You may wish to select other devices and export them into another file, so the **Export Inventory** wizard will remain open until you select **Close**.

Manage the Network Inventory Devices

From the **Network Inventory** view of NIM you can perform two device management tasks, upload the device configurations to the ISM Provision server, and save the currently running device configurations to the device's NVRAM.

Upload Devices

When you upload a device, the device communicator connects to the device, examines its configuration, and updates the ISM Provision server if there are any changes. By default, the device communicator performs an upload every 60 minutes. The automatic update is controlled in the **Server Administration** view on the **Communicators** panel.

See the task, “Modify a Device Communicator”, in Chapter 7, “Managing the ISM Provision Server”, for details on setting the automatic upload parameters.

The **Upload Devices...** button allows you to manually upload the device configuration from the device at any time. You might do this to synchronize the device with the ISM Provision server if you have directly accessed the device and made configuration changes.

For one special case, the **Upload Devices...** button actually moves the configuration from the server to the device. See the task, “Change an Unmanaged Device into a Managed Device”, in Chapter 4, “Network Provisioning”.

To upload the device configuration to the server:

1 Select the Upload Devices... button

From the **Network Inventory** view, select the **Upload Devices...** button. The **Upload Devices...** wizard will appear.



Figure 5-11: Upload Devices... Wizard

2 Select the device folder

You can display the devices from a single folder, or choose **All Device Folders** from the drop-down list to display all devices.

3 Select the devices to upload

Select which device you want to upload, clicking on an individual device, or use the multiple select of your window manager (commonly [SHIFT]-click to select the whole list, [CTRL]-click to add items to a list).

4 Select Upload

The wizard will close and the selected devices' device communicators begin the process of uploading the configurations to the server.

Save Running Configurations

Any changes to a device's configuration will be lost if the power is interrupted, or the device reboots, unless the configuration is saved to non-volatile RAM (NVRAM). When you commit changes to the server, you are given an opportunity to save changes to NVRAM, but you can manually save device configurations to NVRAM at any time from the **Network Inventory** view. Most devices can save two different configuration in NVRAM, called primary and secondary. You can select which configuration is selected upon reboot by modifying the **Management Access** object in the **Network Provision** view.

Steps. To save the running configurations

1 Select the Save Running Config... button

The **Save Running Configuration** wizard appears (see Figure 5-12).

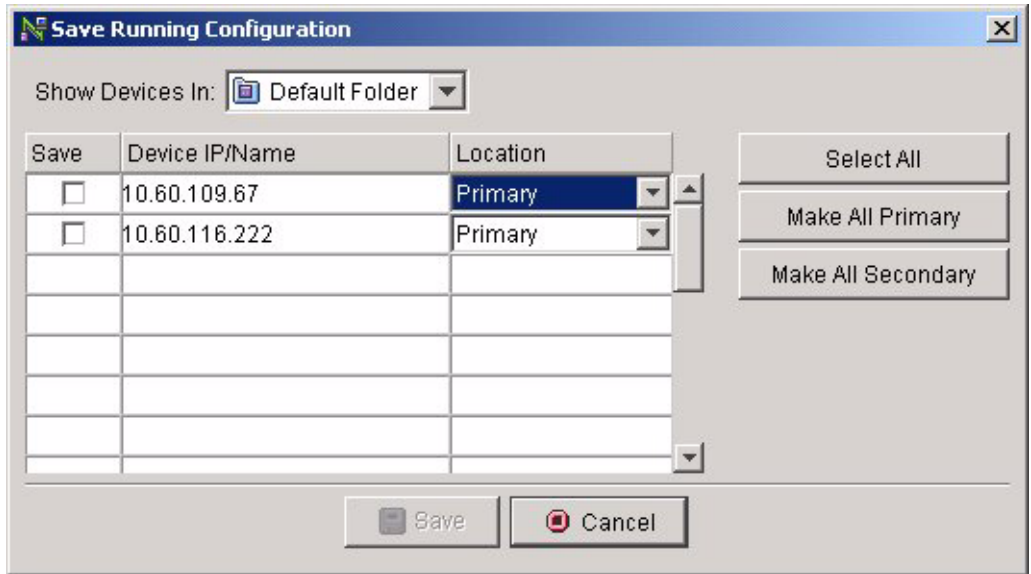


Figure 5-12: Save Running Configuration Wizard

2 Select the device folder

You can display the devices from a single folder, or choose **All Device Folders** from the drop-down list to display all devices.

3 Select the devices and locations

Click to select individual devices or the **Select All** button for all the devices. Use the drop-down list to select the save location (primary or secondary) or use the buttons **Make All Primary** or **Make All Secondary**.

4 Select Save

The wizard disappears and the configuration is saved to NVRAM.



6 Managing Providers

Overview

The **Providers Administration** view in Network Infrastructure Manager allows you to control access to devices, ports, and other resources managed by ISM Provision. You create a provider, add accounts to that provider, decide which ports of which devices they will have access to, and define pools of VLAN tags and IP addresses that they are allowed to use. By creating providers and controlling access, your providers can manage the services to their customers without disrupting the network or each other. The providers you create will access ISM Provision using the IP Service Manager client (IPSM) that will simplify the process of enabling services for their customers. Instead of manually changing the configuration of a device or group of devices, they will be able to add a service to a customer and ISM Provision will take care of the details of making the configuration changes.

This chapter explains the following concepts about managing providers:

- The Infrastructure Provider
- Device Access

This chapter also explains how to perform a number of tasks in the **Providers Administration** view:

- Managing Providers
 - Create a Provider and Provider Accounts
 - Limit Provider Device Access

The Infrastructure Provider

The infrastructure provider entry is a special one. This provider entry is used to manage the user accounts for NIM, controlling access to the ISM Provision server from the NIM client. For this reason, the infrastructure provider cannot be deleted. When you login to NIM, there is a read-only entry of “infrastructure” for the **Provider** field in the login screen.

Device Access

When a provider is created, all of the devices, ports, VLAN tags, and IP addresses currently available in ISM Provision are available to that provider.

When a provider account user in the IP Service Manager client creates a subscriber in IPSM, that user actually creates a VLAN in the device configuration. Creating an IP aggregation point creates a super-VLAN. Creating a service bundle creates a Qos profile and creating a policy based service creates an access list.

You may wish to limit provider access to particular devices, ports, VLAN tags, and IP addresses. If there are no devices displayed for the provider, that provider has access to all devices. However, once you specify access to a device, the provider now only has access to the resources that you have specified. When the IPSM client is in use by one of the provider’s accounts, only the specified resources are available. If a user tries to create subscribers that use ports, VLAN tags, or IP addresses outside of the allowable range, an error will be generated during the verification step, and the subscriber will not be created until the error is corrected.

Managing Providers

To add a provider to ISM Provision, you will create the provider and any additional accounts in the **Providers Administration** view in NIM. To make the provider and accounts available, you must commit these changes to the ISM Provision server.

Create a Provider and Provider Accounts

To create the provider and provider accounts, use the **Providers Administration** view in NIM. From here you can launch the **Create Provider** wizard.

Summary Steps. To create a provider and provider accounts:

- 1 **Launch the Create Provider wizard**
- 2 **Enter the provider name**
- 3 **Select Next**
- 4 **Launch the Create Provider Account wizard**
- 5 **Enter the account login and password**
- 6 **Select Finish when done**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To create a provider and provider accounts:

- 1 **Launch the Create Provider wizard**

To launch the wizard, choose **Edit>Add>Provider** from the menu bar. You can also right-click in the **Providers** pane of **Providers Administration** view, and select **Add>Provider**.



Figure 6-1: Launching the Create Provider Wizard

- 2 **Enter the provider name**

Once the wizard appears, enter the name of the provider you will add.

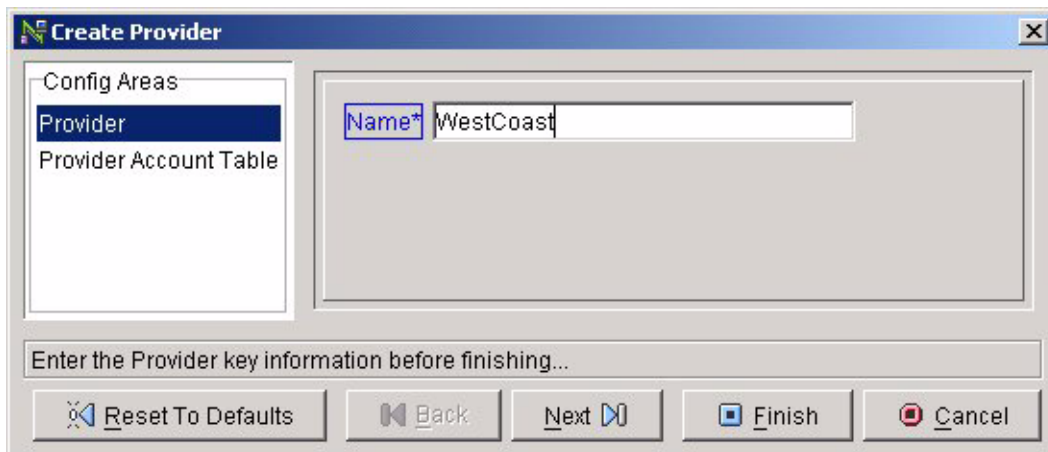


Figure 6-2: Creating a Provider

3 Select Next

Now add user accounts to your provider; select the **Next** button to go to the **Provider Account Table** page. When the **Provider Account Table** appears, you will notice that a default account with username **admin** and no password have been created. To create other accounts, select the plus sign (+) in the **Options** box to add a new provider user account (see Figure 6-3).

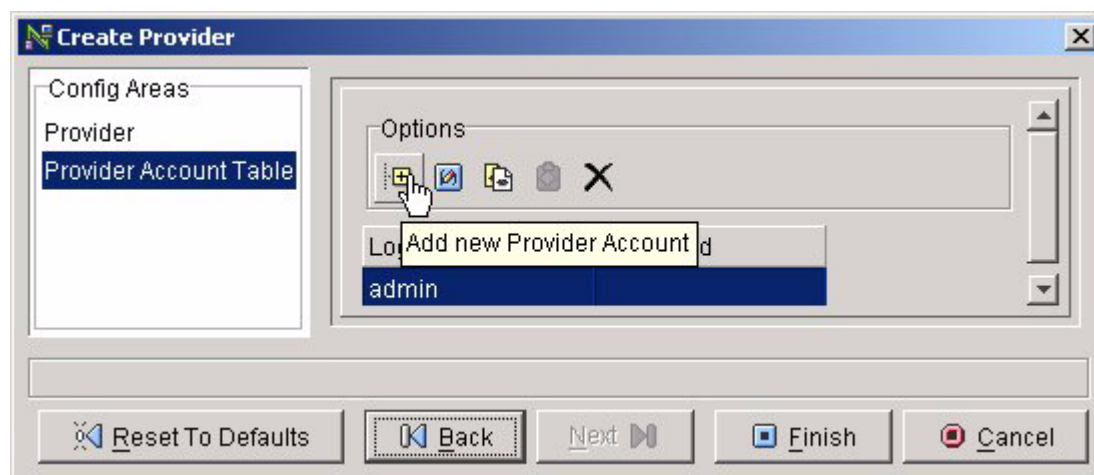


Figure 6-3: Adding a New Provider Account

4 Launch the Create Provider Account wizard

Once you have selected the icon to add a new provider account, the **Create Provider Account** wizard appears (Figure 6-4).

Figure 6-4: Create Provider Account Wizard

5 Enter the account login and password

Enter the account **Login** and **Password**, then select **Finish**. Continue adding accounts for the provider by selecting the plus sign (+) in the **Provider Account Table** page of the **Create Provider** wizard (Figure 6-3). When you have added the accounts for your provider, select the **Finish** button from the **Create Provider** wizard.

6 Select Finish when done

The wizard exits and you will see the new provider you created displayed in the **Providers Administration** view of NIM. You may create other providers at this time, by launching the **Create Provider** wizard again (Figure 6-1).

Limit Provider Device Access

In the **Providers Administration** view of NIM you can control provider access to network resources. You can limit access to devices, to particular ports, to VLAN tags, and to IP addresses. See the section, “Device Access”, for more details.

Summary Steps. To limit provider device access:

- 1 Select the provider
- 2 Launch the Create Provider Device Access wizard
- 3 Select device and ports
- 4 Add, modify, and delete VLAN tag pools and loopback VLAN tag pools
- 5 Add IP ranges
- 6 Select Finish

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To limit provider device access:

- 1 Select the provider
- 2 Launch the Create Provider Device Access wizard

Select the **Edit>Add>Provider Device Access** menu item, or right-click on the provider and select **Add>Provider Device Access** from the pop-up menu. The **Create Provider Device Access** wizard appears (see Figure 6-5).

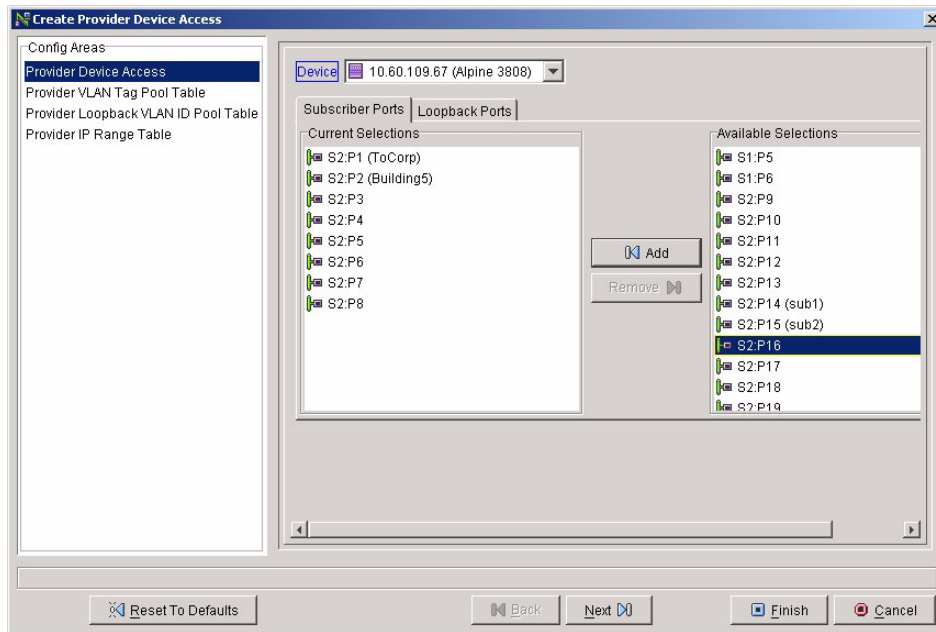


Figure 6-5: Create Provider Device Access Wizard

3 Select device and ports

Select the device from the drop-down list. Select the **Subscriber Ports** from the **Available Selections** panel. Select the desired ports, clicking on an individual port, or use the multiple select of your window manager (commonly [SHIFT]-click to select the whole list, [CTRL]-click to add items to a list). Once you have selected the ports, select the **Add** button to add them to the **Current Selections** panel. Repeat the process for the **Loopback Ports**. Select the **Loopback Ports** tab, select the desired ports from the **Available Selections** panel, then select **Add** to move them to the **Current Selections** panel. Select **Next** to move to the next page of the wizard

4 Add, modify, and delete VLAN tag pools and loopback VLAN tag pools

If you wish to restrict which VLAN tags can be used, specify the start and end of the pool. You can add more than one pool to choose from, and modify the default pool. Select **Next** to move to the loopback page, then specify the pools for loopback tags. Select **Next** to move to the last page.

5 Add IP ranges

If necessary, specify allowable IP ranges.

6 Select Finish

Select **Finish** when you have completed specifying the provider device access parameters.



Managing the ISM Provision Server

Overview

The **Server Administration** view of NIM allows you to view and control the ISM Provision server and device communicators. The **Server Administration** view is divided into three tabs, the **Communicators** tab, the **Logs** tab, and the **Control** tab.

This chapter explains the functions of the **Server Administration** view tabs:

- Communicators Tab
- Logs Tab
- Control Tab

This chapter also explains how to perform a number of tasks in the **Server Administration** view. The first set of tasks are for managing the device communicators:

- Manage Device Communicators
 - Add a Device Communicator
 - Modify a Device Communicator
 - Delete a Device Communicator
 - View Device Communicator Logs

The next set of tasks are for managing the ISM Provision server:

- Manage ISM Provision Server

- View Other Connected Users
- Send Broadcast Message
- Stop Server
- View Server Log

Communicators Tab

The **Communicators** tab allows you to manage the parameters of the device communicators in your system. You can add new device communicator entry to the ISM Provision server, so that the server will allow that communicator to connect. You can also modify the communicator parameters; whether the communicator automatically synchronizes with managed devices, how frequently to synchronize, and how long to wait for a Telnet session (see Figure 7-1).

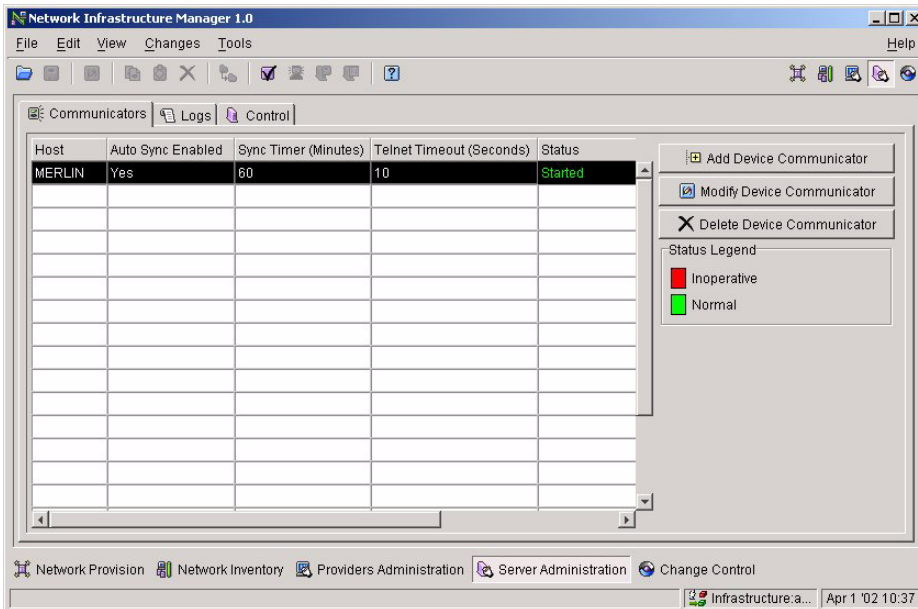


Figure 7-1: Communicators Tab of Server Administration View

Logs Tab

The **Logs** tab allows you to examine the server and device communicator logs (see Figure 7-2).

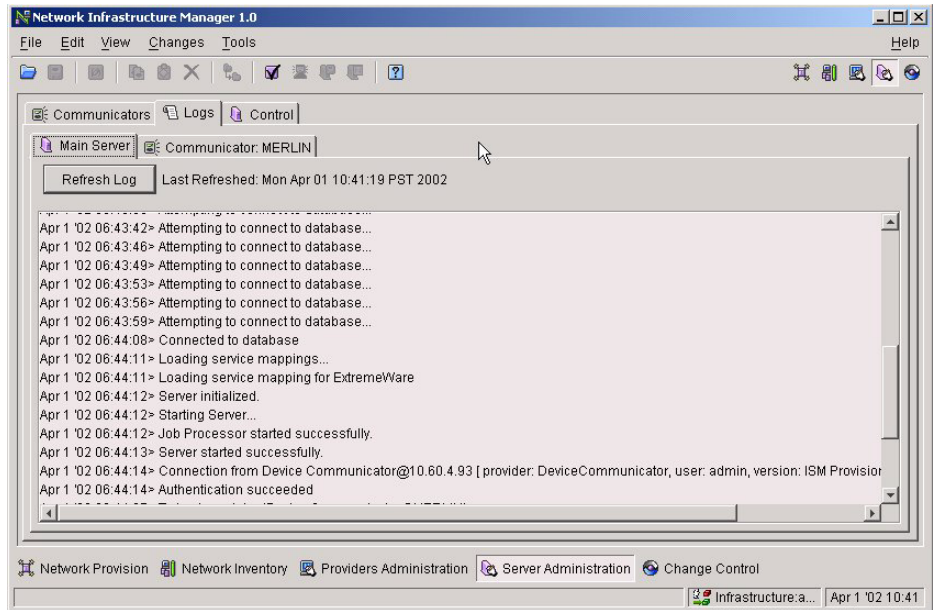


Figure 7-2: Logs Tab of Server Administration View

Control Tab

The **Control** tab allows you to view which other users are connected to the server, to send a broadcast message to those users, and to stop the server.

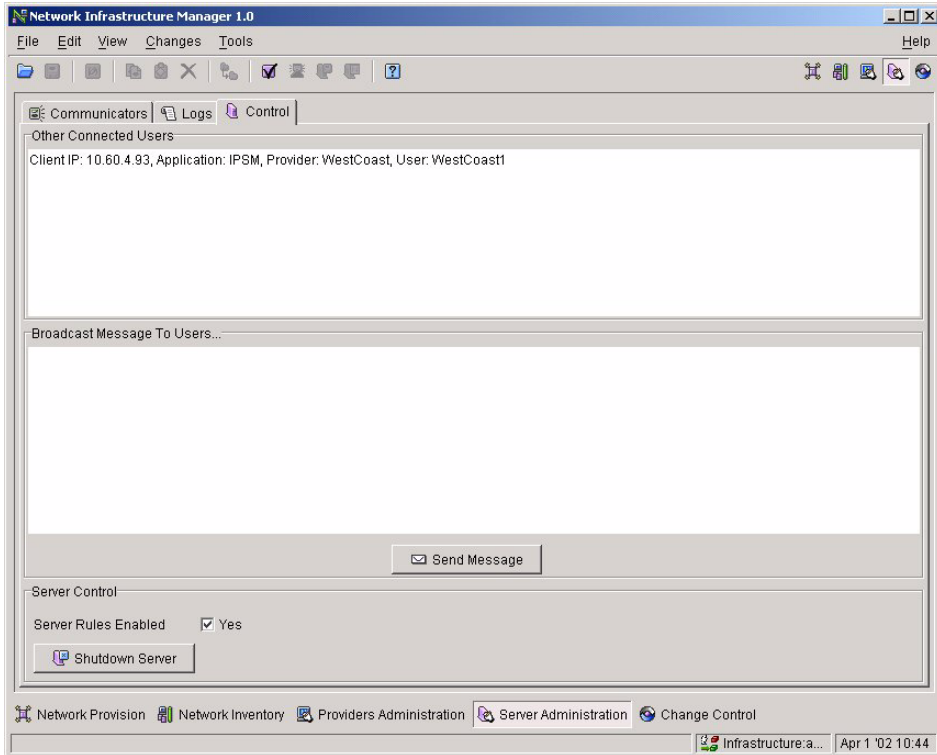


Figure 7-3: Control Tab of Server Administration View

Manage Device Communicators

The following tasks manage the device communicators in your ISM Provision system, and are performed from the **Communicators** tab of the **Server Administration** view of NIM:

- Add a Device Communicator
- Modify a Device Communicator

- Delete a Device Communicator
- View Device Communicator Logs

Add a Device Communicator

From the **Communicators** tab in the **Server Administration** view you can add a device communicator. This task allows an already installed device communicator to connect with the ISM Provision server and begin to manage devices.

This task assumes that the device communicator has already been installed and that you can start the communicator at the end of this task. For information about installing and starting a device communicator, see the document, *ISM Provision Installation Guide*, available as a PDF file, “install-1-0.pdf” on your ISM Provision CDROM.

Steps. To add a device communicator

1 Select Add Device Communicator button

Choose the **Communicators** tab in the **Server Administration** view in order to see the **Add Device Communicator** button.

2 Enter hostname and synchronization parameters

The device communicator should already be installed on the hostname you specify.

3 Select Finish

4 Start device communicator

Frequently, the device communicator will exit if it does not connect with the server you specified when you installed it. Start the device communicator again once you have added its entry to the server. See the *ISM Provision Installation Guide* for instructions on starting a device communicator

Modify a Device Communicator

You would modify a device communicator if you wanted to disable automatic synchronization, or if you wanted to modify the synchronization interval. You can also modify the Telnet time out setting for the communicator.

Steps. To modify a device communicator:

1 Select Modify Device Communicator button

Choose the **Communicators** tab in the **Server Administration** view in order to see the **Modify Device Communicator** button.

2 Enter new values for Auto-Synch Enabled, Synch Timer, and Telnet Timeout

3 Select Finish

The changes take effect immediately. They do not have to be committed to the server.

Delete a Device Communicator

When you delete a device communicator, you actually delete its connection to the ISM Provision server. The communicator is not removed from its host, but it will exit as it loses its connection. Any devices managed by the device communicator will become unmanaged devices. If you would rather manage these devices with another device communicator, see the task, “Modify a Network Inventory Device Listing”, in Chapter 5, “Managing the Network Inventory”. For more information about managed devices, see the section, “Managed and Unmanaged Devices” in Chapter 4, “Network Provisioning”, for more information.

Steps. To delete a device communicator:

1 Select Delete Device Communicator button

The **Delete** wizard will appear, naming the host for the device communicator. It will list the devices managed by the communicator that you plan to delete, and tell you that their network inventory listings will be removed (see Figure 7-4).



Figure 7-4: Delete Device Communicator Wizard

2 Select Delete

The device communicator entry is immediately removed from the server, and the devices become unmanaged devices.

View Device Communicator Logs

You can view the device communicator logs from the **Logs** tab of the **Server Administration** view. You can filter the log to show messages from all devices or from a single device.

Steps. To view a device communicator log:

1 Select the Communicator:HOST tab for the device communicator

For each device communicator there is an individual **Communicator:HOST** tab on the **Logs** tab, where **HOST** is the hostname for the device communicator.

2 Select which device to filter

Choose from the drop-down list, **Filter On Device**, to display one or all devices.

3 Refresh, then view log

Manage ISM Provision Server

The following tasks manage the device communicators in your ISM Provision system, and are performed from the **Communicators** tab of the **Server Administration** view of NIM:

- View Other Connected Users
- Send Broadcast Message
- Stop Server
- View Server Log

View Other Connected Users

Select the **Control** tab of the **Server Administration** view to see all the other users connected to the server (see Figure 7-5).

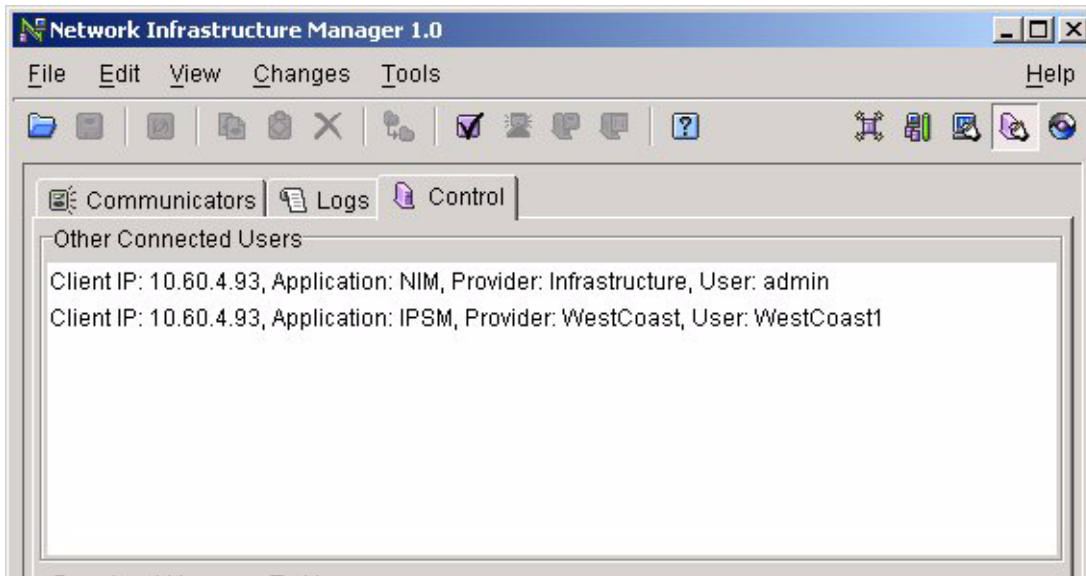


Figure 7-5: Other Connected Users

The **Other Connected Users** panel lists the IP address, the application, the provider, and the provider user account for all the other client connections to the ISM Provision server.

Send Broadcast Message

From the **Control** tab in the **Server Administration** view, you can send a text message to all the clients connected to the ISM Provision server. You may want to do this if you plan on stopping the server, or if you plan to do a configuration rollback.

Summary Steps. To send a broadcast message:

- 1 Type the message into the **Broadcast Message to Users...** panel
- 2 Select the **Send Message** button

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To send a broadcast message:

- 1 **Type the message into the Broadcast Message to Users... panel**

From the **Control** tab in the **Server Administration** view, type the message into the panel (see Figure 7-6).

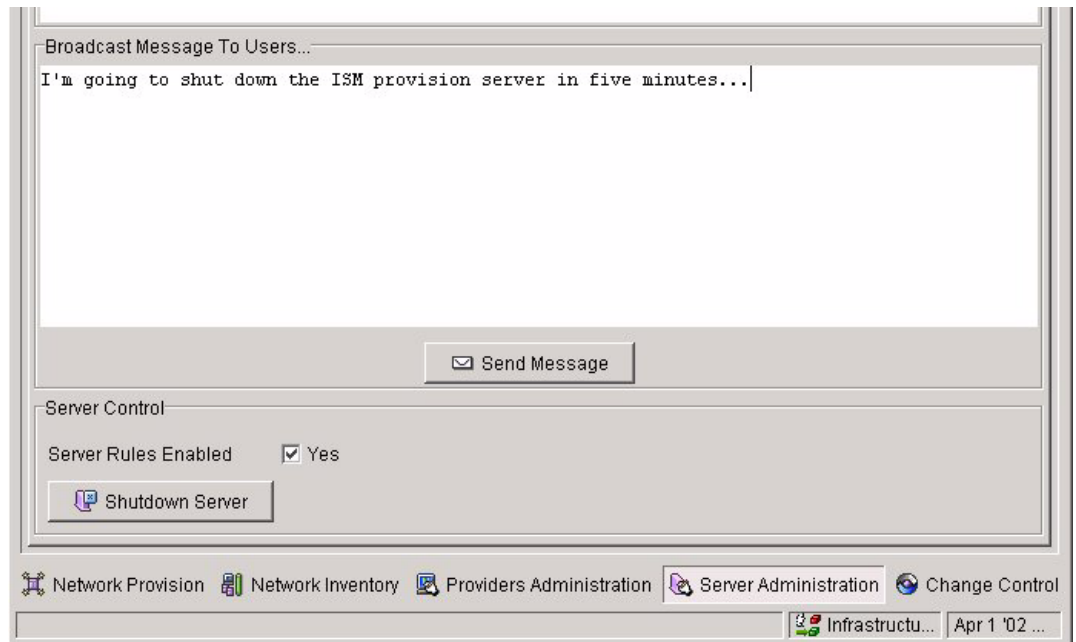


Figure 7-6: Broadcast Message Panel

2 Select the Send Message button

Once the **Send Message** button is selected, the message is sent to all the connected clients. They will see a copy of the message similar to Figure 7-7.

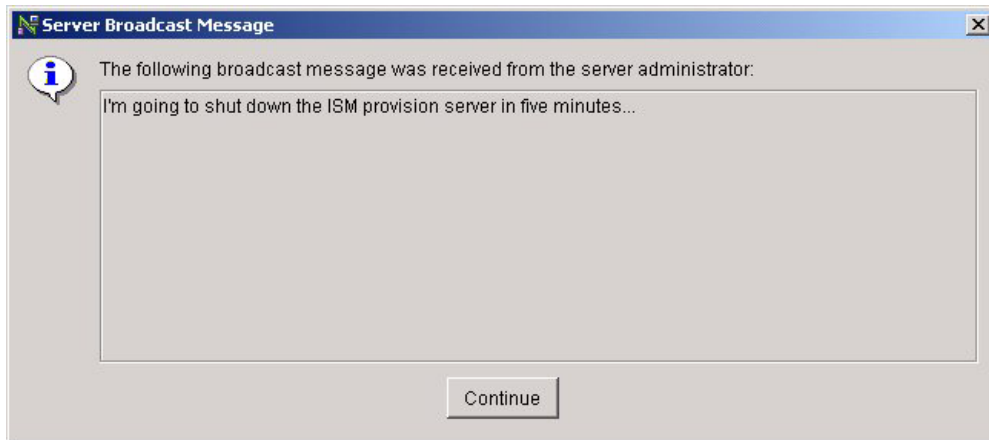


Figure 7-7: Server Broadcast Message

Stop Server

From the **Control** tab in the **Server Administration** view, you can stop the ISM Provision server. However, you will also shut down your client applications; NIM will immediately exit if you stop the server.

To stop the server, select the **Shutdown Server** button. You will see a warning message, Figure 7-8, that asks if you want to continue. Select **Continue** to stop the server and exit NIM.

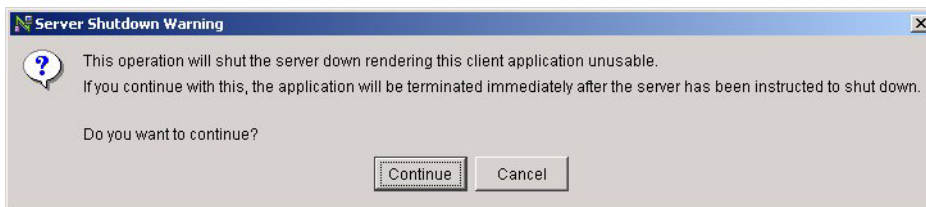


Figure 7-8: Server Shutdown Warning

For Windows and Solaris installations, there are other ways to start and stop the server. See the *ISM Provision Installation Guide* for more information.

View Server Log

You can view the ISM Provision server log from the **Logs** tab of the **Server Administration** view. Select the **Main Server** tab, then the **Refresh** button, to view the log (see Figure 7-9).

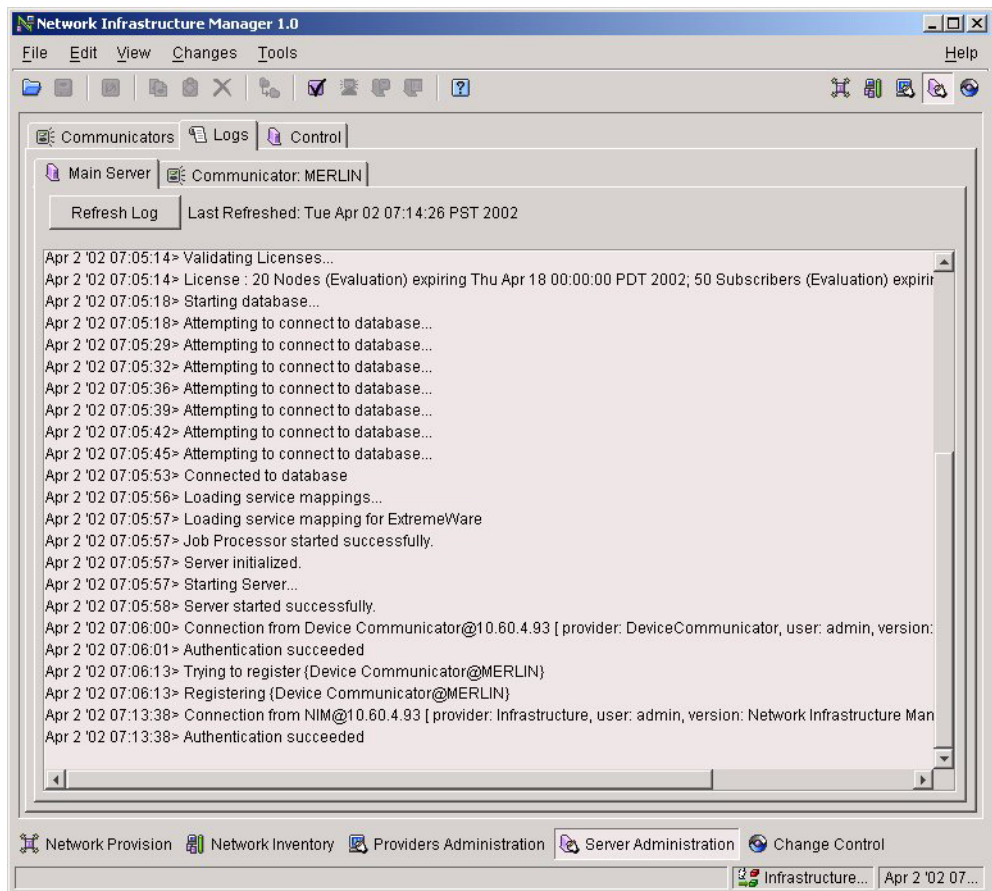


Figure 7-9: ISM Provision Server Log



Change Control

Overview

The **Change Control** view of NIM allows you to commit changes to the ISM Provision server, view the current uncommitted changes that you have made, to view previously committed, scheduled, or saved changes, and to create and rollback configuration versions.

This chapter explains the following concepts about the **Change Control** view of Network Infrastructure Manager:

- Jobs
- Configuration Versions

This chapter explains the following tasks that can be accomplished in the **Change Control** view of Network Infrastructure Manager:

- View Current Job Changes
- View Committed, Scheduled, or Saved Jobs
- Delete Scheduled or Saved Jobs
- Create Configuration Version
- Rollback to a Configuration Version

Jobs

Every time you add, modify, or delete any object, this change is captured by the client to either save or commit to the ISM Provision server. When you save or commit your changes, this list of individual additions, modifications, and deletions is sent to the ISM Provision server as a single entity called a job. A job may consist of a single change to one device parameter or the addition of hundreds of configuration objects, but it is saved or committed as a unit to the ISM Provision server. Once a job is committed, any changes to the configurations of managed devices are sent to the devices using the device communicator assigned to that device.

Different from a committed job is a saved job. A saved job is also stored in the ISM Provision server, but its collection of changes are not sent out to the network, unless the saved job is later committed. A scheduled job is a saved job that will automatically be committed at a scheduled time. One of the options of the commit process is to do the actual commit at a later time. Any job scheduled to be committed at a later time is saved until the commit time, and then committed to the network.

If an error occurs while a job is being committed, and any of the changes that make up the job cannot be committed, the entire job is rejected, and any parts of the job already added are backed out. A committed job that causes an error is still listed along with other committed jobs, but its status is listed as rejected. To correct the errors, view the committed yet rejected job, and review the job results. You will see the details of the problem that caused the error.

Any job can be viewed, whether committed, rejected, scheduled or saved. You can review the individual objects that were created, modified, and deleted. You can also review the results of the job to help you correct any errors that might have occurred.

Configuration Versions

A configuration version in Network Infrastructure Manager is a collection of all the current configurations of all the devices in the ISM Provision server. At any time you can create a configuration version, and later roll your network back to that state. Typically, you would create a configuration version before you roll out new changes to the network on multiple devices, so that you can go back to a known good state easily, in case of difficulties.

Change Control Tasks

The following tasks can be accomplished in the **Change Control** view of Network Infrastructure Manager:

- View Current Job Changes
- View Committed, Scheduled, or Saved Jobs
- Delete Scheduled or Saved Jobs
- Create Configuration Version
- Rollback to a Configuration Version

View Current Job Changes

Every change you make in NIM is captured in the current job. If you want to see what changes have been made that are not yet committed to the ISM Provision server, you would view the current job changes. You will view the changes in the **Current Job Changes** tab of the **Change Control** view of NIM.

Steps. To view the current job changes:

- 1 Select the Current Job Changes tab in Change Control view**
- 2 Select the Created, Modified, or Deleted Objects In This Job tab**

The three tabs on the **Current Job Changes** tab are: **Created Objects In This Job**, **Modified Objects In This Job**, and **Deleted Objects In This Job**. Each tab displays the object changes that are not yet committed to the ISM Provision server. Choose the category of changes you wish to view.

- 3 Select individual objects to view details (if any)**

For some objects, more details are listed in the **Selected Details** panel. Click on the object, and selected details are displayed in the panel (see Figure 8-1).

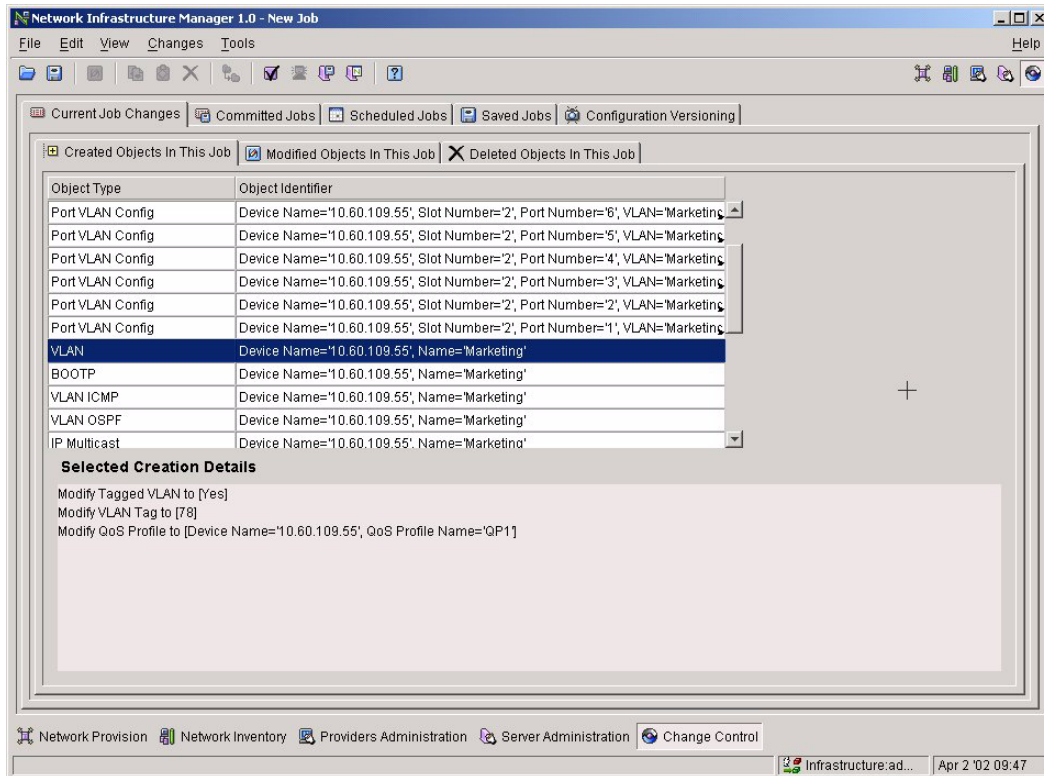


Figure 8-1: Current Job Changes

View Committed, Scheduled, or Saved Jobs

Committed, scheduled, and saved jobs are displayed on tabs in the **Change Control** view of NIM. For these tabs, you can filter which jobs are displayed, by provider and device communicator, and by individual user account. Once selected you can review the job, and view the result of committing or saving it.

Summary Steps. To view a committed, scheduled, or saved job:

- 1 Select the **Committed, Scheduled, or Saved Jobs** tab in the **Change Control** view
- 2 Select the provider and user account from the drop-down lists
- 3 Select the job to review by clicking on the job name
- 4 Select the **Review** button

5 Review the job

6 Select Close

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To view a committed, scheduled, or saved job:

1 Select the Committed, Scheduled, or Saved Jobs tab in the Change Control view

From the Change Control view, select the tab for the job you want to view (see Figure 8-2).

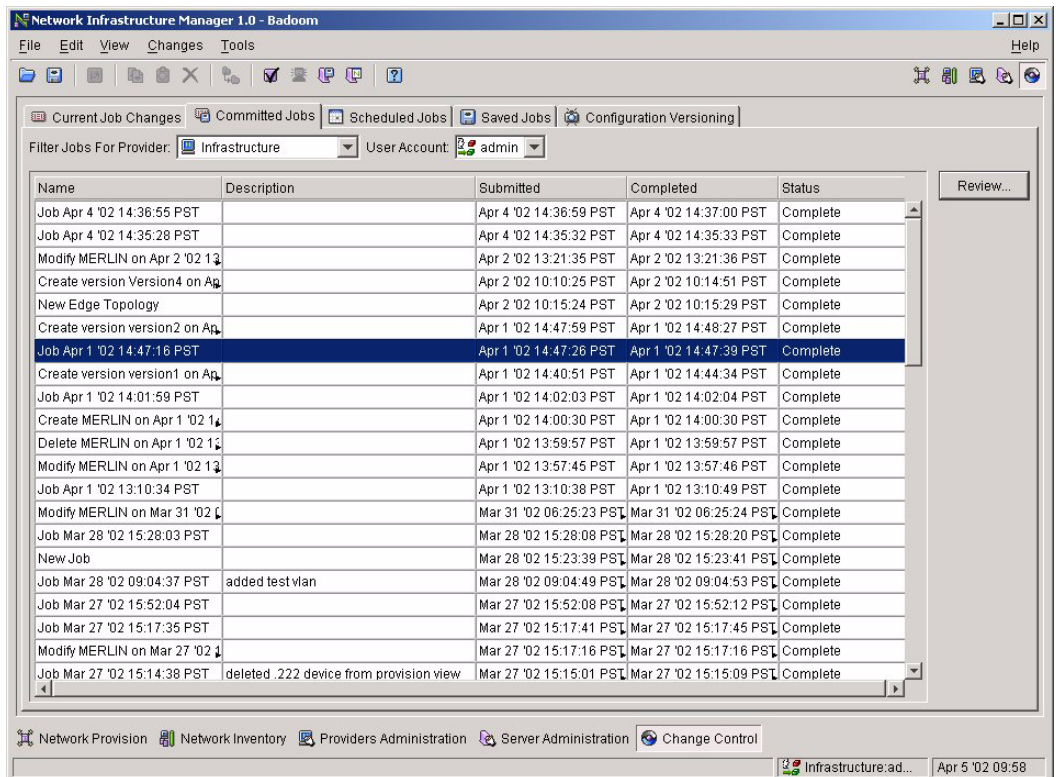


Figure 8-2: Committed Jobs Tab

2 Select the provider and user account from the drop-down lists

Select which category of jobs you want to view. **Infrastructure** represents the jobs originating with a NIM client, **Device Communicator** represents jobs committed when a device communicator synchronizes the server with a managed device, and the other providers represent jobs from the IPSM clients.

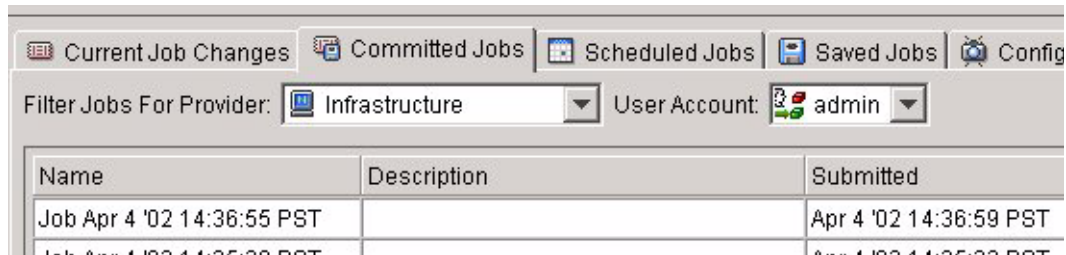


Figure 8-3: Job Filter Choices

3 Select the job to review by clicking on the job name

4 Select the Review button

Once you select the **Review** button, the **Details For Job** window opens.

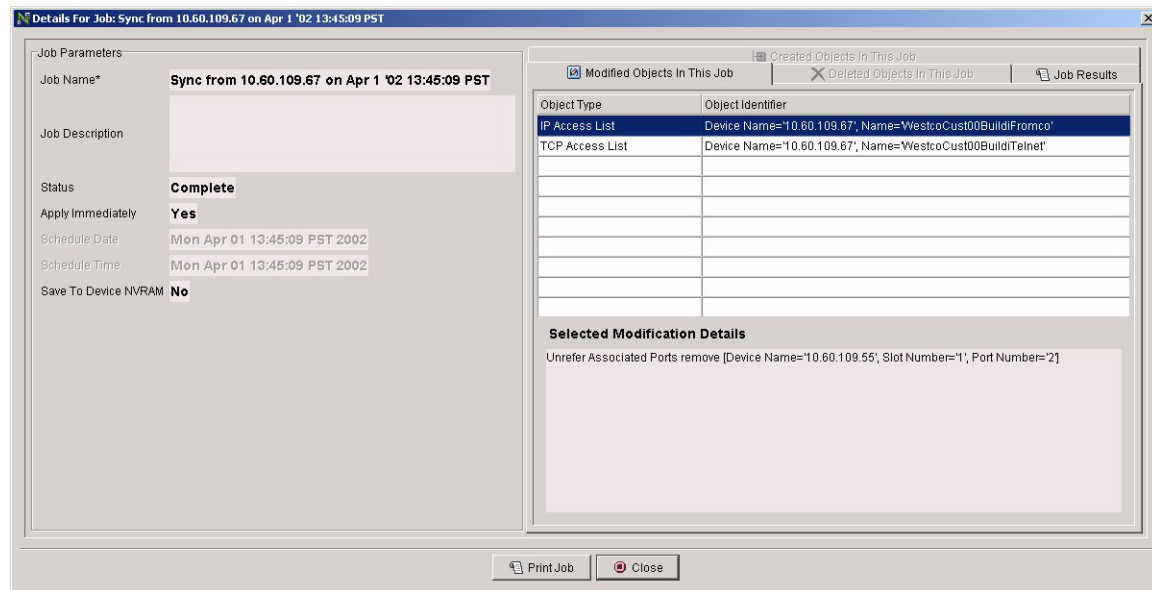


Figure 8-4: Job Details Window

5 Review the job

On the right-hand side of the window you can select tabs to view created, modified, and deleted objects in this job. Select the tab of interest, then select the object of interest by clicking on it. Selected details about the object will be displayed in the **Selected ... Details** panel. If you are examining a committed job that was rejected, you will find useful information in the **Job Results** tab.

6 Select Close

Select **Close** to close the window.

Delete Scheduled or Saved Jobs

You can delete jobs that have not yet been committed to the ISM Provision server, but once a job is committed it cannot be deleted. (Of course, you could review a committed job and reverse the individual changes you made, then commit. You would probably want to create a configuration version if you think you might want to later remove a job you were planning to commit.)

Steps. To delete a scheduled or saved job:

1 View the job in the Scheduled or Saved Jobs tab

See the task, “View Committed, Scheduled, or Saved Jobs”, if you need detailed instructions.

2 Select the Delete button

3 Select Delete to confirm, Cancel otherwise

When you selected the **Delete** button in step 2, a **Delete Job** window appears to confirm your choice. Select the **Delete** button on the window to delete the job.

Create Configuration Version

See the section, “Configuration Versions”, to find out what configuration versions are. Before you create a configuration version, be sure that any changes you have made to the configurations in your current session have been committed to the server, or you have reverted to the current server state.

Configuration versions are created from the **Configuration Versioning** tab of the **Change Control** view of NIM.

Steps. To create a configuration version:

1 Select the Configuration Versioning tab in the Change Control view

The Configuration Versioning tab displays the current versions (see Figure 8-5).

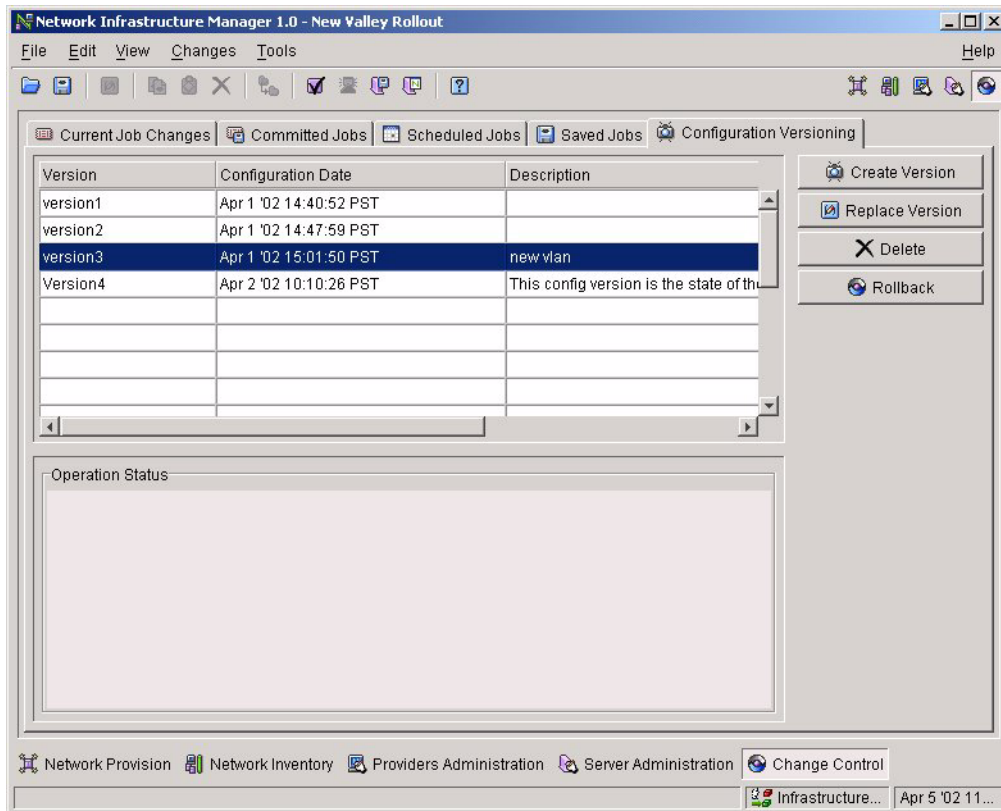


Figure 8-5: Configuration Versioning Tab

2 Select the Create Version button

The **Create Version** button opens the **Create Configuration Version** wizard.

3 Name the Version, add comments

Name the version and add any comments.

4 Select Finish

5 View Operation Status panel for versioning progress

While the configuration version is being created, you can view the progress of the process in the **Operation Status** panel. The mouse cursor for NIM will remain an

hourglass until the process is complete. You cannot perform any other functions with Network Infrastructure Manager until the version is created. When the message, “Configuration version request was completed successfully.”, appears in the panel, the process is complete and you can continue using NIM.

Rollback to a Configuration Version

Rollback will return your network and ISM Provision server to a previously saved configuration version. You perform a configuration version rollback from the **Configuration Versioning** tab of the **Change Control** view of Network Infrastructure Manager.

To rollback, the ISM Provision server must not have any clients connected to it, except for the NIM client initiating the rollback. You may wish to send a broadcast message to any other connected clients to tell them to log out and disconnect. See the tasks, “View Other Connected Users” and “Send Broadcast Message”, in Chapter 7, “Managing the ISM Provision Server”, for more information.

Summary Steps. To rollback to a configuration version:

- 1 Verify no other clients are connected to the ISM Provision server**
- 2 Select the rollback configuration version**
- 3 Select the Rollback button**
- 4 Select Continue to confirm**
- 5 Select Continue to acknowledge the rollback start message**
- 6 View the Operation Status panel for rollback progress**
- 7 Select Update Now, or Update later and Synchronize**
- 8 Select Continue to acknowledge the rollback complete message**

Detailed Steps. The following steps are a more detailed explanation of the previous section.

To rollback to a configuration version:

- 1 Verify no other clients are connected to the ISM Provision server**
See the task, “View Other Connected Users”, for
- 2 Select the rollback configuration version**
Click on the version that you wish to become the rollback configuration version.

3 Select the Rollback button

This will open a confirmation window.

4 Select Continue to confirm

5 Select Continue to acknowledge the rollback start message

A broadcast message window announces that a rollback is in progress.

6 View the Operation Status panel for rollback progress

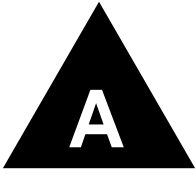
While the rollback configuration version loaded, you can view the progress of the process in the **Operation Status** panel. The mouse cursor for NIM will remain an hourglass until the process is complete. You cannot perform any other functions with Network Infrastructure Manager until the rollback is completed. When the message, "Configuration rollback request was completed successfully.", appears in the panel, the process is complete and you can continue using NIM.

7 Select Update Now, or Update later and Synchronize

Details at the step "Choose Update Now, or choose Update Later and later use the Synchronize icon to update" on page 5-3.

8 Select Continue to acknowledge the rollback complete message

A broadcast message window announces that the rollback is complete.



ISM Provision Devices, Images, and Modules

Supported Devices, Images and Modules

Table A-1 lists the device/module combinations supported by ISM Provision version 1.0. Table A-2 lists the device/image combinations that are supported. ISM Provision will support later image versions than those listed, but can only support the features in the latest image listed. New features introduced in later images are not supported in this version.

Table A-1: Supported Modules¹

Modules	Alpine 3802	Alpine 3804	Alpine 3808	BD 6804	BD 6808	BD 6816
FM8V ²	Y	Y	Y	N	N	N
FM24MF	Y	Y	Y	N	N	N
FM24SF	Y	Y	Y	N	N	N
FM24T	Y	Y	Y	N	N	N
FM32T	Y	Y	Y	N	N	N
GM4S	Y	Y	Y	N	N	N
GM4T	Y	Y	Y	N	N	N
GM4X	Y	Y	Y	N	N	N
WM1T ³²	Y	Y	Y	N	N	N
WM4E ¹²	Y	Y	Y	N	N	N
WM4T ¹²	Y	Y	Y	N	N	N

Table A-1: Supported Modules¹ (continued)

Modules	Alpine 3802	Alpine 3804	Alpine 3808	BD 6804	BD 6808	BD 6816
WDM	Y	Y	Y	Y	Y	Y
F48T	N	N	N	Y	Y	Y
F96T	N	N	N	Y	Y	Y
G8T	N	N	N	Y	Y	Y
G8X	N	N	N	Y	Y	Y
G12SX	N	N	N	Y	Y	Y
P3CM	N	N	N	Y	Y	Y
P3CS	N	N	N	Y	Y	Y

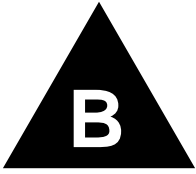
1. Not all supported module types are supported in all image versions

2. Requires WAN image for support

Table A-2: Supported Devices and Images¹

Device Type	6.1.8	6.1.9	6.2.0	6.2.1	6.1.8w3.0.x	6.1.8w3.1.x	6.2e3
Summit1i(TX/SX)	Y	Y	Y	Y	N	N	N
Summit5i(TX/LX/SX)	Y	Y	Y	Y	N	N	N
Summit7i(TX/LX/SX)	Y	Y	Y	Y	N	N	N
Summit48i	Y	Y	Y	Y	N	N	N
Summit24e3	N	N	N	N	N	N	Y
Alpine 3802	N	N	N	Y	Y	Y	N
Alpine 3804	Y	Y	Y	Y	Y	Y	N
Alpine 3808	Y	Y	Y	Y	Y	Y	N
BlackDiamond 6804	Y	Y	Y	Y	N	N	N
BlackDiamond 6808	Y	Y	Y	Y	N	N	N
BlackDiamond 6816	N	N	Y	Y	N	N	N

1. ISM Provision supports future image versions, but cannot support newly added features. For example, if 6.2.2 is discovered on a device, it will support all features through 6.2.1, or if 6.1.8w3.2.1 is discovered it will support all features through 6.1.8w3.1.x.



ISM Provision Rules

Overview

The ISM Provision clients will check device configurations against their own set of rules and issue errors or warnings whenever the rules are violated. This rule checking occurs manually whenever you select the **Verify Configuration** icon or the menu item **Changes>Verify Configuration**. This checking occurs automatically when changes are committed to the ISM Provision server and the option, **Verify configuration before commit**, is selected (found at the menu item **Tools>Options>Rules Options**).

If the verification step finds an error or warning, the **Verification** panel of the **Network Provision** view shows which rules were violated and suggests a possible configuration change to correct the problem. If you still wish to commit configurations that display errors or warnings after verification, select the option **Allow errors to be committed** from the **Rules Options** tab of **Tools>Options**.

When the configurations are committed to the ISM Provision server, the server again checks the client rules before storing the configurations (unless the **Server Rules Enabled** checkbox is not checked, found on the **Control** tab of the **Server Administration** view of NIM), and checks additional server rules. These server rules are always checked and cannot be disabled.

The rules are listed in the following tables:

- Table B-1: Rules Checked by the NIM client and ISM Provision server
- Table B-2: Rules Checked by the IPSM client and ISM Provision server
- Table B-3: Rules Checked by ISM Provision server

Table B-1: Rules Checked by the NIM client and ISM Provision server

Object	Rule	Type
Access List (ICMP, IP, TCP, & UDP)	Check if the label/name is already in use by an Abstract VLAN (VLAN or Sub-VLAN) or a STPD object	Error
	Check if the specified addresses extend into their address masks	Error
	Check if the specified precedence of all access lists are not unique	Error
Device	Check module/slot compatibility in Alpine 3802	Error
Device IGMP	Check if response interval > query interval in timer	Error
Device OSPF	Check if Default Route is enabled when modifying Cost, Tag, or External Type parameters	Error
	Check if at least one VLAN in the device is in an IP Forwarding mode while enabling OSPF	Error
Device RIP	Check if Default Route is enabled when modifying Cost, Tag, or Always Advertise parameters	Error
	Check if at least one VLAN in the device is in an IP Forwarding mode while enabling RIP	Error
	Check if update time > route timeout in timer	Error
EAPS Domain	Check if hello time > fail time in timer	Error
	Check if control VLAN's QoS Profile is not QP8	Warning
	Check if the primary and secondary ports are not tagged and added to the control VLAN	Warning
FDB Entry	For each port in the entry, check if it is not in the VLAN	Error
	Check if a VLAN is not assigned to the entry	Error
Gigabit Ethernet Port	For ports 49 and 50 on Summit 48i, check if the user has configured a software-based redundant port	Error
IO Board	Check if explicit configuration has been unselected	Error
	Check if module is not supported by the device type and agent version	Error
Load Sharing	Check if the logical port does not exist in the list of physical ports	Error
	Check if member ports of a Black Diamond are on same board	Error
	Check if any of the member ports are not enabled	Error
	Check if there are more than eight member ports	Error

Table B-1: Rules Checked by the NIM client and ISM Provision server (continued)

Object	Rule	Type
Multilink Port Group	Check if the group is not in any VLAN while being enabled	Error
	Check if the group does not have any ports while being added to a VLAN	Error
	Check if the group is IPCP and is being added to a Sub-VLAN	Error
Multilink PPP	Check if the PPP configuration's group does not have any ports while configuring the group to run PPP with BCP or IPCP.	Error
Port VLAN Config	Check if an untagged VLAN is marked as tagged	Error
Radius Server	Check if TACACS is enabled	Error
Route Advertisement	Check if min interval > max interval in timer	Error
	Check if lifetime < max interval in timer	Error
STP Domain	Check if the STPD's tag does not match any of its member VLANs' tag	Error
	Check if the label/name is already in use by an Access List or an Abstract VLAN (VLAN or Sub-VLAN) object	Error
Sub-VLAN	Check if the label equals 'all'	Error
	Check if the VLAN has more than one WAN port	Error
	Check if the VLAN has more than IPCP MLP or PPP port	Error
	Check if the VLAN's protocol causes a conflict in any of its member ports	Error
	Check if the VLAN's tag conflicts with its own loopback id	Error
	Check if the VLAN has been untagged after it was tagged	Error
	On a Black Diamond, check if the loopback port is not in the same slot as all the other ports	Error
	Check if a super-VLAN has not been assigned	Warning
	Check if the super-VLAN's IP address is not configured	Error
	Check if the IP range does not overlap with the super-VLAN's IP address	Error/Wa arning
	Check if any ports (including multilink ports) are added as tagged when the VLAN is untagged	Error
	Check if the label/name is already in use by an Access List or an STPD object	Error
	Check if the VLAN contains ports that are in another STPD	Error
TACACS Server	Check if RADIUS is enabled	Error

Table B-1: Rules Checked by the NIM client and ISM Provision server (continued)

Object	Rule	Type
Topology	Check if both ends of the trunk:	Error
	<ul style="list-style-type: none">• have the same port type• have the same Auto Negotiation/Speed/Duplex setting• are both fiber or both copper• have the same PPP parameters• have the same channel size• have the same framing• have the same VLAN tag• have the same VLAN IP subnet• have unique VLAN IP addresses	
	Check if both ends of the trunk have the same VLAN tag	Error
	Check if the number of links in the load-sharing group on each end of the trunk are the same	Error
	Check if the number of links in the multilink group on each end of the trunk are the same	Error
VLAN	Check if the label equals 'all'	Error
	Check if the VLAN has more than one WAN port	Error
	Check if the VLAN has more than one IPCP MLP or PPP port	Error
	Check if the VLAN's protocol causes a conflict in any of its member ports	Error
	Check if the VLAN's tag conflicts with its own loopback id	Error
	Check if the VLAN has been untagged after it was tagged	Error
	On a Black Diamond, check if the loopback port is not in the same slot as all the other ports	Error
	Check if the IP subnet is not unique among all the VLANs in the device	Error
	If IP MTU >1500, check if jumbo frames are not enabled on any of the VLAN's member ports	Error
	Check if any ports (including multilink ports) are added as tagged when the VLAN is untagged	Error
Check if the label/name is already in use by an Access List or a STPD object	Error	
Check if the VLAN contains ports that are in another STPD	Error	

Table B-1: Rules Checked by the NIM client and ISM Provision server (continued)

Object	Rule	Type
VLAN Bootp	When enabling, check if the IP address is configured on the VLAN	Error
VLAN DVMRP	When enabling, check if PIM is also enabled on the VLAN	Error
	When enabling, check if the IP address is not configured on the VLAN	Error
	When enabling, check if IP forwarding is not enabled on the VLAN	Warning
VLAN ESRP	While changing the group number, check if ESRP is currently enabled/running on the VLAN	Error
	Check if a tracked VLAN is also running ESRP	Error
	Check if a domain master VLAN has sub-VLANs	Error
VLAN ESRP Track Ping	Check if the frequency for pinging an IP address is not greater than 0 seconds	Error
VLAN ICMP	When enabling, check if the IP address is not configured on the VLAN	Error
	When enabling, check if IP forwarding is not enabled on the VLAN	Warning
VLAN IP Forwarding	When enabling, check if the IP address is not configured on the VLAN	Error
VLAN IP Multicast Routing	When enabling, check if IP forwarding is not enabled on the VLAN	Warning
VLAN NAT	When enabling, check if the IP address is not configured on the VLAN	Error
VLAN OSPF	When enabling, check if IP forwarding is not enabled on the VLAN	Warning
VLAN PIM	When enabling, check if DVMRP is also enabled on the VLAN	Error
	When enabling, check if the IP address is not configured on the VLAN	Error
	When enabling, check if IP forwarding is not enabled on the VLAN	Warning
VLAN RIP	When enabling, check if IP forwarding is not enabled on the VLAN	Warning
WAN Port (T1, T3, and E1)	Check if the port is enabled, but is not under any VLAN	Error

Table B-1: Rules Checked by the NIM client and ISM Provision server (continued)

Object	Rule	Type
	Check if the port is enabled and is IPCP, but the VLAN which the port is under does not have an IP address configured	Error
	Check if the port is IPCP and is being added to a Sub-VLAN	Error

Table B-2: Rules Checked by the IPSM client and ISM Provision server

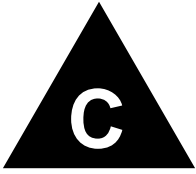
Object	Rule	Type
IP Range Subscriber	Check if the IP address is not within the Provider's IP ranges	Error
	Check if the VLAN tag is not within the Provider's VLAN tag pool	Error
IP Subscriber	Check if the IP address is not within the Provider's IP ranges	Error
	Check if the loopback port is the same as the subscriber port	Error
Traffic Policy	Check if the specified source addresses of the traffic policy do not extend into their address masks	Error
	Check if the precedence of all policy based services is not unique	Error
Service Bundle	Check if the service category does not match the service category of the services within the bundle	Error

Table B-3: Rules Checked by ISM Provision server

Object	Rule	Type
Device Communicator Entry	Check if the server license has expired or if the maximum number of managed devices allowed by the license has been exceeded	Error
Subscriber License	Check if the server license has expired or if the maximum number of managed devices allowed by the license has been exceeded	Error
IP Range Subscriber	Check if the IP address range is within the Provider IP range	Error

Table B-3: Rules Checked by ISM Provision server (continued)

Object	Rule	Type
	Check if the VLAN tag is within the provider tag pool	Error
IP Subscriber	Check if the IP address range is within the Provider IP range	Error
	Check if the loopback port is the same as the subscriber port	Error



ISM Provision Server Maintenance

Overview

You will want to periodically backup the ISM Provision server to avoid having to recreate your ISM Provision information. There is a database backup utility available to safely perform the task. See the section, “Database Backup Utility”, for instructions on backing up a database and installing a backup database.

Another database related task is to add license keys to the server. If you have evaluation licenses, they will eventually expire, and if the number of nodes or subscribers you want to support exceeds your current licenses, you will want to add additional license keys. See the section, “Adding a License Key”, for instructions on adding new keys.

Database Backup Utility

The Sybase database backup utility is shipped with the ISM Provision software.

The backup utility makes a backup copy of all data in the database. Backing up your database regularly will ensure that you will not need to re-enter or recreate all the ISM Provision information in the event that the database is corrupted or destroyed. Access the backup utility from the Windows or Solaris command line using the `dbbackup` command. This convention also allows incorporation into batch or command files.

Database Backup Utility Location

In this appendix, the term “<install_dir>” represents the directory where you installed ISM Provision.

For Windows installations, the backup utility is found in the following location:

```
<install_dir>\sybase\SQL Anywhere7\win32\dbbackup.exe
```

or if ISM Provision was installed in the default location:

```
c:\Program Files\Extreme Networks\ISM Provision\sybase\SQL Anywhere7\win32
```

For Solaris installations the backup utility is found in the following location:

```
<install_dir>/sybase/SYBSsa7/bin/dbbackup
```

or if ISM Provision was installed in the default location:

```
/opt/extreme/ismprov/sybase/SYBSsa7/bin
```

Using the Database Backup Utility

To back up the ISM Provision database running under Windows, use the command:

```
<install_dir>\sybase\SQL Anywhere7\win32\dbbackup -c  
"uid=DBA;pwd=SQL;dbf=<install_dir>\server\database\ismp.db" <backup_dir>
```

Under Solaris, use the command:

```
<install_dir>/database/dbbackup -c  
"uid=DBA;pwd=SQL;dbf=<install_dir>/server/database/ismp.db" <backup_dir>
```

This assumes a database user ID of `DBA`, with password `SQL`. These are the defaults used when the database server is installed through the ISM Provision installation process. If you have changed your database user ID and password, substitute your actual user ID and password in the command.

<install_dir> is the directory where the ISM Provision software is installed. Substitute the actual directory name in the command.

<backup_dir> is the directory where the backup copy of the database should be stored. Substitute an actual directory name in the command.

This command generates a backup of the database in the specified backup directory. The backup consists of two files, `ismp.db` and `ismp.log`. All database files are backed up. These files should be saved so they can be used to replace the original files in the event of a problem.

Syntax: `dbbackup [switches] directory`

Table C-1: dbbackup Command Switches

Switch	Description
<code>-c "keyword=value; ..."</code>	Supply database connection parameters
<code>-y</code>	Replace files without confirmation

Installing a Backup Database

The backup database is named `ismp.db`, and is kept in the directory you specified when you ran the `dbbackup` command.

To replace a damaged database with the backup copy, follow these steps:

- 1 Shut down the ISM Provision software following the instructions for your operating system in the *ISM Provision Installation Guide*, or from within NIM in the **Server Administration** view. See the task, “Stop Server”, in Chapter 7, “Managing the ISM Provision Server”.
- 2 Move or delete the old copy of `ismp.db` found in the ISM Provision installation, in the directory `<install_dir>\server\database`.
- 3 Copy the backup copy of `ismp.db` to the directory `<install_dir>\server\database`.
- 4 Restart the ISM Provision software following the instructions in the *ISM Provision Installation Guide* for your operating system environment.

Adding a License Key

The license keys are just long strings of characters stored in a simple text file.

For both Windows and Solaris the license file is:

```
<install_dir>/ISMPLicenseKey.txt
```

Steps. To add an additional license key:

1 Make a backup copy of the ISMPLicense.txt file

In case you have some problem, you can always revert to the original file.

2 Stop the ISM Provision server

The server periodically accesses the file, so you may want to stop the server. You will definitely need to start the server again to force it to read the license file after you add the new key, so we recommend that you stop the server at this point.

3 Open the ISMPLicense.txt file in a text editor

Use an editor that can save the file as text only (see Figure C-1).

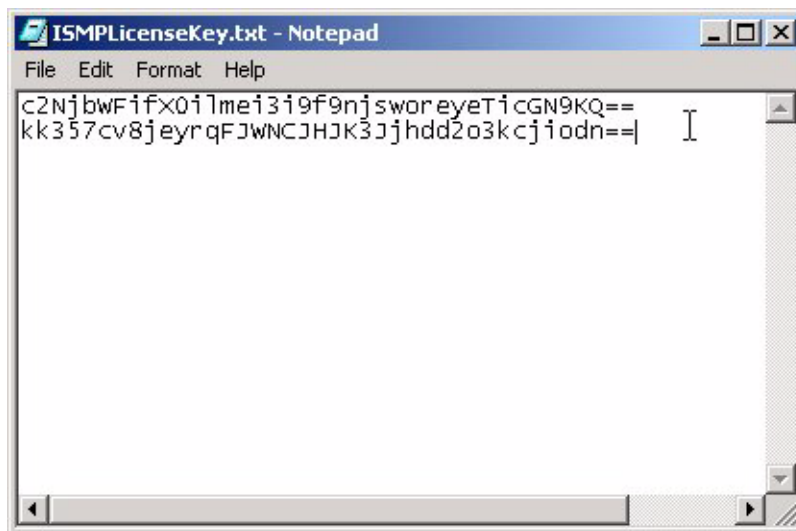


Figure C-1: ISMPLicenseKey.txt File

4 Add the new license key on its own line

Be sure there are no extra spaces at the end of the lines (see Figure C-2).

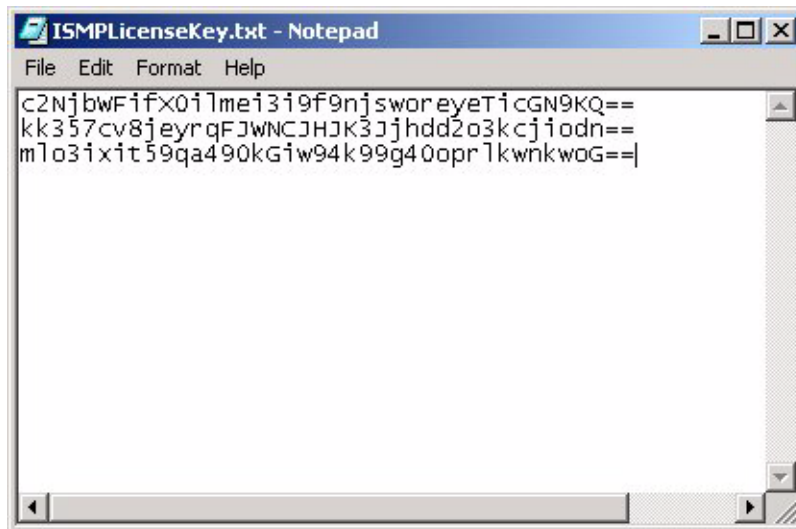


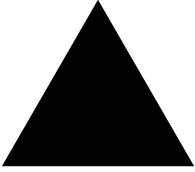
Figure C-2: ISMPLicenseKey.txt File with New Key Added

5 Save the file

6 Start the ISM Provision server

When you start the server, it will read the new ISMPLicenseKey.txt file and update your access. Start the ISM Provision software following the instructions in the *ISM Provision Installation Guide* for your operating system environment.

To verify if the current licenses have been read correctly by the server, examine the server log. The beginning of the log displays the number of node and subscriber licenses. To view the server log, see the task, “View Server Log”, in Chapter 7, “Managing the ISM Provision Server”.



Index

A

account password	2-4
add	
configuration object	4-22
device	5-2
provider	6-2

C

capture	
configurations	5-1
capture existing network	5-1
change	
unmanaged device to managed	4-35
changes	
remove	4-29
revert	4-29
save	4-34
commands	
unsupported	4-6
configuration	
display	4-8
save running	5-18
unsupported commands	4-6
verify	B-1
view options	4-18
configuration errors	B-1
configuration object	
add	4-22
create	4-22
modify	4-26
configuration warnings	B-1
configurations	
capturing	5-1

create	4-20
modify	4-20
conventions	
notice icons, Preface	x
text, Preface	x
copy	
device	4-29
object	4-29
create	
configuration object	4-22
configurations	4-20
provider	6-2

D

delete	
from network inventory	5-11
device	
add	5-2
copy	4-29
limit access	6-5
new	4-21
upload	5-16
Device Communicators	1-4
device communicators	1-4
devices	
managed	4-7
unmanaged	4-7
display configurations	4-8

E

enable	
server rules	B-1
error	B-1

existing network	
capture	5-1
export	
inventory file	5-15

I	
icons, named	3-4
import	
inventory file	5-11
infrastructure provider	6-2
inventory	
network	5-2
inventory file	5-11
export	5-15
IP Service Manager	1-1, 1-5
ISM Provision	1-1
ISM Provision Server	1-4
ISM Provision server	1-4

J	
job	8-2

K	
key information	4-6

L	
Launch	
NIM client	2-2
login	2-2
NIM client	2-2

M	
managed devices	4-7
modify	
configuration object	4-26
configurations	4-20
network inventory	5-10

N	
named icons	3-4
network	
inventory	5-2
Network Infrastructure Manager	1-1, 1-5
network inventory	
delete	5-11
modify	5-10
Network panel	4-4
Network Provision view	3-5, 4-1
new device	4-21

NIM	1-5
NIM client	
account password	2-4
launch	2-2
login	2-2
user account	2-4
NIM views	
selecting	3-2

O	
object	
copy	4-29
open	4-15
Objects	4-5
objects	
suppress display	4-18
open	
object	4-15
options	
configuration view	4-18
view	4-20

P	
panels	
network	4-4
Properties	4-5
Template	4-5
verification	4-5
policy based services	1-5
Properties panel	4-5
provider	
add	6-2
create	6-2
infrastructure	6-2
limit device access	6-5
provider accounts	1-5
providers	1-5

R	
remove	
changes	4-29
revert	
changes	4-29
rules	B-1
running configuration	
save	5-18

S	
save	
changes	4-34
running configuration	5-18
selecting	

NIM views	3-2
server	1-4
update	5-6
server rules	B-1
enable	B-1
service bundles	1-5
special case	
upload device	4-39
start	2-1
subscribers	1-5
suppress	
display of objects	4-18
synchronize	5-6

T

Telnet	4-39
Templates panel	4-5

U

unmanaged device	
change to managed	4-35
unmanaged devices	4-7
unsupported configuration commands	4-6
update	
server	5-6
upload	
device	5-16
upload device	
special case	4-39
user account	2-4
NIM client	2-4

V

Verification panel	4-5
verification panel	B-1
verify configuration	B-1
view options	4-20
views	
Network Provision	3-5, 4-1

W

warning	B-1
WebVista	4-39

