Enterprise Manager Administrator Guide

version 1.2.2

MAN-0223-02

Product Version

This manual applies to product version 1.2.2 of the Enterprise Manager.

Publication Date

This manual was published on January 29, 2007.

Legal Notices

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, Internet Control Architecture, IP Application Switch, iRules, OneConnect, Packet Velocity, SYN Check, Control Your World, ZoneRunner, uRoam, FirePass, TrafficShield, Swan, WANJet, and WebAccelerator are registered trademarks or trademarks, and Ask F5 is a service mark, of F5 Networks, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. F5 Networks' trademarks may not be used in connection with any product or service except as permitted in writing by F5.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler <bazsi@balabit.hu>, which is protected under the GNU Public License.

This product includes software developed by Niels Miller <nisse@lysator.liu.se>, which is protected under the GNU Public License.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with "386BSD" and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to "NetBSD," "FreeBSD," "Mach" (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

Table of Contents

1
Introducing Enterprise Manager

2
Installation and Setup

3
Licensing and Configuring the System

4
Discovering and Managing Devices

5
Managing UCS Archives

6
Managing Device Configurations

7
Managing Software Images

8
Managing User Account Data

9
Monitoring and Alerting

10
Managing Device Certificates

11
Auditing Enterprise Manager System Events

Glossary

Index

1

Introducing Enterprise Manager

- Working with Enterprise Manager
- Using Enterprise Manager features
- Working with the Enterprise Manager interface
- Finding user assistance

Working with Enterprise Manager

F5 Networks Enterprise Manager is a device management appliance that provides you with a wide variety of features to assist in the management of multiple F5 Networks devices. Enterprise Manager can help simplify several administrative tasks associated with managing multiple F5 Networks devices including software and hotfix upgrades, configuration backup and archiving.

Enterprise Manager can automatically discover and manage F5 Networks traffic management devices through a secure socket layer (SSL) connection. It collects and stores information about devices in a database and makes it available through a web-based interface similar to that of other F5 Networks version 9.x traffic management products. The product is scalable so that as you add F5 Networks devices to the network, you can manage them using Enterprise Manager.

Using the features of Enterprise Manager, you can perform the following tasks from a centralized location:

- Discover F5 Networks devices in your enterprise, and manage them from a central location.
- Save a full device configuration, including network object and system settings, then deploy it to one or more additional devices
- Archive and restore multiple UCS archives.
- Schedule the automatic creation of UCS archives.
- Import and store multiple software and hotfix images in a central software repository.
- Deploy software and hotfix images to one or more devices.
- Synchronize device configurations between managed peer devices.
- Manage the active or standby state of devices in high availability systems.
- Organize devices into device groups to facilitate the management of related devices.
- Change user passwords on multiple devices.
- Copy user account data from one device to multiple devices.
- Configure custom alerts to notify specific users of network events such as certificate expiration, or a completed software upgrade.
- Track changes made by users of Enterprise Manager.
- Monitor basic network health.

◆ **Important**

*Enterprise Manager can currently manage devices running the BIG-IP 9.1.1 or later software version. See **Working with compatible managed devices**, on page 1-2 for detailed information about managed device compatibility by feature.*

Working with compatible managed devices

Enterprise Manager version 1.2 can manage devices running the BIG-IP 9.1.1 or later software version. Additionally, Enterprise Manager can manage all Enterprise Manager devices.

Although Enterprise Manager works with several versions of BIG-IP software, certain features require that managed devices are running software later than the 9.1.1 minimum. To help ensure the best performance, we recommend that you upgrade your managed devices to the latest version. The tables on the following pages outline the features supported by managed device.

Many new features introduced in Enterprise Manager version 1.2 are not supported by existing BIG-IP software. The upcoming BIG-IP version 9.4 software will support many Enterprise Manager features such as copying user access settings and saving and deploying device configurations.

The tables in the following section indicate which managed devices are compatible with Enterprise Manager features. Devices that support the corresponding feature are denoted with an **X** in each table.

Reviewing user management feature compatibility

The basic user management features of Enterprise Manager are compatible with all managed devices that meet the minimum requirements. You can view user account names, user web roles, and user shell roles for any managed device in the network.

User Management Feature	Enterprise Manager v1.0	Enterprise Manager v1.2	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.4
View all user account names in the network	X	X	X	X	X
View all user web roles in the network	X	X	X	X	X
View all user shell roles in the network	X	X	X	X	X

Table 1.1 *Managed device compatibility with basic User Management features*

Enterprise Manager version 1.2 introduces advanced user management features that enable you to view additional user information on managed devices in the network. If you use Enterprise Manager with BIG-IP version 9.4 (an upcoming release), or Enterprise Manager version 1.2, you can view details about authentication or shell access settings.

User Properties Feature	Enterprise Manager v1.0	Enterprise Manager v1.2	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.4
Open user and user access configuration settings for a device using the Launch Pad screen	X	X	X	X	X
Single sign-on to managed devices from Launch Pad screen					
View Authentication properties for user accounts on a device	-	X	-	-	X
View Shell Access properties for user accounts on a device	-	X	-	-	X

Table 1.2 *Managed device compatibility with User Properties features*

Changeset feature compatibility

The changeset feature, which enables you to save, verify, and deploy an advanced set of device configuration data is only compatible with BIG-IP version 9.4 (which is an upcoming release), and Enterprise Manager version 1.2.

Changeset Feature	Enterprise Manager v1.0	Enterprise Manager v1.2	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.4
Create changeset source	-	X	-	-	X
Verify changeset data	-	X	-	-	X
Deploy changeset data	-	X	-	-	X

Table 1.3 *Managed device compatibility with changeset features*

Task compatibility

Using Enterprise Manager, you can configure tasks to assist you in managing devices in the network. New tasks related to copying user access configuration data and changesets are only supported by BIG-IP version 9.4 (which is an upcoming release), and Enterprise Manager version 1.2. The new Change User Password task is compatible with all managed devices.

Task	Enterprise Manager v1.0	Enterprise Manager v1.2	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.4
Install Software Image	X	X	X	X	X
Install Software Hotfix	X	X	X	X	X
Copy User Access Configuration	-	X	-	-	X
Deploy Device Configuration	-	X	-	-	X
Change User Password	X	X	X	X	X

Table 1.4 *Managed device compatibility with task features*

Using Enterprise Manager features

If you follow the chapters in this guide, you can learn about how each feature can enhance your network management options, and how you can use each feature. We arranged the chapters in a logical order that guide you through the process of setting up Enterprise Manager in your network, to discovering devices, to grouping devices, and finally performing management tasks on these devices.

Each chapter explains one or two main features, explains new concepts related to enterprise management, and provides procedures to help you complete the tasks required to use the Enterprise Manager system.

Using each feature usually requires configuring a set of tasks. Enterprise Manager provides a wizard to assist you in setting up these tasks. You can use this wizard to discover devices, manage UCS archives, save and deploy full device configurations, deploy software and hotfix images, and manage user accounts.

Once you start these tasks, you can use Enterprise Manager's features to monitor the progress of these tasks, track changes by users, and monitor the basic network health of devices in the enterprise network.

Installing and setting up the system

We designed the Enterprise Manager system to work in your network in a manner similar to your other F5 devices. Installing and setting up Enterprise Manager should be familiar if you have set up several other F5 devices.

The difference with Enterprise Manager is that instead of helping you manage traffic, it helps you manage your F5 devices. The management appliance is robust and flexible so that it can work in many types of network topologies, even if you use multi-tiered configurations, address translation, or multiple firewalls.

You can find detailed information about configuring Enterprise Manager to work with your network in Chapter 2, *Installation and Setup*.

Discovering devices

After you set up Enterprise Manager in your network, you can use it to discover devices in the network. Discovering devices is the first step toward centrally managing the devices in the network. Enterprise Manager can search for devices by individual address, or it can scan an entire subnet.

Configuring a discovery task involves providing IP address ranges, user names, and passwords to the Enterprise Manager system and starting the task. For detailed instructions, see *Discovering and adding devices*, on page 4-2. Once you complete a device discovery task, you can manage software, device configurations, alerts, and user account information on all F5 devices in your network through Enterprise Manager.

Chapter 4, *Discovering and Managing Devices* describes which devices Enterprise Manager can manage and how to discover devices and add them to the device list, and introduces the concept of device grouping.

Grouping devices

Once devices are part of the managed device list, you can create custom device groups to further enhance your management options. When you create a device group, you can configure management tasks on a group in order to save time over configuring tasks on individual devices.

For example, when a number of devices belong to a device group, you can deploy software or assign alerts to the group, ensuring that all individual members of the group receive the same upgrade, or are assigned the same alert. Additionally, grouping devices may help organize the management of a wide range of devices. For detailed information about creating and managing device groups, see *Working with device groups*, on page 4-10.

Archiving and restoring device configurations

After you discover devices and create device groups, you can start managing the devices in your network. Prior to your managing software or user accounts, we recommend that you archive device configurations and set up rotating archive schedules to back up device configurations on managed devices in your network.

Enterprise Manager serves as a central user configuration set (UCS) repository, enabling you to save multiple UCS archives per device, providing the additional security of stable configurations in the event of a system restore. You can schedule the automatic archiving of device configurations, and you can save multiple known stable configurations. To learn more about device configuration archiving options, see Chapter 5, *Managing UCS Archives*.

Managing device configuration data

In addition to managing basic UCS archives, you can store and deploy extended sets of device configuration data through the use of changesets. A ***changeset*** stores all the configuration data on a BIG-IP Local Traffic Management system that is required to manage traffic including information about system settings and network objects.

Using Enterprise Manager you can store this information, or even deploy it to one or more additional BIG-IP systems in your network.

Enterprise Manager's configuration management features can greatly reduce the time required to install and configure multiple F5 devices in your network. For example, you can configure one BIG-IP system with a prototypical configuration, save the system's configuration data, then deploy the configuration data to additional BIG-IP systems in the network, saving time by creating a basic configuration on each device.

Enterprise Manager provides a wizard to create, verify, and deploy changesets to help you better manage configurations on BIG-IP systems in the network. You can even use a wizard to take a current device configuration setting, edit it to suit your needs, and then immediately deploy it to another device. For more information on managing device configuration data see Chapter 6, *Managing Device Configurations*.

Software and hotfix upgrades

After you have configured device configurations in your network, or deployed a device configuration to other managed devices, you can start managing the software images on managed devices. Enterprise Manager includes a software repository that you can use to store both software and hotfix images. Once you add these images to the repository, you can deploy a hotfix or software upgrade to one device, or configure multiple device upgrades. If you choose to configure device groups, you can create an upgrade task that installs software to all members of a device group.

You can also check which upgrades are compatible on a per device basis and install only the upgrades that suit your needs. In any software upgrade, you can choose multiple upgrade options, including the installation location and reboot location on each device. For detailed information about software upgrades see Chapter 7, *Managing Software Images*.

Managing user accounts in the network

Once you configure your network and install software upgrades on managed devices, you may want to manage the individual user accounts on these devices. Normally, managing user accounts on multiple devices can be a time-consuming process. However, Enterprise Manager provides tools to manage user accounts across multiple managed devices.

Using Enterprise Manager, you can view user roles on each device in the network, change the password for any user on any device, and even copy the user access configuration settings from one device to one or more other devices. A wizard assists you in creating tasks to change a user password, or copy user configuration settings.

For more information on working with user accounts on managed devices see Chapter 8, *Managing User Account Data*.

Monitoring the network and creating custom alerts

After you configure user accounts on managed devices, you may want to monitor the health of these devices. Enterprise Manager provides tools for monitoring the health of managed devices in the network. You can use these tools to create customized alerts to notify people when certain events occur. Using the device list, you can see a simple view of the state of managed devices in the network, including the failover state of high availability pairs.

You can create custom alerts to notify specific team members when a task completes or if a certificate expires, or you can send an SNMP trap to an existing network management server. To assist you in maintaining the health of BIG-IP systems in your network, an alert log provides a record of alerting events. For detailed information about device monitoring and alerting, see Chapter 9, *Monitoring and Alerting*.

Monitoring certificate expiration dates

Another important task of maintaining a robust network is ensuring that all certificates on managed devices are current. Enterprise Manager can monitor every certificate on each managed device in the network. This provides you the opportunity to monitor certificate expiration dates and renew certificates before they expire.

When you combine the certificate monitoring features with the alerting features of Enterprise Manager, you can create warnings when certificates expire or near their expiration dates. For detailed information about working with certificates on managed devices, see Chapter 10, *Managing Device Certificates*.

Auditing Enterprise Manager system events

As a final step in managing your network with Enterprise Manager, you may want to monitor tasks configured by Enterprise Manager users.

Enterprise Manager provides a comprehensive set of auditing features so that you can track what types of enterprise management tasks were initiated from a particular Enterprise Manager system. Depending on the options you choose, you can create and view logs of system, local traffic, and audit events on the Enterprise Manager system. See Chapter 11, *Auditing Enterprise Manager System Events* for more information about system event auditing.

Working with the Enterprise Manager interface

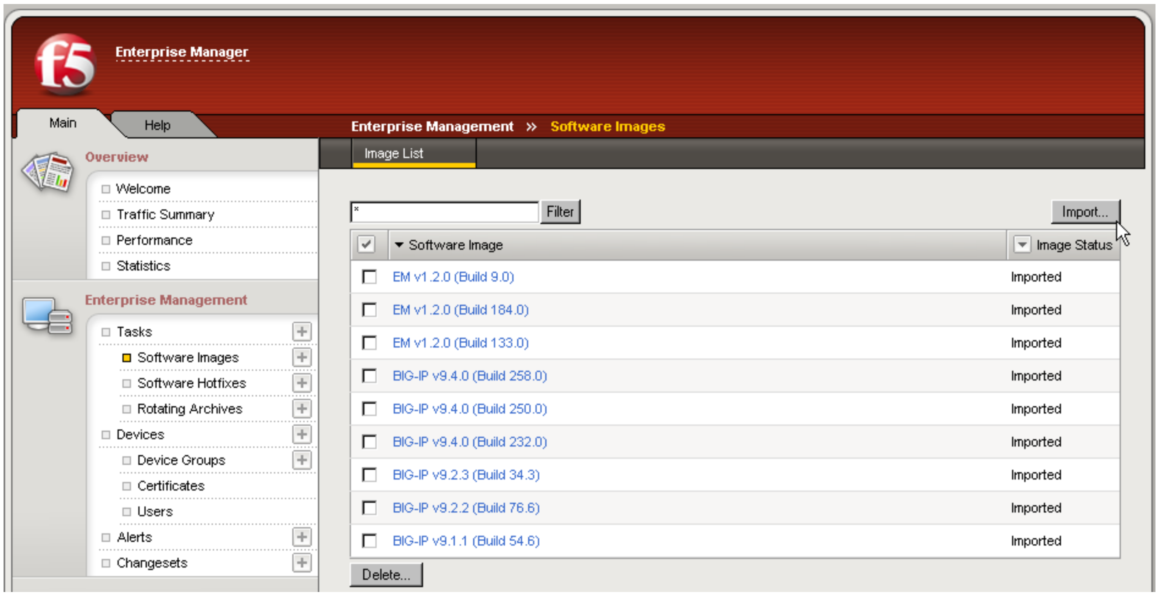
Because Enterprise Manager uses the TMOS platform, like other F5 Networks Application Delivery Networking products, Enterprise Manager presents a web-based interface called the Configuration utility that is similar to the one you use when working on a BIG-IP system.

The Enterprise Manager Configuration utility uses a navigation pane and menu bar comparable to those in other F5 Networks products. It also provides screens that have both a consistent look and feel, and consistent functionality across different management areas.

You can use the navigation tabs to access the device management areas and context-sensitive online help. In each management area, you can use the menu bar to select more specific options.

Navigating object list screens

Once you have selected a management area on the Main tab, the object list screen for that management area opens. Object list screens display a list of all running or completed tasks, managed devices, alerts, or software and hotfix images stored in the Enterprise Manager software repository. You can remove objects from a list by checking the box to the left of an object name, and clicking the appropriate button below the list.



Filter: *

☑	Software Image	Image Status
□	EM v1.2.0 (Build 9.0)	Imported
□	EM v1.2.0 (Build 184.0)	Imported
□	EM v1.2.0 (Build 133.0)	Imported
□	BIG-IP v9.4.0 (Build 258.0)	Imported
□	BIG-IP v9.4.0 (Build 250.0)	Imported
□	BIG-IP v9.4.0 (Build 232.0)	Imported
□	BIG-IP v9.2.3 (Build 34.3)	Imported
□	BIG-IP v9.2.2 (Build 76.6)	Imported
□	BIG-IP v9.1.1 (Build 54.6)	Imported

Figure 1.1 *Enterprise Management: Software Images object list screen*

Management screens are a starting point for all device management tasks, and provide a high-level overview of objects that you can centrally manage.

Enterprise Manager uses several types of screens that share common navigation and behavior across different management areas. These screens work similarly wherever you encounter them. Many screens use check boxes and buttons to enable or disable objects or services, or to select objects for deletion.

The tables on many screens are sortable by column. You can click certain column headings to sort the table, enabling you to more easily find objects among a large list. You can find sortable column headings by looking for the sorting arrows next to a column heading (⇕). For example, in the software image list in Figure 1.1, on page 1-9, the software images are sorted in descending order in the Software Image column with the latest version of the software at the top of the list. If you click the Software Image heading, the information in the table re-sorts to show the earliest version of the software available in the software repository.

In certain tables, you can filter objects displayed in the table by a column heading. If you click the Column Filter button (▼), a menu appears to offer filtering options. In the software image list in Figure 1.1, on page 1-9, you can filter the Image Status column. If you click the Column Filter button, you can filter the list to display only software images in a particular state such as Imported, Importing, or Corrupt.

Above the list table on object list screens is a **Filter** box. You can use this box to limit the list so that the object list displays only objects that contain the terms you type in the **Filter** box.

If the object list contains more items than can appear on one page, a paging control appears below the list table. You can use the arrow buttons to move to the next or previous screen, or you can select a specific screen from the drop-down list.

◆ **Tip**

*In the navigation pane you can use the Add button (+) to immediately add a network object to an object list instead of using a button on an object list screen. For example, if you want to import a software image, you can either open the Software Image list screen, then click the **Import** button, or you can click the Add button (+) next to **Software Images** in the navigation pane.*

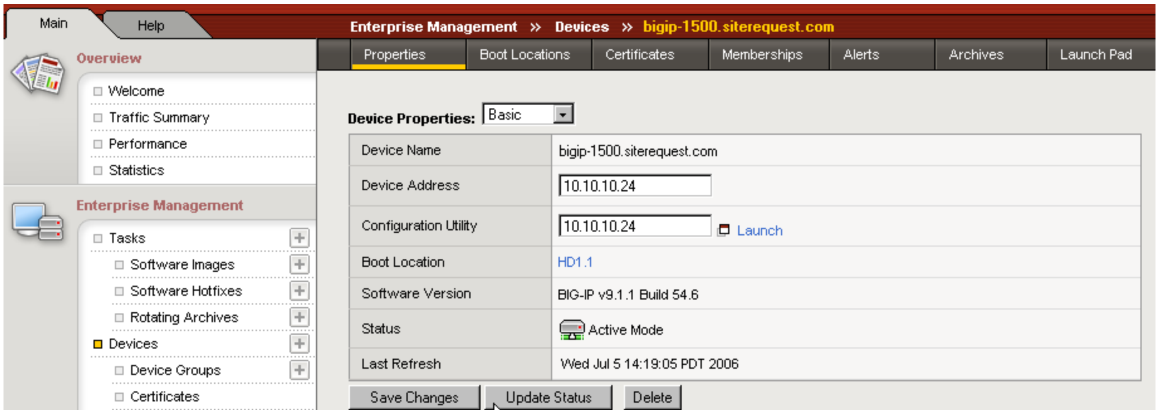
Using general properties screens

If you click the name or IP address of a device, task, alert, or software image on most object list screens, the general properties screen opens. As the title suggests, a general properties screen provides more detailed information about the selected object.

The general properties screen provides an overview of a device, task, alert, or software image and is usually the starting point for more specific management activity on a particular object.

Using the Menu bar

On general properties screens (and screens other than an object list screen), a menu bar appears above the main configuration area. From the menu, you can select options to enable specific management tasks, depending on the device, task, alert, or software image you are working with.



Device Properties: Basic

Device Name	bigip-1500.siterequest.com
Device Address	10.10.10.24
Configuration Utility	10.10.10.24
Boot Location	HD1.1
Software Version	BIG-IP v9.1.1 Build 54.6
Status	Active Mode
Last Refresh	Wed Jul 5 14:19:05 PDT 2006

Figure 1.2 *A device general properties screen with menu bar*

Selecting a menu option opens a screen where you can manage specific details of the currently selected device, task, alert, or software image. Each menu heading opens a particular configuration screen related to the currently selected object.

You will find additional navigation that is specific to the task you are configuring throughout the Enterprise Manager interface. You can find details about these additional navigation methods throughout this guide, as new concepts are introduced.

You can view help specific to a screen, including a definition of screen elements, when you click the Help tab on the navigation pane.

Understanding status icons

Enterprise Manager displays status icons to denote a particular status about devices that it manages.

Status icons that appear on Enterprise Manager screens reflect the connection status between Enterprise Manager and the device as well as the active or standby state of the device. The icons dynamically update as Enterprise Manager polls managed devices, or as an object's state changes. When you move the cursor over the status icon, a tooltip indicates the status and failover state of the device (if the device is reachable).

Icon	Connection Condition
🖥	Active Mode
🖥	Standby Mode
☒	Unreachable

Table 1.5 *Status icons for managed devices*

Both the Active and Standby icons indicate that Enterprise Manager can connect to the device. The Unreachable icon indicates that Enterprise Manager cannot connect to the device. This could be due to many factors, including a disconnected network cable, powered down or rebooting device, or other network issues. For more information about working with device communication see *Setting device communication properties*, on page 4-5.

Finding user assistance

This section describes the Enterprise Manager documentation. It outlines the contents of the Administrator Guide, and explains how we refer to examples, introduce new terms, use cross references, and detail the conventions we use in command syntax. It also explains where to find the release notes and online help, and how to get technical support.

Contents of the Administrator Guide

The ***Enterprise Manager Administrator Guide*** is designed to help you install and configure the Enterprise Manager to manage devices in your enterprise network. The Administrator Guide contains the following chapters:

- **Introducing Enterprise Manager**
  This chapter describes the features and navigation of Enterprise Manager.

- **Installation and Setup**
  This chapter explains setting up the networking environments required to work with Enterprise Manager.

- **Licensing and Configuring the System**
  This chapter explains the software licensing, basic network settings, and management preferences.

- **Discovering and Managing Devices**
  This chapter introduces the initial steps in centrally managing the devices in the network.

- **Managing UCS Archives**
  This chapter explains how Enterprise Manager can store and manage archived device configurations.

- **Managing Device Configurations**
  This chapter describes the concept of managing device configurations using changesets.

- **Managing Software Images**
  This chapter illustrates the steps required to centrally manage software and hotfix upgrades on managed devices.

- **Managing User Account Data**
  This chapter explains how to manage user access privileges and passwords on multiple devices in the network.

- **Monitoring and Alerting**
  This chapter describes how you can monitor the health of your network devices and how to create custom alerts when specific events occur.

- **Managing Device Certificates**
  This chapter explains how Enterprise Manager monitors certificates on managed devices.

- **Auditing Enterprise Manager System Events**
  This chapter examines the options that you have to track changes made to devices in your network.

◆ **Note**

All references to hardware platforms in this guide refer specifically to systems supplied by F5 Networks, Inc. If your hardware was supplied by another vendor, and you have hardware-related questions, please refer to the documentation from that vendor.

Stylistic conventions

To help you easily identify and understand certain types of information, this documentation uses the following stylistic conventions.

Using the solution examples

All examples in this documentation use only private class IP addresses. When you set up the solutions we describe, you must use IP addresses suitable to your own network in place of our sample IP addresses.

Identifying new terms

When we first define a new term, the term is shown in bold italic text. For example, a ***managed device*** is an F5 Networks device that is managed by Enterprise Manager.

Identifying references to objects, names, and commands

We apply bold text to a variety of items to help you easily pick them out of a block of text. These items include web addresses, IP addresses, browser screen controls, and portions of commands, such as variables and keywords. For example, to discover devices requires that you include at least one **<ip_address>** or an **<ip_subnet>** variable.

Identifying references to other documents

We use italic text to denote a reference to another document. In references where we provide the name of a book as well as a specific chapter or section in the book, we show the book name in bold, italic text, and the chapter/section name in italic text to help quickly differentiate the two. For example, you can find information about deploying a hotfix to multiple devices in the ***Enterprise Manager Administrator Guide***, Chapter 7, *Managing Software Images*.

Identifying command syntax

We show actual, complete commands in bold Courier text. Note that we do not include the corresponding screen prompt, unless the command is shown in a figure that depicts an entire command line screen.

Table 1.6 explains additional special conventions used in command line syntax.

Item in text	Description
\	Continue to the next line without typing a line break.
< >	You enter text for the enclosed item. For example, if the command has **<your name>**, type your name.
|	Separates parts of a command.
[ ]	Syntax inside the brackets is optional.
...	Indicates that you can type a series of items.

Table 1.6 *Command line conventions used in this manual*

Finding documentation and technical support resources

The ***Enterprise Manager Administrator Guide*** provides simple instructions for quick, basic configuration, and also provides detailed information about more advanced features and tools.

You can find comprehensive technical documentation using the following resources:

- **Enterprise Manager Administrator Guide**
  The ***Enterprise Manager Administrator Guide*** introduces the concepts of managed devices, software image management, configuration management, and custom alerting. For example, you can learn how to add a variety of devices to the device list, create device groups, and deploy software upgrades to different groups of devices.
- **Platform Guide: Enterprise Manager 500** or **Platform Guide: Enterprise Manager 3000**
  The ***Platform Guide: Enterprise Manager 500*** or ***Platform Guide: Enterprise Manager 3000*** each includes information about the Enterprise Manager system hardware platform. They also contain important environmental warnings.
- **Release notes**
  Release notes for the Enterprise Manager are available in HTML format on the F5 Networks Technical Support web site, **http://tech.f5.com**. The release note contains the latest information for the current version, including a list of new features and enhancements, a list of fixes, and a list of known issues.

- **Enterprise Manager Quick Start Instructions**
  The Enterprise Manager hardware includes the printed ***Enterprise Manager Quick Start Instructions***. This document provides basic instructions for a quick set up and initial configuration of the Enterprise Manager system.

- **Online help for Enterprise Manager features**
  Enterprise Manager has online help for each screen. On the navigation pane, click the help tab to receive context-sensitive user assistance.

- **Technical support through the World Wide Web**
  The F5 Networks Technical Support web site, **http://tech.f5.com**, provides the latest release notes, technical notes, answers to frequently asked questions, updates for the Administrator Guide (in PDF format), and the Ask F5^{SM} natural language question and answer engine.

◆ **Important**

*Procedures and examples described in the **Enterprise Manager Administrator Guide** and in the online help assume that the user is an administrator-level user with full access privileges to the Enterprise Manager device. The Enterprise Manager system logs on to managed devices using an administrator-level account, so all users with administrator-level access to Enterprise Manager can perform the high-level management tasks described in this document on devices in the network through the Enterprise Manager interface.*

2

Installation and Setup

- Installing Enterprise Manager in the network
- Working with different network configurations

Installing Enterprise Manager in the network

Incorporating Enterprise Manager into your network is as simple as adding any F5 Networks device. You can use the ***Enterprise Manager Quick Start Instructions*** included with the system to get started with the physical installation and initial network configuration. See Chapter 3, *Licensing and Configuring the System* for detailed information on licensing, platform configuration, and basic default settings.

This chapter describes how to configure devices in your network to work with Enterprise Manager.

Depending on your network topology, you may have to configure a SNAT, NAT, or multiple virtual servers external to the Enterprise Manager device in order to ensure proper communication between Enterprise Manager and managed devices.

Choosing a network topology

Enterprise Manager is designed to work within virtually any network configuration and can adapt to the management configuration you already use for F5 Networks devices in your network. You connect Enterprise Manager to devices in the network through the interfaces available on both the Enterprise Manager device and the F5 Networks devices in the network. The ***interfaces*** on the Enterprise Manager or other F5 Networks system are the physical ports that you use to connect each system to other devices on the network.

◆ **Note**

Throughout this guide, the term interface refers to the physical ports on the Enterprise Manager or BIG-IP system.

Enterprise Manager can work with the network topology of your choice in two distinct ways:

- You can use a management network through the management interface (MGMT port) on both the Enterprise Manager device and each managed device for enterprise management communications.
- You can use a self IP address through a TMM switch interface on both the Enterprise Manager device and each managed device for enterprise management communications.

◆ **Important**

For Enterprise Manager to work properly, you must enable two-way communication between the Enterprise Manager device and each managed device. Enterprise Manager communicates with managed devices using port ***443****, and requests a response from each device through this port.*

Using the management interface

We recommend that, whenever possible, you create a management network that you administer through the management interface on each managed device and the Enterprise Manager system. The ***management interface*** is a special port on the BIG-IP system, used for managing administrative traffic. Named MGMT, the management interface does not forward user application traffic, such as traffic slated for load balancing.

This type of configuration requires the least amount of additional configuration when you discover and begin to manage devices. Additionally, when you add new devices to a management network, you do not need to perform extensive configuration to manage the new device with Enterprise Manager when you add a new device to the network, as long as all devices on the management network exist on the same subnet.

This type of configuration keeps traffic management communication separate from enterprise management communications, and does not require you to dedicate a TMM switch interface to device management traffic.

Using a TMM switch interface for device management

You can use Enterprise Manager to communicate with managed devices through one of the managed device's TMM switch interfaces. ***TMM switch interfaces*** are those interfaces that the BIG-IP system uses to send or receive application traffic, that is, traffic slated for load balancing. However, this type of network setup frequently requires some additional configuration in order to maintain a two-way connection between Enterprise Manager and managed devices.

If you want to connect to a managed device through a TMM switch interface, you must associate the interface on the managed device with a VLAN and a self IP address so that Enterprise Manager can recognize and connect to the device in the network (through its own MGMT interface or through a self IP address and VLAN that you configure on Enterprise Manager). If you choose to use a TMM switch interface on managed devices, Enterprise Manager uses this interface for sending software upgrades to the managed device and we recommend that you do not use the interface for managing traffic. When you are deciding on which interface to use for the connection to Enterprise Manager, we recommend that you use the same interface that you currently use for device administration.

For information on how to configure and use the management interface, see Chapter 4, *Configuring the BIG-IP Platform and General Properties* in the ***BIG-IP® Network and System Management Guide.***

Working with different network configurations

When you initially configured the F5 Networks devices in your network, you made a decision to administer each device through the MGMT interface or through a TMM switch interface. Your previous device management choice generally determines how you configure Enterprise Manager to work as your enterprise management system, but you can use this opportunity to build separate management networks that will keep device administration separate from traffic management.

Because Enterprise Manager communicates with managed devices on a regular interval, you must keep a two-way communication open between Enterprise Manager and managed devices. On each managed device, you must ensure that device management traffic does not interfere with traffic management activity.

Whether this means configuring your managed devices to use virtual servers to communicate through a multi-tiered device configuration or, configuring a firewall NAT to translate IP addresses depends on your existing network topology.

The following sections outline three of the most common network topology scenarios:

- A network using a NAT to facilitate address translation
- A network set up in a tiered configuration with multiple BIG-IP systems.
- A tiered network configuration using a SNAT to communicate with Enterprise Manager

Enterprise Manager can work well in any of these configurations, or in configurations that combine some of the scenarios described.

In many cases, you may have already completed some of the required tasks while configuring your network for traffic management.

Working with a NAT configuration

If you use a firewall with a NAT to translate IP addresses, you must ensure that the NAT is properly configured for Enterprise Manager to use for device management. Usually, if your NAT works well for your traffic management, you may not have to perform any additional configuration other than ensuring that Enterprise Manager recognizes devices in the network at the IP addresses you expect, and that each device can properly communicate back to Enterprise Manager.

In this common configuration, a NAT translates the IP addresses of managed devices through the firewall into addresses that Enterprise Manager can use to talk to a managed device.

After you discover devices in this kind of configuration, you must configure the device general properties so that each managed device can initiate communications with Enterprise Manager.

◆ **Tip**

If you use a NAT in your network, you may want to take notes of translated addresses for reference when discovering and managing devices with Enterprise Manager.

Configuring your devices to work with a NAT

To open a two-way connection between each managed device and Enterprise Manager, ensure that you perform the following tasks:

- Configure a TMM switch interface or the MGMT interface on each managed device to accept and send communications on port **443**.
- If you choose to use TMM switch interfaces, on each of these interfaces, configure a self IP address that the managed device should use for device management activity such as receiving software or hotfix upgrades. ***Note****: You do not need to configure a self IP address on the managed device if you connect to the MGMT interface on the managed device.*
- Configure the NAT so that the management IP address that Enterprise Manager uses to connect to each device maps to the MGMT interface on each managed device, or to the management self IP address you defined for a TMM switch interface.
- Discover the devices using the IP addresses translated by the NAT. See *Discovering devices*, on page 4-2 for detailed information on discovering devices.
- Configure the general properties of newly discovered devices so that each managed device can initiate communications to the Enterprise Manager device. See *Setting device communication properties*, on page 4-5 for instructions on how to set device communication properties.
- Test the two way connection by opening a Telnet session on the managed device to test communication over port **443** to the Enterprise Manager system. See *Testing communications between devices and Enterprise Manager,* on page 4-6 for more information on working with the connection between Enterprise Manager and managed devices.s

Working with a tiered network configuration

Another common network deployment involves placing multiple F5 Networks devices behind a BIG-IP system in order to load balance requests to multiple devices. For example, if you use ten BIG-IP systems to load balance requests to multiple servers, you may add another tier to the load balancing by using another BIG-IP system to load balance requests to the ten BIG-IP systems.

In this configuration, virtual servers provide a route through the multiple tiers for network requests. For Enterprise Manager to work properly in this configuration, you must set up multiple virtual servers on the top traffic management tier to properly send device management traffic through each tier. Additionally, you must configure one virtual server on each managed device exclusively for enterprise management traffic.

Like a NAT in the previous example, you should use the BIG-IP system that balances requests to the other systems to translate enterprise management traffic through virtual server addresses. Alternately, you can configure a SNAT on the top tier BIG-IP system to send communications back to Enterprise Manager. See *Working with a tiered configuration using a SNAT*, on page 2-6 for more information on using a SNAT in a tiered configuration.

On the top tier device in your tiered configuration, you must configure two virtual servers, each using port **443**. Enterprise Manager uses the first virtual server to communicate to the managed devices on the lower tier, and the managed devices use the second virtual server to initiate communication with Enterprise Manager.

When you discover devices, you should discover the virtual server addresses that you configured for device management. After you discover devices, you must configure the device general properties on the Enterprise Manager system so that managed devices can properly communicate with the Enterprise Manager system.

Configuring your devices to work in a tiered configuration

To open a two-way connection between each managed device and Enterprise Manager in a tiered network configuration, ensure that you perform the following tasks:

- Configure a virtual server on the top tier BIG-IP system to accept communications such as software or hotfix upgrades from Enterprise Manager on port **443**.
- Configure a virtual server on the top tier BIG-IP system to send communications to Enterprise Manager on port **443**.
- If you use the TMM switch interfaces, configure a VLAN and self IP address on each lower tier managed device to receive communications (translated through the top tier system) from the Enterprise Manager device on port **443**.
- If you use the TMM switch interfaces, configure an additional VLAN and self IP address on each lower tier managed device to send communications (translated through the top tier system) to Enterprise Manager on port **443**.
- Discover the devices using the first set of virtual server IP addresses that you configured for managed devices to receive communications from Enterprise Manager. See *Discovering devices*, on page 4-2 for detailed information on discovering devices.

- Configure the general properties of newly discovered devices so that each managed device can initiate communications to the Enterprise Manager device. See *Setting device communication properties*, on page 4-5 for instructions on how to set device communication properties.

Working with a tiered configuration using a SNAT

Another network configuration involves using the tiered approach described in the previous section in addition to using a SNAT for secure address translation on the top tier BIG-IP system.

In this configuration, virtual servers provide a route through the top tier for Enterprise Manager to contact managed devices, while a SNAT allows the managed device to contact the Enterprise Manager system. For Enterprise Manager to work properly in this configuration, you must set up multiple virtual servers and configure a SNAT to properly translate the IP addresses of these virtual servers for outbound communications to the Enterprise Manager system.

Configuring your devices to work with a tiered network using SNAT address translation

To open a two-way connection between each managed device and Enterprise Manager in a tiered network configuration with a SNAT, ensure that you perform the following tasks:

- Configure a virtual server on the top tier BIG-IP system to accept communications such as software or hotfix upgrades, from Enterprise Manager on port **443**.
- Configure a SNAT on the top tier BIG-IP system to translate the IP address from the virtual servers on the managed device to the Enterprise Manager system.
- If you use the TMM switch interfaces, configure a VLAN and self IP address on each lower-tier managed device to receive communications (translated through the top tier system) from the Enterprise Manager device on port **443**.
- Discover the devices using the first set of virtual server IP addresses that you configured for managed devices to receive communications from Enterprise Manager. See *Discovering devices*, on page 4-2 for detailed information on discovering devices.
- Configure the general properties of newly discovered devices so that each managed device can initiate communications to the Enterprise Manager device. See *Setting device communication properties*, on page 4-5 for instructions on how to set device communication properties.

3

Licensing and Configuring the System

- Setting up Enterprise Manager for the first time
- Licensing the Enterprise Manager software using the Configuration utility
- Creating the platform management configuration
- Rerunning the Setup utility
- Configuring the enterprise management network
- Configuring Enterprise Manager defaults and preferences
- Managing user accounts

Setting up Enterprise Manager for the first time

Enterprise Manager fits into your existing network configuration in a similar manner to your other F5 Networks devices. The ***Enterprise Manager Quick Start Instructions*** included with the device introduce the basic steps required to set up and start working with the Enterprise Manager system.

This chapter details the process of licensing and configuring the system, including setting up management network defaults, default self IPs and VLANs, and setting general preferences for working with Enterprise Manager.

This chapter assumes that you have previously set up, licensed, and configured one or more BIG-IP systems in your network, and that you have connected the Enterprise Manager system to a management workstation or network.

The initial licensing, platform setup, and network configuration procedures in the following sections are based on the procedures described in the ***Installation, Licensing, and Upgrades for BIG-IP® Systems*** guide. Consult that guide if you require additional information not described in this chapter.

Licensing the Enterprise Manager software using the Configuration utility

To activate the license for the system, you must have a base registration key. The base registration key is a 33-character string that lets the license server know which F5 products you are entitled to license. If you do not already have a base registration key, you can obtain one from the sales group (**http://www.f5.com**).

If the system is not yet licensed, the Configuration utility prompts you to enter the base registration key. Certain systems may require you to enter keys for additional modules in the **Add-On Registration Key List** box.

After you configure an IP address, net mask, and gateway on the management port, you can access the Configuration utility (graphical user interface) through the management port.

For more information on how to work with a console connection, and how to configure network settings on the MGMT interface, see the *Connecting a Management Workstation or Network* chapter in the ***Installation, Licensing, and Upgrades for BIG-IP® Systems*** guide.

To license the system using the Configuration utility

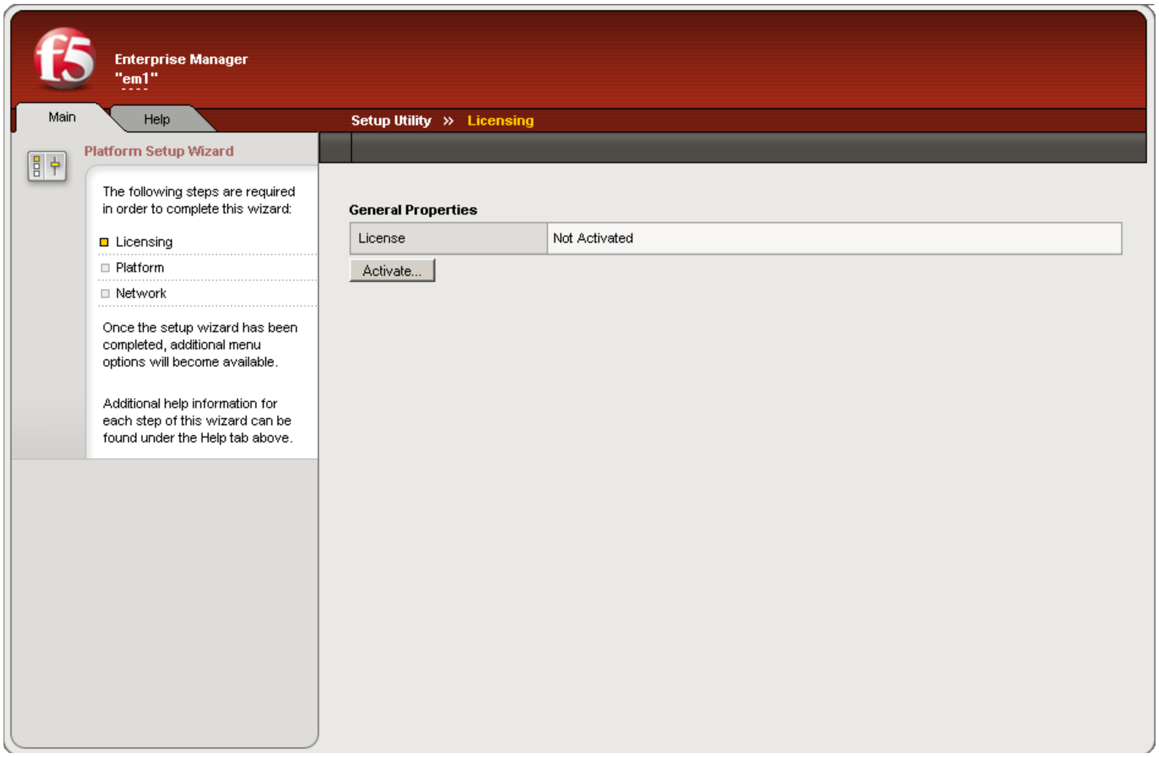
1. Open a web browser on a work station attached to the network on which you configured the management port.
2. Type the following URL in the browser, where **<IP address>** is the address you configured for the management port (MGMT):

   ```
   https://<IP address>/
   ```

3. At the password prompt, type the user name **admin** and the password **admin**, and click **OK**.

   The Licensing screen of the Configuration utility opens (Figure 3.1). The Setup utility appears the first time you run the Configuration utility.

4. To begin the licensing process, click the **Activate** button. Follow the on-screen prompts to license the system. For additional information, click the Help tab.



The following steps are required in order to complete this wizard:

- ■ Licensing
- □ Platform
- □ Network

Once the setup wizard has been completed, additional menu options will become available.

Additional help information for each step of this wizard can be found under the Help tab above.

General Properties

License	Not Activated

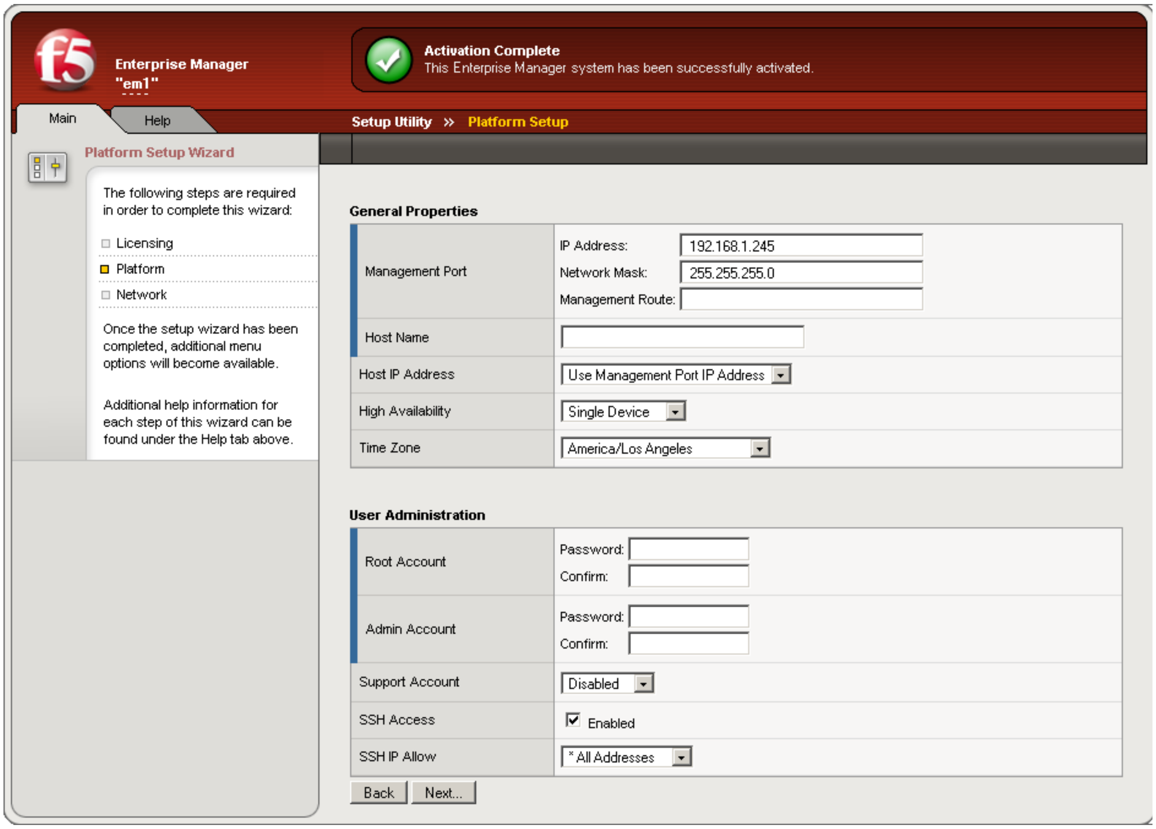
Figure 3.1 The Licensing screen in the Setup utility

Note that you can update the license at any time by using the Licensing option that is available in the **System** area on the Main tab.

Creating the platform management configuration

After you have activated the license on the system, the Configuration utility prompts you for the basic configuration information for managing the system (Figure 3.2). This required information includes the following settings.

- Management interface settings such as the IP address, netmask, and default gateway
- Host name and IP address
- High availability settings
- Time zone settings
- User account settings, such as the root and admin passwords
- Support access
- SSH access



Activation Complete
This Enterprise Manager system has been successfully activated.

Platform Setup Wizard

The following steps are required in order to complete this wizard:

- □ Licensing
- ■ Platform
- □ Network

Once the setup wizard has been completed, additional menu options will become available.

Additional help information for each step of this wizard can be found under the Help tab above.

General Properties

Management Port	IP Address: 192.168.1.245 Network Mask: 255.255.255.0 Management Route:
Host Name	
Host IP Address	Use Management Port IP Address
High Availability	Single Device
Time Zone	America/Los Angeles

User Administration

Root Account	Password: Confirm:
Admin Account	Password: Confirm:
Support Account	Disabled
SSH Access	☑ Enabled
SSH IP Allow	* All Addresses

Figure 3.2 *The Platform Setup screen*

Platform setup screen settings

Each heading in this section provides a basic description to assist you in choosing settings on the Platform Setup screen.

Management port

You can specify an IP address for the management (administrative) port. If you set the management interface IP address using the LCD screen that is available on some platforms, you do not need to configure this setting. You can also specify a network mask for the administrative port's IP address and the IP address of the default route for the management port.

Host name

You must enter a fully qualified domain name (FQDN) for the system. Only letters, numbers, and the characters dash (**-**) and period (**.**) are allowed.

Host IP address

The host IP address is the IP address that you want to associate with the host name:

- Select **Use Management Port IP Address** to associate the host name with the management port's IP address. This is the default setting.
- Select **Custom Host IP Address** to type an IP address other than the management port's IP address.

High availability

A high availability system consists of two units that share configuration information:

- Select **Single Device** if the system is not a unit in a high availability system.
- Select **Redundant Pair** if the system is a unit in a high availability system.

◆ **WARNING**

Enterprise Manager high availability systems do not support many of the high availability features of a BIG-IP system. The main function of Enterprise Manager high availability is to provide an updated back up of the configuration of the active Enterprise Manager system. For more information on how Enterprise Manager works in a high availability configuration, see ***Configuring Enterprise Manager as a high availability system****, on page 3-8.*

Unit ID

Select **1** or **2** to identify the system's unit ID number in the redundant system. The default unit ID number is **1**. If this is the first unit in the redundant system, use the default. When you configure the second unit in the system, type **2**.

◆ **Note**

If the device is not a part of a high availability system, you do not need to specify the unit ID.

Time zone

Select the time zone that most closely represents the location of the system. This ensures that the clock for the Enterprise Manager system is set correctly, and that dates and times recorded in log files correspond to the time zone of the system administrator. Scroll through the list to find the time zone at your location.

Root account

The root account provides access to this system from the console.

- In the **Password** box, type the password for the built-in account, **root**.
- In the **Confirm** box, retype the password that you typed in the **Password** box.
  If you mistype the password confirmation, the system prompts you to retype both entries.

Admin account

The admin account provides access to the system through a browser.

- Type the password for the built-in account, **admin**.
- In the **Confirm** box, retype the password that you typed in the **Password** box.
  If you mistype the password confirmation, the system asks you to retype both entries.

Support account

This setting enables the built-in account, **support**, for access to the system's command line interface and browser interface. If you activate the account, you must also supply a password and password confirmation. The technical support staff uses the support account to analyze the system if you need assistance with troubleshooting issues.

SSH access

Check the **Enabled** box if you want to activate SSH access to the Enterprise Manager system.

SSH IP allow range

If you have enabled SSH access, you can specify the IP address or address range for other systems that can use SSH to communicate with the system. To grant unrestricted SSH access to all IP addresses select ***All Addresses**. To specify a range, select **Specify Range**, and then type an address or address range in the box, to restrict SSH access to a block of IP addresses. For example, to restrict access to only systems on the **192.168.0.0** network, type **192.168.*.***.

Rerunning the Setup utility

Once you have configured the system, if you need to reconfigure any system settings, you can run the Setup portion of the Configuration utility again by clicking the **Run the Setup utility** link on the Welcome screen. As you proceed through the Setup utility, click the Help tab for information about the settings on each screen.

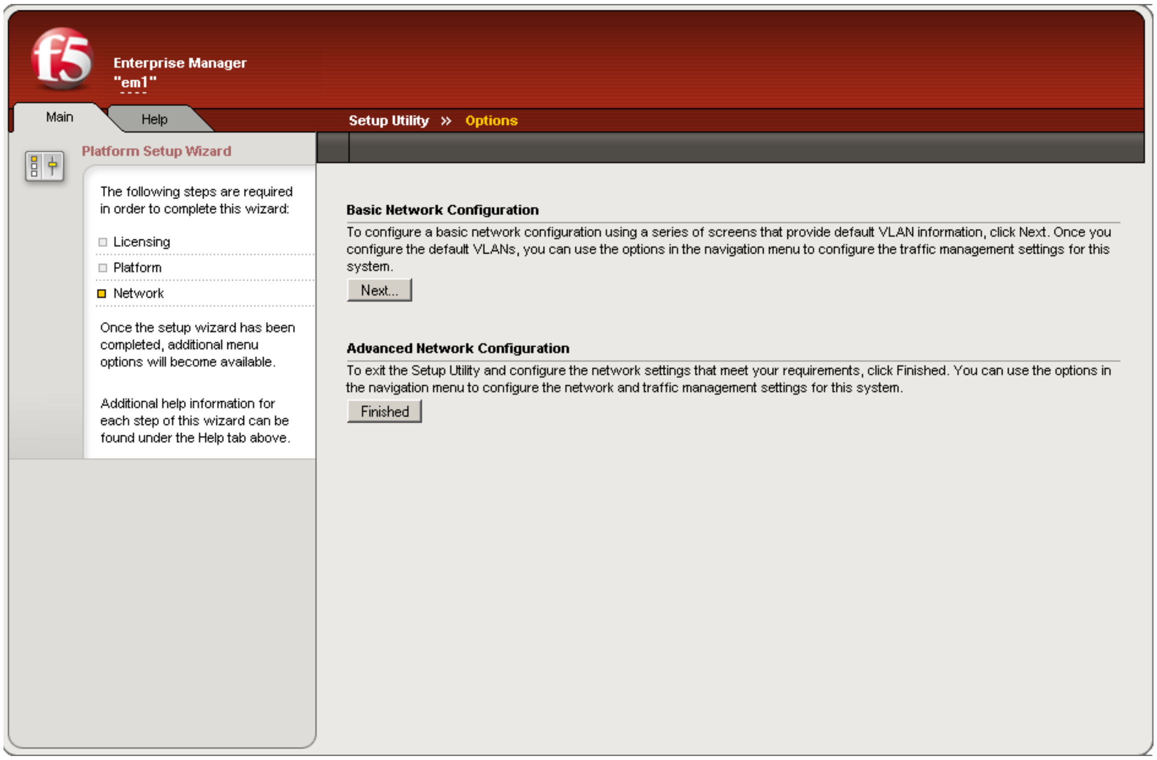
Configuring the enterprise management network

Once you have licensed the system, and configured the basic management system settings, the Options screen opens in the Configuration utility. The Options screen, as shown in Figure 3.3, contains two options for creating the enterprise management configuration.

- **Basic Network Configuration**
  Click the **Next** button to start the basic network configuration wizard. This wizard guides you through a basic network configuration that includes an internal and external VLAN and interface configuration.
- **Advanced Network Configuration**
  If you want to create a custom management configuration, click the **Finished** button to exit to the Main tab. Select this option if you want to create a custom VLAN configuration. If you choose this option, after you click the **Finished** button, you should click the **Network** option on the Main tab.

◆ **Tip**

Although the Advanced option is available, you do not need to create an advanced network configuration for enterprise management purposes.



The following steps are required in order to complete this wizard:

□ Licensing

□ Platform

□ Network

Once the setup wizard has been completed, additional menu options will become available.

Additional help information for each step of this wizard can be found under the Help tab above.

Basic Network Configuration

To configure a basic network configuration using a series of screens that provide default VLAN information, click Next. Once you configure the default VLANs, you can use the options in the navigation menu to configure the traffic management settings for this system.

Advanced Network Configuration

To exit the Setup Utility and configure the network settings that meet your requirements, click Finished. You can use the options in the navigation menu to configure the network and traffic management settings for this system.

Figure 3.3 *The Options screen for configuring the enterprise management network*

Using the Basic Network Configuration wizard

You can use the Basic Configuration wizard to configure two default VLANs for the system, **internal** and **external**. Note that you can update the network configuration at any time by using the options that are available under the **Network** or **System** sections on the Main tab.

Consult the online help if you need detailed information about specific settings when configuring the default VLANs and self IPs.

Configuring Enterprise Manager defaults and preferences

To successfully manage devices, you must set up Enterprise Manager preferences. These preferences determine how Enterprise Manager handles such features as high availability, software management, device configuration archiving, certificate management, alerting, logging, and user management.

Configuring Enterprise Manager as a high availability system

You can configure Enterprise Manager as a part of a high availability system, but the high availability features are not the same as a BIG-IP system high availability that you may be familiar with. Enterprise Manager high availability mainly provides a ***warm backup*** of an active system. A ***warm backup*** is a system that duplicates the configuration information of its peer device, and can perform all of the functions of its peer, but requires manual intervention to maintain the integrity of the backup configuration information.

The primary advantage of an Enterprise Manager high availability system is that you can maintain an active-standby configuration where you back up the Enterprise Manager configuration, including device, alert, archive, certificate, and software repository information. This ensures that once you manage multiple devices with Enterprise Manager, you can maintain a back up of all the network management information stored in the Enterprise Manager database as long as you run regular ConfigSync tasks whenever you change the Enterprise Manager configuration.

You can manage the ConfigSync task on the Enterprise Manager device in the same way that you manage high availability managed devices. See *Working with high availability systems*, on page 4-6 for more information.

Additionally, you can monitor the sync status of the Enterprise Manager pair from the device’s general properties screen, or by looking at the status displayed in the upper left corner of the screen above the navigation pane.

◆ **Tip**

To maintain the best possible backup capabilities of an Enterprise Manager pair, we recommend that you start a ConfigSync task after major configuration changes.

Understanding the Enterprise Manager high availability differences

There are four main differences between high availability on an Enterprise Manager system and a BIG-IP system. The first is that Enterprise Manager can only use an active-standby configuration for high availability. The second is that the failover function on Enterprise Manager does not work in the same way that it does on a BIG-IP system. The third is that the

ConfigSync process requires much more time on an Enterprise Manager system. Finally, you cannot make configuration changes on an Enterprise Manager system in standby mode.

Setting the high availability configuration

When you configure the settings on the Platform Setup screen during the initial system setup, you can specify the type of high availability system, if appropriate. If you use Enterprise Manager in a high availability configuration, you can only use the active-standby configuration, and not the active-active configuration.

Working with the failover function

In an Enterprise Manager high availability system, if the active device fails over, the standby device becomes active. However, if any processes are running, such as a software installation or device archiving task, this process is not continued by the new active device.

Because the Enterprise Manager system is designed to manage enterprise devices instead of traffic, it cannot synchronize user-configured or scheduled tasks in real time. Instead, for a failover to be successful, Enterprise Manager requires a ConfigSync operation after each major configuration change.

After a failover, the newly active system maintains the last known configuration before any user-initiated or scheduled task if the systems were properly synchronized. If a failover occurs during a running task, you must reconfigure and re-start the task.

Working with the ConfigSync process

The Enterprise Manager database contains considerably more configuration data than a typical BIG-IP system because it stores configuration data for a large number of devices. The main effect of this is that a ConfigSync process requires much more time than a similar process on a typical BIG-IP system. Also, when you start a ConfigSync task for Enterprise Manager, the system may report that the task is complete, although it is still running.

To ensure that the configurations are synchronized after you start a ConfigSync task, you should check the status of devices on the target device where you are copying the configuration. If a Maintenance Task appears in the task list, then the ConfigSync task is not complete.

Additionally in a failover scenario, if a task is running, the task does not continue when a standby peer becomes the active peer. If you encounter this situation, you should re-configure the task and restart it.

Making configuration changes on a standby system

When an Enterprise Manager system is in standby mode, you cannot make configuration changes such as adding devices, importing software, or configuring alerts on the standby device. If you attempt to make changes on a system in standby mode, you receive an error.

To ensure that you do not initiate tasks on a standby system, check for an **Active** or **Standby** status message in the upper left corner of the screen.

Configuring initial settings for an Enterprise Manager pair

If you choose to configure two Enterprise Manager systems in a high availability configuration, you must run an initial configuration synchronization in order for the systems to work properly. Additionally, you must specify the same password for the **admin** user on each device in the redundant configuration.

To initialize an Enterprise Manager pair

This procedure describes the basic steps necessary to set up an Enterprise Manager high availability system. To configure these settings, you must have already configured two Enterprise Manager systems and set each device as a **Redundant Pair** on the Platform Setup screen in the Setup utility.

1. On the Main tab of the Navigation pane, expand **System** and click **High Availability**.
   The System Redundancy Properties screen opens.

2. For the **Primary Failover Address**, specify in the appropriate boxes, the **Self** and **Peer** IP addresses for each Enterprise Manager system.

3. In the **Redundancy State Preference** list, select whether you prefer the current device to be the Active or Standby system. Select **None**, if you have no preference.

4. In the **Network Failover** box, if you want the standby system to use the network to check the state of the active system, check the Select box to enable network failover detection.

5. Click **Update** to save your changes.

6. On the menu bar, click **ConfigSync**.
   The System ConfigSync screen opens.

7. In the **Configuration** list above the table, select **Advanced**.
   The table changes to show additional options.

8. In the **ConfigSync User** list, select a user account that has Administrator privileges and can perform the ConfigSync operation.
   Important: *The user account and password must be the same on both units in the redundant system.*

9. In the **Detect ConfigSync Status** box, check the Select box to enable this unit to regularly compare its configuration status with that of its peer.

10. In the Synchronize row, click either **Synchronize TO Peer** or **Synchronize FROM Peer** to perform an initial configuration synchronization.

Changing the device refresh interval

When you start up Enterprise Manager, one device option is already set by default: the rate at which Enterprise Manager requests updated metrics from each managed device. When you discover devices and add them to the device list, Enterprise Manager refreshes the device information at a default interval of once every 10 minutes. You can reduce the amount of management traffic by increasing the interval, or you can more closely monitor the state of devices by decreasing the interval. For more information about discovering and managing devices, see Chapter 4, *Discovering and Managing Devices*.

To change the device refresh interval

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Devices**.
   The Device List screen opens.
2. On the menu bar, click **Options**.
   The Device Options screen opens.
3. In the Device Communication table, in the **Refresh Interval** box, change the value to adjust the regular interval at which Enterprise Manager requests new information from each managed device.
4. Click **Save Changes**.

◆ **Tip**

*If you need immediately updated device information at any time, you can refresh device information using the **Update Status** button for any number of devices that you select on the Device List screen, or on an individual device General Properties screen.*

Changing the device archive options

Enterprise Manager provides a secure location to store device configuration archives for all managed devices. You can set up a rotating schedule for archiving, and you can save multiple archives in the Enterprise Manager database.

When you first start Enterprise Manager, the number of rotating archives or pinned archives Enterprise Manager can store in its database is set by default. Enterprise Manager is initially set to store up to 10 rotating device archives and 10 saved, or pinned, archives per device in its database.

Enterprise Manager manages rotating archives in its database in a first in, first out manner. That is, once the database reaches the maximum number or archives, it deletes the oldest archive in the rotating archive list.

Conversely, pinned archives require manual intervention once Enterprise Manager reaches the maximum. When a user attempts to create a pinned archive that exceeds the limit, the system warns that it cannot create a new pinned archive until the users deletes at least one from the current list or increases the maximum limit.

If you want to maintain more device configuration for backup and restore flexibility, you can increase this value as needed, but the number of stored archives can affect the disk space on the Enterprise Manager device. For detailed information about how Enterprise Manager works with device archives, including setting up rotating archive schedules or saving multiple configuration archives, see Chapter 5, *Managing UCS Archives*.

To change the device configuration archive options

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Devices**.
   The Device List screen opens.
2. On the menu bar, click **Options**.
   The Device Options screen opens.
3. In the Configuration Archives table, in either the **Maximum Rotating Archives** box, or the **Maximum Pinned Archives** box, change the maximum number of archives that Enterprise Manager saves in its database.
4. Click **Save Changes**.

◆ **Note**

If you reduce the maximum number of rotating archives on a system where the number of archives exceeds the new value, the system deletes the oldest archives to reach the new limit. If you set a lower pinned archive limit, the system does not automatically delete pinned archives. You must delete pinned archives manually.

Setting alerting system options

Because Enterprise Manager can send email alerts, log events in a remote syslog file, or send SNMP traps, you should configure these defaults before enabling alert instances that use any of these options. Additionally, Enterprise Manager can log each alert event in the alert history. Depending on how many alerts you need to track over time, you can control the maximum size of this alert log.

For information on how the alerting process works in Enterprise Manager and how to configure alerts for managed devices in the network, see Chapter 9, *Monitoring and Alerting*.

To set alert defaults

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Alerts**.
   The Device Alerts screen opens.
2. On the menu bar, click **Options**.
   The Alert Options screen opens.
3. In the **Email Recipient** box, type the email address of the user or alias that you want to set as the default mail recipient for an alert.
4. In the **Syslog Server Address** box, type the IP address of the remote server that you want to set as the default if you opt to log an event in a server's syslog file.
5. In the Alert History table, in the **Maximum History Entries** box, type the maximum number of alerts that you want logged in the Alert History.
   If the alert history reaches the limit you set, the system deletes the oldest entries to create room for newer entries.
6. Click **Save Changes**.

◆ **Tip**

If you do not want to use the email or syslog defaults for a particular alert, you have the option to specify a unique email address or syslog server address when you create a new alert.

Setting up SNMP options

If you use the alerting features of Enterprise Manager, you can send SNMP traps to a remote SNMP server. ***Simple Network Management Protocol (SNMP)*** is an industry-standard protocol that gives a standard SNMP management system the ability to remotely manage a device on the network. The SNMP versions that the Enterprise Manager system supports are: SNMP v1, SNMP v2c, and SNMP v3.

Enterprise Manager works with SNMP is the same way that a BIG-IP system works with SNMP. If you elect to send SNMP traps when configuring alerts, you must configure the SNMP agent and SNMP client access to the Enterprise Management system.

Because the Enterprise Manager system shares the same operating system as a BIG-IP system, you can configure SNMP on the Enterprise Manager system in the same way that you do on a BIG-IP system. See the *Configuring SNMP* chapter in the ***BIG-IP® Network and System Management Guide*** for detailed information on how to configure SNMP information.

◆ **Tip**

The System section on the Main tab of the navigation pane contains most of the same configuration options as it does for a BIG-IP system.

Configuring internal email options

When you configure alerts, you have the option for the system to send email messages to a user that you specify when the alert is triggered. In order to enable this feature, you must configure the Enterprise Manager system to deliver locally generated email messages.

To configure Enterprise Manager to deliver locally generated email messages complete the following steps:

- Ensure that the **postfix** service is running.
- Configure DNS on the system.
- Verify DNS resolution.
- Configure email notification.

To configure internal email requires **root** access to the command console and Administrator privileges for the Configuration utility.

To enable the postfix service

By default, the **postfix** mail server service is enabled when you install the Enterprise Manager software, but you may need to confirm this.

1. On the Main tab of the navigation pane, expand **System** and click **Services**.
   The System Services screen opens displaying the available system services and how long each service has been running.
2. Confirm that the postfix service is running by at the message in the History column next to the **postfix** service.
3. If you need to start or restart the postfix service, check the Select box next to the postfix service, and click the **Start** or **Restart** button below the list.

To configure DNS

1. On the Main tab of the navigation pane, expand **System** and click **General Properties**.
   The System: General Properties screen opens.
2. From the Device menu, choose DNS.
   The System: DNS screen opens.
3. In the **DNS Lookup Server List** section, in the **Address** box, type the IP address of your DNS server(s).
4. Click **Add**.
   The address moves to the box below the **Add** button.

5. Click the **Update** button.

Verify DNS resolution

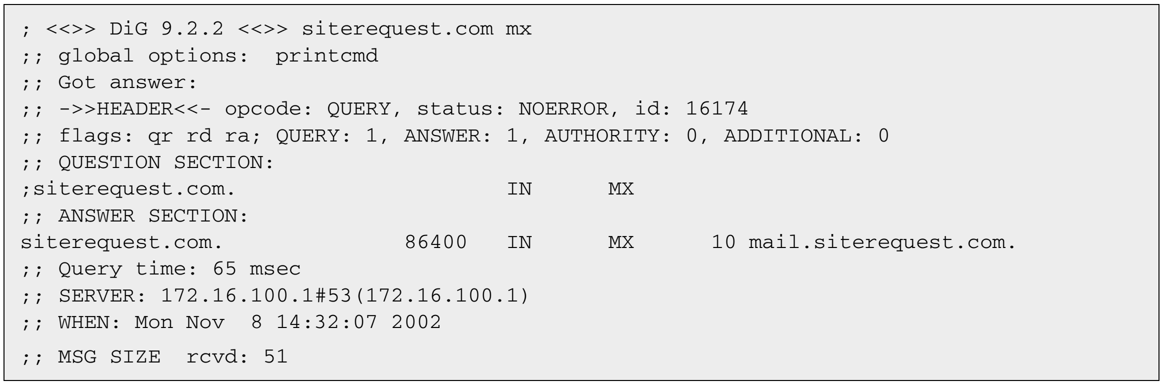
1. Log in as **root** at the command line.
2. Verify the DNS resolution for the domain to which you will be sending email, by typing the following command:

   ```
   dig <domain> mx
   ```

   For example, to query type **MX** and **siterequest.com**, which is where email is delivered, you would type the following command:

   ```
   dig siterequest.com mx
   ```

   You should receive a response similar to the following figure, indicating that Enterprise Manager is able to resolve the mail exchanger.



```
; <<>> DiG 9.2.2 <<>> siterequest.com mx
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16174
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;siterequest.com.                       IN      MX
;; ANSWER SECTION:
siterequest.com.              86400   IN      MX      10 mail.siterequest.com.
;; Query time: 65 msec
;; SERVER: 172.16.100.1#53(172.16.100.1)
;; WHEN: Mon Nov  8 14:32:07 2002
;; MSG SIZE  rcvd: 51
```

Figure 3.4 *A sample reply from the mail exchanger*

To configure email notification

By default, the postfix mail server is started when you start Enterprise Manager. If you need to modify postfix files, perform the following steps from the command line of the Enterprise Manager system, then restart the postfix service.

1. Using a text editor, such as **vi** or **pico**, edit the **/etc/postfix/main.cf** file.
2. Find the **mydomain** variable and change it to specify your site's domain. For example, if your domain is **siterequest.com**, change the variable to:

   ```
   mydomain = siterequest.com
   ```

3. Set the **relayhost** variable as in the following example:

   ```
   relayhost = $mydomain
   ```

4. If you want email sent only from **localhost**, set the **inet_interfaces** variable by typing the following:

```
inet_interfaces = localhost
```

5. Save and exit the file.
6. Edit the **/etc/hosts** file.
7. Create a record for the fully qualified domain name of your mailserver by typing the following command:

   ```
   echo "<your_mailserver_IP_address>
   <your_mailserver_fqdn>" >> /etc/hosts
   ```

   For example:

   ```
   echo "10.10.65.1 mail.siterequest.com" >> /etc/hosts
   ```

8. Save and exit the file.
9. From the command line, send a test email by typing the following command:

   ```
   echo test | mail <your email address>
   ```

10. View the mail queue, by typing the following command:

    ```
    mailq
    ```

11. To send any unsent mail, type the following command:

    ```
    postfix flush
    ```

12. Edit the **/etc/postfix/aliases** file.
13. Locate the following entry:

    ```
    ------------------------
    # Person who should get root's mail.  This alias
    # must exist.
    # CHANGE THIS LINE to an account of a HUMAN
    root:          postfix
    ------------------------------------------------
    ```

14. Change the **root** alias mapping to the email account to which you want mail to be sent.

    For example:

    ```
    root: helpdesk@postfix.fix
    ```

15. Save and exit the file.
16. Type the following command:

    ```
    newaliases
    ```

17. From the command line, send a test email by typing the following command:

    ```
    echo test | mail <your email address>
    ```

    If configured properly, the email is delivered to the address that you specified in the **/etc/postfix/aliases** file.

    For example:

    ```
    echo  "this is a test" |mail root
    ```

18. From the command line type the following command and press Enter.

    ```
    service postfix restart
    ```

Managing user accounts

When you initially set up Enterprise Manager, you configure a default administrator user account that permits you to set up and start working with the system through the web interface.

In order to discover and manage devices in the network, you must configure an administrator-level user account that matches an administrator-level user name on devices that you want to manage.

Enterprise Manager maintains a local authentication list of users, but you can choose to use a remote LDAP, Active Directory, or RADIUS authentication source.

◆ **Tip**

When you create an administrator-level user for Enterprise Manager, we recommend that you use the same user name that you currently use to administer F5 Networks devices in your network. This ensures that you can successfully manage devices as soon as Enterprise Manager discovers them and adds them to the device list.

Working with the user list

The Enterprise Manager user list specifies all user accounts that have administrator access to managed devices in the network. Each managed device authenticates the user names stored in the Enterprise Manager User List in order to authorize Enterprise Manager to perform device management tasks.

To add new users to the user list

When you add new users, ensure that you use the same administrator-level user name that you currently use for managing BIG-IP systems in your network.

1. On the Main tab of the navigation pane, expand **System** and click **Users**.
   The Users List screen opens.

2. Above the list, click **Create**.
   The New User screen opens.

3. In the **User Name** box, type the user name that you want to add to the Enterprise Manager user list.

4. In the Authentication row, in the **Password** and **Confirm** boxes, type the password for the user you just entered and confirm the password.

5. In the **Web User Role** box, select **Administrator**.
   The Allow Console Access box appears in the table.

6. In the **Allow Console Access** box, if you want to allow the user to access the command console, check the Select box to permit the user to access the Enterprise Manager device from the command line.

◆ **Important**

When you define a new user for Enterprise Manager, you must set their Web User Role to Administrator. If you select a user role other than Administrator, managed devices cannot authorize this user to perform management tasks, nor will the user be able to initiate tasks using the Enterprise Manager system.

Selecting the authentication source

By default, Enterprise Manager uses a local database to authenticate users. If you use a remote authentication source, you should configure Enterprise Manager to use your remote database.

To set the authentication source

1. On the Main tab of the navigation pane, expand **System** and click **Users**.
   The Users List screen opens.
2. On the menu bar, click **Authentication Source**.
   The Authentication Source screen opens.
3. Below the table, click **Change**.
   The **User Directory** box changes to a list.
4. In the **User Directory** list, select the type of remote source:
   - **Active Directory**: Specifies that the system uses a remote Active Directory server to authenticate users.
   - **LDAP**: Specifies that the system uses a remote LDAP server to authenticate users.
   - **RADIUS**: Specifies that the system uses a remote RADIUS server to authenticate users.

   After you select the type of remote authentication source, the Configuration table appears, where you can enter the remote server information.
5. In the Configuration table, enter the appropriate settings to configure Enterprise Manager to use a remote authentication server. See the online help for detailed information about the Configuration table.

4

Discovering and Managing Devices

- Working with Enterprise Management features
- Discovering and adding devices
- Performing basic device management
- Working with device groups

Working with Enterprise Management features

The Enterprise Manager provides you the ability to remotely manage certain aspects of your F5 Networks devices. Once the devices are a part of the Enterprise Manager device list, you can perform a variety of tasks including software upgrades, managing configuration archives, and configuring alerts. A ***managed device*** is a device in the network managed by Enterprise Manager.

You can store and deploy software upgrades and hotfixes, perform ConfigSync operations on high availability systems, archive and restore device configurations, and configure and manage custom alerts such as warnings for upgrades, communication issues between Enterprise Manager and a managed device.

Understanding device types

Enterprise Manager can identify all network devices on your network, including host servers. However, Enterprise Manager can only manage F5 Networks products, such as a BIG-IP system and the Enterprise Manager system itself.

BIG-IP systems

A BIG-IP system is an Internet device used to implement a wide variety of load balancing and other network traffic solutions. Enterprise Manager can manage all BIG-IP systems version 9.1.1 or later, and can manage software for BIG-IP Local Traffic Management systems.

Enterprise Manager systems

The Enterprise Manager system provides remote, centralized, administrative management of F5 Networks devices. If you have more than one Enterprise Manager device in your network, you can perform remote management on those devices in the same fashion as you do with other managed devices, such as a BIG-IP system.

Non-F5 devices

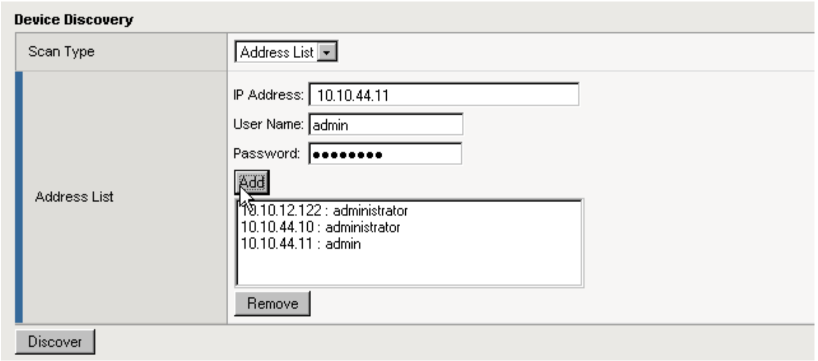
During the device discovery process, Enterprise Manager may find non-F5 Networks devices such as routers or servers, on the network. Although Enterprise Manager lists these devices in a results table after a discovery task, you cannot use Enterprise Manager to perform any management tasks on these devices. Because Enterprise Manager uses the iControl port (**443**) to communicate with managed devices, it does not connect to non-F5 devices other than to identify their presence in the network.

Discovering and adding devices

Enterprise Manager can automatically discover F5 Networks devices in your network. Once Enterprise Manager identifies these devices, and then logs onto the device using the administrator user name and password that you provide, it adds them to the managed device list. The ***device list*** is the list of devices managed by Enterprise Manager. In the navigation pane, if you click **Devices**, the Device List screen opens. Once devices are added to the device list, you can manage a variety of options on these devices from the Enterprise Manager web interface.

Discovering devices

Enterprise Manager can discover devices in your network if you click the **Discover** button on the Enterprise Management: Devices screen. You can search for devices by specific IP address or IP subnet. Enterprise Manager searches the network, querying devices on an iControl port (port **443**), attempting to log on to devices with an administrator user name and password that you supply. If Enterprise Manager succeeds in logging on to devices that it discovers, it automatically adds these devices to the device list.



Device Discovery

Scan Type: Address List

Address List

IP Address: 10.10.44.11

User Name: admin

Password: ●●●●●●●●

10.10.12.122 : administrator
10.10.44.10 : administrator
10.10.44.11 : admin

Figure 4.1 *Adding individual device addresses on the Device Discovery setup screen*

To discover devices

To successfully discover devices, Enterprise Manager must be able to access devices in the network through port **443** using the IP address you specify in the discovery setup process.

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Devices**.
   The Enterprise Management: Devices screen opens.

2. Click **Discover**.
   The Discover screen opens.

3. In the Device Discovery table, in the **Scan Type** row, specify how you want Enterprise Manager to scan your network: by **Address List**, where you specify one or more individual IP address, or by **Subnet**, where you specify a network address and netmask to scan. The table changes depending on what you selected.

4. If you opted to search by **Address List** in step 3, do the following:

   a) In the **IP Address** box, type the device IP address.

   b) In the **User Name** and **Password** boxes, type a user name and password to use to log on to the device.

   c) To add the device to the address list, click **Add**.

   d) Continue to add devices by repeating steps a through c.

5. If you choose to search by **Subnet** (class B or C network) in step 3, then do the following:

   a) In the **IP Address** box, type the device IP address.

   b) In the **Network Mask** box, type the netmask to use when searching the network. (You can search by class B or C network).

   c) In the **User Name** and **Password** boxes, type a user name and password to use to log on to each device discovered during the subnet scan.

6. To begin the discovery task, click the **Discover** button.
   The Task Properties screen opens. Discovered devices appear below the Properties section, and the list refreshes until all addresses in the range specified are checked, or until you click **Cancel Pending Items**.

◆ **Important**

*When you configure a range of addresses to scan, Enterprise Manager sends the user name and password to each device within the address range. If a device within the address range has an active SSL server listening for traffic on port **443**, the device receives the user name and password combination.*

Managing the refresh interval

Enterprise Manager polls managed devices at a default interval of 10 minutes. In each polling cycle, Enterprise Manager collects information about device status, peer synchronization, software installed on a device, and about tasks running on a device such as a software upgrade. Enterprise Manager polls this information at a specified refresh interval and displays it on the device list and general properties screens.

You can adjust this refresh interval so that polling cycles occur more or less often. Additionally, you can manually poll a managed device for updated information from the device's general properties screen.

To change the refresh interval

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Devices**.
   The Enterprise Management: Devices screen opens.
2. On the menu bar, click **Options**.
   The Device Options screen opens.
3. In the **Refresh Interval** box, type a new value.
4. Click **Save Changes**.
   Enterprise Manager now polls devices at the rate you specified in the **Refresh Interval** box.

To refresh device information immediately

On the Devices screen, check the box to the left of a device name, then click the **Update Status** button.
Enterprise Manager communicates with the selected managed device, and updates the information in the device list.

◆ **Note**

You can update information for an individual device by clicking the ***Update Status*** *button on that device's general properties screen.*

Deleting devices from the device list

If you delete a device from the device list, Enterprise Manager no longer manages the device or its software images.

To delete a device from the Devices screen, check the box to the left of the device name in the device list and click the **Delete** button.

◆ **WARNING**

If you delete a device from the managed device list, Enterprise Manager removes all configuration information associated specifically with this device such as device group memberships, alerts, certificate information, and device archives from the Enterprise Manager database. If you add this same device to Enterprise Manager in the future, you must re-configure these settings.

Performing basic device management

Once you add devices to the device list, you can remotely perform basic management functions such as a ConfigSync between high availability systems, or reboot a device using a different boot image location.

Setting device communication properties

When Enterprise Manager discovers a device, it adds it to the device list at the default IP address that you specified. While Enterprise Manager can see the device at this address, you must ensure that a managed device can communicate back to Enterprise Manager. If a device cannot communicate back to Enterprise Manager, the software update functionality does not work properly.

To set device communication properties

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Devices screen opens.

2. In the device list, click the device name of the device for which you want to set communication properties.
   The Device Properties screen opens, displaying the current device's IP address (as discovered by Enterprise Manager) and the address of the device's Configuration utility.

3. Above the table, in the **Device Properties** list, select **Advanced** to display additional device properties.

4. In the **EM Address** box, ensure that the IP address correctly specifies the address of the Enterprise Manager system.
   This is the address that the managed device uses to communicate with Enterprise Manager.

Testing communications between devices and Enterprise Manager

After you discover a device and configure the IP addresses on the general properties screen, we recommend that you test the communication between Enterprise Manager and each managed device to ensure that the connection is a two-way connection. When Enterprise Manager successfully adds a device to the device list, this means that the connection works in one way. To ensure that the connection works in the other direction, you must test the connection from the command line of each managed device. To test the connection, you must have **root** access to the managed device's command line.

To test a managed device's connection to Enterprise Manager

1. Log onto the managed device command line as the **root** user.
2. From the command line type the following command where **<EM_address>** is the IP address of the Enterprise Manager system:

   ```
   telnet <EM_address> 443
   ```

   This command tests the ability of the managed device to communicate with Enterprise Manager on port **443**.

   - If you receive a **connected to <EM_address>** message, the managed device can properly communicate with Enterprise Manager.
   - If you receive a **connection refused** message, you may need to adjust some settings, so that the IP address the managed device uses correctly communicates with the IP address specified in the EM Address box on the Device Properties screen. Some settings you may consider changing include the IP address in the EM Address box, or addresses specified in your NAT or SNAT.

Working with high availability systems

Enterprise Manager identifies and provides basic management of high availability redundant systems. During the device discover process, Enterprise Manager detects BIG-IP devices that are part of a redundant system, and displays each device's failover state.

A ***redundant system*** is a pair of BIG-IP systems configured for failover. In a redundant system, there are two units, often with one running as the active unit and one running as the standby unit. If the active unit fails, the standby unit takes over and manages connection requests. For more information about configuring redundant systems and different configurations of redundant systems such as an active-active configuration, see the ***BIG-IP Network and System Management Guide***.

Identifying high availability systems

During the discovery process, Enterprise Manager identifies redundant systems by displaying a device peer's host name in an adjacent column in the device list. When you move the cursor over the status icon to the left of a device name, a tooltip indicates the status and failover state of the device (if the device is reachable).

Changing a device's failover state

When you use Enterprise Manager to manage a high availability system, you can switch the failover states of the managed device pair. You can use this feature to switch the modes of an active-standby or an active-active pair.

To change a device's failover state

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Devices screen opens.
2. In the device list, click the device name of the device for which want to change the failover state.
   The Device Properties screen opens, displaying the current device's state in the Device Properties table and the device peer's state in the Peer Properties table.
3. Below the Device Properties table, click **Switch to Standby Mode** or **Switch to Active Mode**, depending what mode you want to set on the managed device.
   After you confirm this change, the device list screen opens, indicating the new state of the device and its peer.

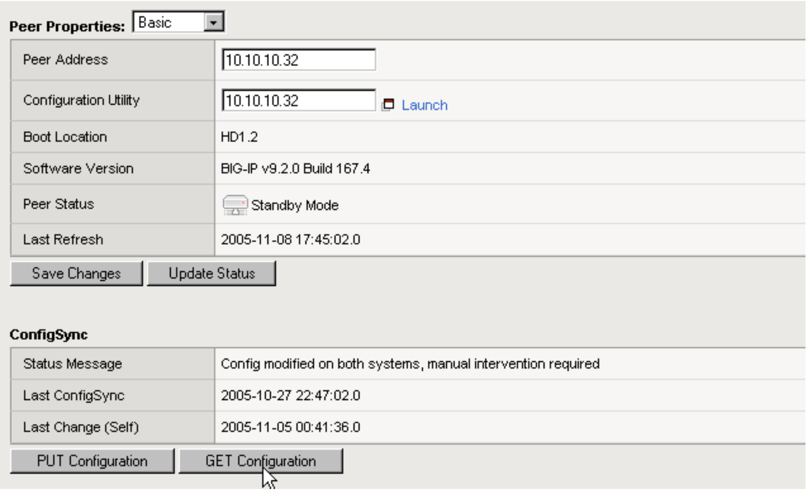
Synchronizing peer configurations

When you manage high availability systems with Enterprise Manager, you can remotely run a ConfigSync process to synchronize the configurations between peer devices, if the ConfigSync auto-detect is enabled on the managed device. Before you synchronize configurations between managed peer devices, you must enable the ConfigSync Auto-detect setting on the managed device pair.

To enable ConfigSync auto-detect

1. From the Devices screen, click the device name of the device that you want to enable ConfigSync auto-detect for.
   The Device Properties screen opens.

2. Below the ConfigSync table, click **Enable Auto-Detect**.
   The Device Properties screen refreshes, and ConfigSync status information appears in the ConfigSync table.



Peer Properties: Basic

Peer Address	10.10.10.32
Configuration Utility	10.10.10.32 Launch
Boot Location	HD1.2
Software Version	BIG-IP v9.2.0 Build 167.4
Peer Status	Standby Mode
Last Refresh	2005-11-08 17:45:02.0

ConfigSync

Status Message	Config modified on both systems, manual intervention required
Last ConfigSync	2005-10-27 22:47:02.0
Last Change (Self)	2005-11-05 00:41:36.0

Figure 4.2 *Peer information on the device general properties screen*

To synchronize configurations between peers

1. On the Devices screen, click the device name of the device that you want to synchronize with its peer.
   The Device Properties screen opens, displaying the current configuration information in the ConfigSync table.

2. Below the ConfigSync table, select one of the following options:

   - If you want to copy the current device's configuration to the peer device, click **PUT Configuration**.

   - If you want to copy the peer device's configuration to the current device, click **GET Configuration**.

Rebooting managed devices remotely

If you have different software or hotfix versions installed on different boot image locations on a managed device, you can use Enterprise Manager to reboot using a different boot image location.

To reboot with a different boot image location

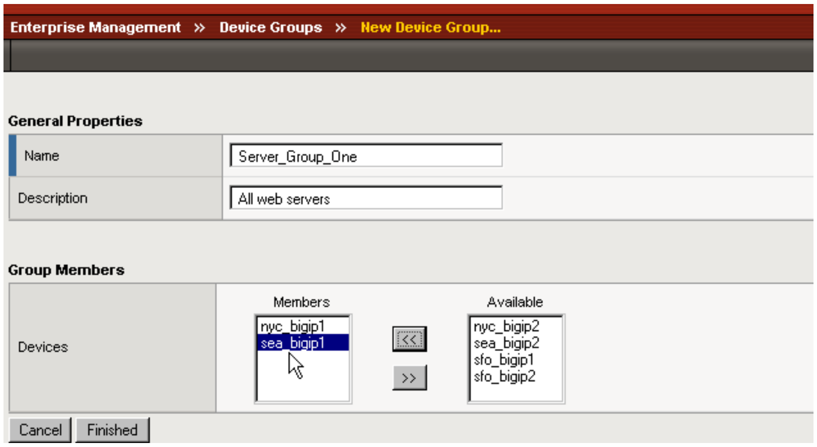
1. On the Devices screen, click the name of a device.
   The Device Properties screen opens.

2. On the menu bar, click **Boot Locations**.
   The Boot Image Locations screen opens, displaying the active and available boot locations and the software installed on each.

3. In the Select column, click the option button to select the boot image that you want to use to reboot the device.
4. Click **Reboot**.
   After you confirm the reboot, the device reboots and the table updates to indicate the new active boot location.

Working with device groups

Once Enterprise Manager adds devices to the device list, you can create customized groups of devices. Using these device groups, you can manage a set of devices at once rather than individually. This gives you additional flexibility in managing alerts, software installations, and configurations on a large number of devices.



Enterprise Management » Device Groups » New Device Group...

General Properties

Name	Server_Group_One
Description	All web servers

Group Members

Devices

Members	Available
nyc_bigip1 sea_bigip1	nyc_bigip2 sea_bigip2 sfo_bigip1 sfo_bigip2

Figure 4.3 Adding members to a new device group

To create a device group

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Enterprise Management: Devices screen opens.

2. On the menu bar, click **Device Groups**.
   The Device Groups list screen opens.

3. Click the **Create** button.
   The New Device Group screen opens.

4. In the General Properties section, in the **Name** box type the name of the device group. You can use all alphanumeric characters and certain special characters (**. * / - : _ ? = ,**) in the **Name** box.
   This name subsequently appears on the Device Groups list screen and in list boxes on screens where you can assign attributes to a device group.

5. In the **Description** box, type information that can help identify the group when it appears on the Device Group list screen.

6. In the Group Members section, you can add devices to the device group. Devices listed in the **Members** box are members of the current device group, and devices listed in the **Available** box can be added to the current device group.

a) To add devices to the group, select a device in the **Available** box and click the Move button (**<<**) to move the device name to the **Members** box.

b) To remove devices from the group, select a device in the **Members** box and click the Move button (**>>**) to move the device name to the **Available** box.

7. Click **Finished** to save the new device group information.
   The Device Groups list screen opens and the new device group appears in the list.

◆ **Important**

Once you create and save a new device group, you cannot change the device group name. If you need to change a device group name, you must create a new group.

Managing device group members

Once you create one or more device groups, you can add devices to, or remove devices from the group. When you add devices to the device group, the newly added devices inherit the properties of a device group, if you assign alerts or other configuration options to the group.

To manage device group members

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Enterprise Management: Devices screen opens.

2. On the menu bar, click **Device Groups**.
   The Device Groups list screen opens.

3. Click the name of the device group whose members that you want to manage.
   The Device Group general properties screen opens.

4. In the Group Members section, you can add devices to, or remove devices from the device group. Devices listed in the **Members** box are members of the current device group, and devices listed in the **Available** box can be added to the current device group.

   a) To add devices to the group, select a device in the **Available** box and click the Move button (**<<**) to move the device name to the **Members** box.

   b) To remove devices from the group, select a device in the **Members** box and click the Move button (**>>**) to move the device name to the **Available** box.

5. Click **Save Changes** to save the device group information.

Managing device memberships to a device group

In addition to managing members of a device group, you can adjust the groups that a particular device belongs to. When a device belongs to a device group, it has a membership in that group. A device can belong to more than one device group, thus you may need to manage a device's memberships.

To manage a device's memberships

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Enterprise Management: Devices screen opens.
2. On the Devices screen, click the name of a device.
   The device general properties screen opens.
3. On the menu bar, click **Memberships**.
   The memberships list screen opens, listing all of the device groups that the current device belongs to.
4. To add the device to one or more device groups, click **Manage** above the list and perform the following on the Membership Management screen:

   a) Select one or more device groups in the **Available** box and click the Move button (**<<**) to move the device groups to the **Active Memberships** box.
   The current device is a member of device groups listed in the **Active Memberships** box.

   b) Click **Finished** to save changes to the device's memberships.
5. To remove the device from one or more device groups, check the box to the left of a group name, and click **Remove From Group** below the list.
   The device is removed from the groups that you checked and the device general properties screen opens.

Software upgrades and alerts on device groups

The device groups feature allows you to manage software upgrades and alerts on more than one device at a time. You can elect to deploy a software upgrade to a device group and the software is installed on all members of the group. Additionally, if you assign an alert to a device group, all members of the group inherit the alert properties.

For detailed information about working with software upgrade and device groups, see Chapter 7, *Managing Software Images*. For detailed information about working with alerts and device groups, see Chapter 9, *Monitoring and Alerting*.

5

Managing UCS Archives

- Working with device archives
- Managing rotating archives
- Saving device configuration archives
- Restoring device archives

Working with device archives

When you initially configure a BIG-IP system, you can elect to store the system's configuration information in a user configuration set (UCS) archive. A ***UCS archive*** is a compressed file that contains all the configuration files that are typically required to restore a configuration on a system. These files are useful in recovering information vital to the traffic management functions of a BIG-IP system. A UCS archive consists of:

- All BIG-IP system configuration files
- BIG-IP system product licenses
- User accounts and password information
- DNS zone files and NameSurfer configuration
- SSL certificates and keys

On a BIG-IP system, you can create UCS archives using the BIG-IP System Configuration utility or from the command line. On the Enterprise Manager system, you can configure Enterprise Manager to create UCS archives on regularly scheduled intervals with the option of storing any archive indefinitely.

You must store these archives in a secure location because UCS archives contain critical system files, user account information, passwords, and SSL private keys used by SSL proxies configured on a BIG-IP system.

Enterprise Manager provides a secure location for multiple configurations. When you use Enterprise Manager to manage your device configurations, you can automatically back up device configurations at intervals you control to ensure that you have a working configuration to use if you need to restore the system.

Enterprise Manager is initially set to store up to 10 rotating device archives and 10 saved, or pinned, archives per device in its database. If you want to change these default values, see *Changing the device archive options*, on page 3-11.

Managing Enterprise Manager device archives

In addition to managing device configuration archives for a BIG-IP system, Enterprise Manager can manage UCS archives for itself or other Enterprise Manager systems.

An Enterprise Manager UCS archive contains all of the same information that a BIG-IP system UCS archive does, but it also contains additional information about managed devices in an Enterprise Manager system, including:

- Device properties information
- Device certificates
- Custom alerts
- Device groups

- Certificate lists
- History information such as the task list and alert history list
- Rotating archive schedules

Enterprise Manager UCS archives contain all the essential managed device information stored in the Enterprise Manager database. However, they do not archive imported information such as software or hotfix images and managed device UCS archives.

Creating Enterprise Manager configuration archives

You have two main options for creating a UCS archive of an Enterprise Manager configuration: basic and advanced. A basic UCS archive for an Enterprise Manager system contains device configuration information, as noted in the previous section. An advanced UCS archive includes the basic information and all of the data that you imported to the Enterprise Manager system, such as software images and managed device configuration archives.

To create a basic UCS archive, you can add an Enterprise Manager device to a rotating archive schedule (in the same way that you do for any managed device) and store basic UCS archives on an Enterprise Manager system. See *Managing rotating archives*, on page 5-4 for more information on working with rotating archive schedules.

To create an advanced configuration archive of an Enterprise Manager system, you must use the **em-backup** script. This script backs up all the Enterprise Manager UCS information and additional data such as the software repository and managed device UCS archives.

Because this may involve a large amount of data, ensure that you have adequate disk space available on the Enterprise Manager system and that you move the archive file to a remote system when it completes.

To create an advanced Enterprise Manager backup

To perform a full backup, you must have **root** access to the command line. Before you run the **em-backup** script, ensure that no tasks are running on the Enterprise Manager system.

1. At the command line, log in as **root**.
2. At the command prompt, type the following command, where **<archive_name>** is the path and file name for the archive file, and press Enter.

   ```
   em-backup <archive_name>.ucs
   ```

   The **em-backup** script begins the process of archiving all configuration and imported data stored on the Enterprise Manager system.

3. When the process completes, move the **<archive_name>.ucs** file to a remote system.

◆ **Note**

*The **em-backup** script may take several minutes to complete depending on how many software images or UCS archives are stored on the Enterprise Manager system.*

Restoring Enterprise Manager configuration archives

If you need to restore a configuration to an Enterprise Manager system, you have basic and advanced options. A basic restoration can re-establish all Enterprise Manager configuration information regarding managed devices, including certificate information, device groups, and custom alerts. An advanced restoration includes all of the basic data in addition to imported data such as software images and managed device UCS archives.

You can perform a basic restoration from the Device Archive Properties screen. See *Restoring device archives*, on page 5-10 for information on restoring UCS archives from an Enterprise Manager system.

If you want to perform an advanced restoration, you can use the **em-restore** script. If you want to use the **em-restore** script, you must have an advanced device configuration file created using the **em-backup** script. If you use the **em-restore** script, this restores all configuration settings and all of the data you imported into Enterprise Manager such as software images and UCS archives of managed devices.

To restore a full Enterprise Manager backup

To perform a full restoration, you must have **root** access to the command line. Before you run the **em-restore** script, ensure that you have a valid advanced UCS archive created by the **em-backup** script.

1. Log in as **root** at the command line of the Enterprise Manager system that you want to restore.

2. Copy the advanced Enterprise Manager UCS archive that you created with the **em-backup** script to the Enterprise Manager system that you want to restore.

3. At the command prompt, type the following command, where **<archive_name>** is the path and file name for the archive file, and press Enter.

   ```
   em-restore <archive_name>.ucs
   ```

   The **em-restore** script begins the process of restoring all configuration and imported data stored on the Enterprise Manager system.

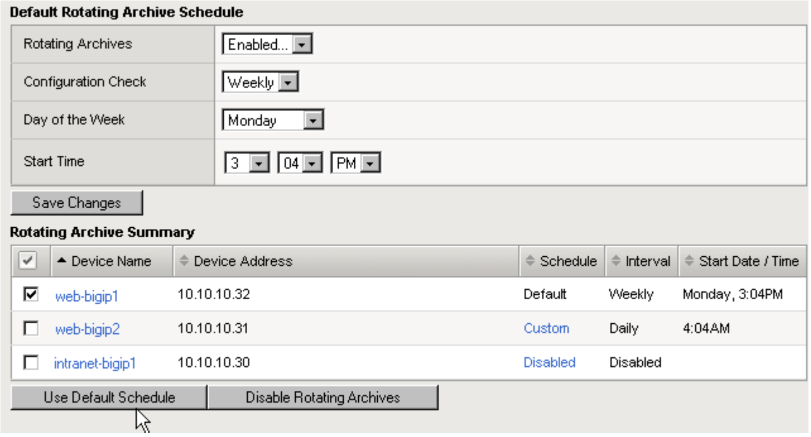
4. When the process completes, delete the **<archive_name>.ucs** file from the target system, and reboot the device.

Managing rotating archives

Enterprise Manager can create and store UCS archives for managed devices on demand, or at regularly scheduled intervals using rotating archives. ***Rotating archives*** are UCS archives created at a regular interval according to a schedule that you set in Enterprise Manager.

The advantage of scheduling rotating archives is that you can set Enterprise Manager to create archives on a regular interval so that after Enterprise Manager recognizes that a managed device's configuration has changed, it schedules the creation of a UCS archive during the current rotating archive schedule. This way, you can have a recent backup configuration for a managed device, which provides added stability in case a configuration change results in a need for a system restore. For example, if you set up a daily rotating archive schedule, Enterprise Manager creates a UCS archive on each day that the managed device configuration changes. This ensures that you do not unnecessarily save any duplicate configuration archives, and that you always have one or more archives of recent configurations with which to restore. In a rotating archive schedule, Enterprise Manager saves multiple archives and cycles out old archives as it creates new ones.

After Enterprise Manager adds devices to the device list, you can set up a default rotating archive schedule for all managed devices. If you need to set up a custom schedule for any devices, you can do that individually for each device.



Default Rotating Archive Schedule

Rotating Archives	Enabled...
Configuration Check	Weekly
Day of the Week	Monday
Start Time	3 : 04 : PM

Rotating Archive Summary

☑	Device Name	Device Address	Schedule	Interval	Start Date / Time
☑	web-bigip1	10.10.10.32	Default	Weekly	Monday, 3:04PM
□	web-bigip2	10.10.10.31	Custom	Daily	4:04AM
□	intranet-bigip1	10.10.10.30	Disabled	Disabled	

Figure 5.1 *Adding a device to the default rotating archive schedule on the Rotating Archive Schedule screen*

To configure a default rotating archive schedule

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Devices**.
   The Device List screen opens.

2. On the menu bar, click **Rotating Archive Schedule**.
   The Rotating Archive Schedule screen opens.
3. In the Default Rotating Archives Schedule table, in the **Rotating Archives** box, select **Enabled**.
   The table changes to show additional options.
4. In the **Configuration Check** box, select how often you want Enterprise Manager to check managed device configurations.
   The table changes to provide options for the frequency you selected.
5. Depending on the frequency you selected, you can specify a day of the week, month, and time of day that you want Enterprise Manager to check for changes to device configurations.
   The Rotating Archive Schedule Summary table details the rotating archive schedule of each managed device.

After you set up a default rotating archive schedule, then whenever a device configuration changes during the interval you specify, Enterprise Manager creates an archive of the device's configuration and adds it to the Rotating Archives table on the Device Archives screen.

To configure a custom rotating archive schedule

If you need to specify a different rotating archive schedule for a device, or need to apply a rotating archive schedule to one device, you can create a schedule for individual devices

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. Click the name of the device for which you want to create a custom rotating archive schedule.
   The Device Properties screen opens.
3. On the menu bar, click **Archives**.
   The Device Archives screen opens.
4. In the Rotating Archive Schedule table, in the Rotating Archives box, select **Custom**.
   The table changes to enable additional options.
5. In the **Configuration Check** box, select how often you want Enterprise Manager to check the managed device’s configuration.
   The table changes to provide options for the frequency you selected.
6. Depending on the frequency you selected, you can specify a day of the week, month, and time of day that you want Enterprise Manager to check for changes to device configurations.
7. After you set the details, click **Save Changes**.

When you check the status of rotating archives on the Rotating Archive Schedule screen, this device’s schedule appears as **Custom**.

To exclude one or more devices from a default rotating archive schedule

When you create a default rotating archive schedule, all managed devices subscribe to this schedule unless you create a custom schedule for a device, or unless you disable rotating archives for a device.

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Devices**.
   The Device List screen opens.
2. On the menu bar, click **Rotating Archive Schedule**.
   The Rotating Archive Schedule screen opens.
3. In the Rotating Archive Summary table, check the Select box next to any device that you want to exclude from the default rotating archive schedule.
   The Rotating Archive Schedule screen opens.
4. Below the table, click **Disable Rotating Archives**.
   The table changes to indicate which devices are disabled from the rotating archive schedule.

◆ **Tip**

You can use this screen to both enable and disable the default rotating archive schedule for multiple devices.

Modifying or deleting configuration archives

Once you set up a rotating archive schedule or create pinned archives, you can modify the descriptions of archives, or delete archives if you need to. You can perform these actions from a device archives or archive properties screen.

To delete device configuration archives

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. Click the name of the device for which you want to delete configuration archives.
   The Device Properties screen opens.
3. On the menu bar, click **Archives**.
   The Device Archives screen opens.
4. In either the Rotating Archives or Pinned Archives table, check the Select box next to the name of the archive(s) that you want to delete.
5. Below the appropriate table, click **Delete**.

To modify an archive description

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. Click the name of the device for which you want to modify the description of a UCS archive.
   The Device Properties screen opens.
3. On the menu bar, click **Archives**.
   The Device Archives screen opens.
4. In either the Rotating Archives or Pinned Archives table, click the name of the archive for which you want to modify the description.
   The Archive Properties screen opens.
5. In the **Description** box, type the new description.
6. Click **Save Changes**.

Saving device configuration archives

When you set up a rotating archive schedule, Enterprise Manager saves multiple archives, and cycles out old archives as it creates new ones. Although this ensures that you maintain a useful list of the most recent UCS archives for each of your managed devices, you may want to save certain archives.

Using Enterprise Manager, you can save pinned archives almost indefinitely. A ***pinned archive*** is a UCS archive (that you create or move from the rotating archive list) that is saved in the Enterprise Manager database until you remove it.

This feature is useful if you want to save device configurations after important changes such as before or after a software upgrade or hotfix installation. This ensures that you can restore a saved configuration from any specific point in time.

To create a new pinned archive

You can create a new UCS archive from a device's Rotating Archive Schedule screen.

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. Click the name of the device for which you want to create a new pinned archive.
   The Device Properties screen opens.
3. On the menu bar, click **Archives**.
   The Device Archives screen opens.
4. Above the Pinned Archives table, click **Create**.
   The New Archive screen opens.
5. In the **File Name** box, type the file name of the new archive that you want to create.
6. In the **Description** box, type a note that you want to appear in the Pinned Archives table next to the archive file name.
7. Click **Create**.
   Enterprise Manager creates a UCS archive of the current device and the archive appears in the Pinned Archives table when the Rotating Archive Schedule screen opens.

To pin an existing configuration archive

You can save a UCS archive from a device's Rotating Archive Schedule screen.

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. Click the name of the device for which you want to pin an archive from the rotating archive list.
   The Device Properties screen opens.
3. On the menu bar, click **Archives**.
   The Device Archives screen opens.
4. In the Rotating Archives table, check the box to the left of an archive name to select it.
5. Click **Pin Archive** below the table.
   The selected archive moves to the Pinned Archive table where it is saved until you delete it.

Restoring device archives

You can use Enterprise Manager to restore a UCS archive on any managed device. In the event of a system restore, you can save time by not logging on to an individual device console to restore a device archive, and use Enterprise Manager instead.

◆ Important

You can only restore a device configuration to the device that Enterprise Manager saved the configuration archive from.

To restore a device archive

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. Click the name of the device for which you want to restore a UCS archive.
   The Device Properties screen opens.
3. On the menu bar, click **Archives**.
   The Rotating Archive Schedule screen opens.
4. In either the Rotating Archives or Pinned Archives table, click the name of the archive that you want to restore.
   The Archive Properties screen opens.
5. To restore the archive to the source location on the managed device, click **Restore**.

◆ WARNING

Restoring an archive to a managed device overwrites all current configuration information on the device.

6

Managing Device Configurations

- Managing device configurations
- Creating a changeset for a device
- Modifying a changeset
- Verifying a changeset
- Deploying configuration data and settings to target devices

Managing device configurations

After you initially configure a BIG-IP system, you can create a device configuration set that archives all of the basic settings for the system. The system stores this information in the user configuration set (UCS) file.

A UCS file is a compressed file that contains all of the configuration files that are typically required to restore the current configuration to the system. These files include:

- All BIG-IP system specific configuration files
- BIG-IP product licenses
- User accounts and password information
- DNS zone files and ZoneRunner configuration
- SSL certificates and keys

For more information about how to manage UCS archives with Enterprise Manager, see Chapter 5, *Managing UCS Archives*.

Although UCS files are useful in fully restoring an individual BIG-IP system, Enterprise Manager can create a more flexible data set of BIG-IP system device configuration settings that allows you to copy all or part of the device's configuration settings to a separate BIG-IP system.

Using Enterprise Manager, you can create a flexible collection of configuration data and store it as a changeset. A ***changeset*** is a user-defined collection of configuration data that enables you to archive and distribute a customized device configuration of a BIG-IP system. With Enterprise Manager, you can create a changeset for any managed device in the network. A changeset can include the following information for a managed device:

- Network object information
- Local Traffic Management objects
- System settings

You can use this feature for a variety of configuration data on a managed device, such as system information, or basic traffic management configurations. Once you create a changeset, you can verify the compatibility with managed devices in the network, then deploy that changeset to those managed devices. This gives you better control over device configurations on managed devices in the network.

Understanding changesets

Although a changeset is a collection of configuration files that you could use to restore a configuration, changesets differ from UCS files in three primary ways. The following table outlines the main differences.

UCS archives	Changesets
Contain a comprehensive set of all configuration data for a device.	Contain a versatile set of configuration data for a device.
Designed for use on a single device.	Designed so that you can deploy configuration data to other devices.
Used exclusively for archiving and restoring the configuration for a single device.	Can be used for a wide variety of tasks, including setting up a device, maintaining consistent configurations on multiple devices, and creating new applications.

Table 6.1 *Differences between UCS archives and changesets*

Working with changesets

With the configuration management flexibility of changesets, you now have the ability to manage device configurations in new ways. You can use changesets to assist in deploying new devices, establishing consistent settings across multiple devices, with rolling out new applications, and for making simple configuration changes.

Using changesets when adding new devices

If you add a new device to the network, you can use a changeset to deploy common configuration elements to the new device. This makes it possible for you to deploy new devices with a standard, consistent configuration when you create a changeset from a prototypical device.

When you initially configure a BIG-IP system, typically, you set up profiles, monitors, and iRules. If you set up systems individually, you must keep track of settings for each of these, and manually input these values for each new device you add to the network. However, if you use changesets, you can deploy the profiles, monitors, and iRules configurations from one device to as many devices as needed.

This essentially designates one device as the prototypical device, and requires that you configure it individually.

Once you configure the primary device, you can create a changeset that includes profiles, monitors, and iRules (and other standards such as IP addresses or network objects) selected from the primary device. After you have created the changeset, deploy the changeset to a new device. During the deploy changeset task, you can change specific settings in the changeset data to be compatible with the new device.

Deploying new standards with changesets

In certain situations, you may change a standard configuration element on one managed device, then deploy that change to all other managed devices in the network.

To maintain configuration integrity and consistency, you must ensure that when you change a configuration setting on one managed device, you also change it on other devices. You can create a changeset for any class of network object and deploy it to additional devices.

For example, if you want to change an HTTP profile’s compression settings, you can change it on one device, create a changeset for HTTP profiles, then deploy it to additional devices.

Configuring new applications using changesets

When you roll out a new application, you can use changesets to deploy the important settings to as many devices as needed. This can reduce the time required to install a new application on multiple BIG-IP systems.

For example, when you create a new virtual server that you want to duplicate on other devices, you can use changesets to deploy the virtual server while maintaining unique dependencies on each managed device.

To do this, you create a changeset of the model virtual server and dependencies. Then, when you deploy the virtual server, you can change the important variables (such as the virtual server name and IP address) before you deploy it to a new device. Although this requires that you have important IP address information available, it reduces the time required to create an entirely new virtual server on each device.

Performing simple configuration changes using changesets

Although it is straightforward to perform simple configuration changes on an individual device, you can use a changeset to modify settings on managed devices so that your changes are tracked in the Enterprise Manager database. This can assist in auditing changes later.

For example, if you want to change the settings for a virtual server on a device, you can create a changeset that contains the virtual server. Then, you can modify the changeset by adjusting the properties. After you do this, you can deploy the changeset to the same device, and the new settings will replace the old settings.

Understanding dependencies

In order to successfully copy a network object from one BIG-IP system to another, you must honor the network object’s dependencies when you define the network object on the new system. A ***dependency*** is additional network object data or resources required for the primary object to function correctly. For example, when you configure a virtual server, this usually requires defining dependent objects, or resources of the virtual server such as pools, nodes, or profiles. These pools, nodes, or profiles are the dependencies of the virtual server.

The presence of these dependencies adds complexity to the process of storing and copying device object configurations in changesets. If you were to manually copy configuration files from one system to another, you would need to know each of the dependencies for every object or system setting that you plan to copy. Enterprise Manager automatically manages these dependencies when you create a changeset, and provides you the option to modify dependent object information before you distribute a changeset to a different device.

Creating a changeset for a device

When you create a changeset, we recommend that you use the changeset wizard to create a changeset. However, you have the option to use manual text entry to create a changeset.

The easiest way to create a changeset is to use the changeset wizard to assist you. The changeset wizard works in a way similar to other task wizards such as the upgrade wizard. The main difference between using a wizard and using text entry to create a changeset is that a wizard can automatically locate object dependencies for each network object that you select to include in the changeset. Additionally, the changeset wizard writes all the syntax necessary to correctly classify network objects and system settings in a changeset configuration file. This helps ensure that you can successfully deploy the changeset to other managed devices.

If you use the text entry option, you must know all of the dependencies for each of the objects that you include in the changeset so that you can include these objects in the changeset text. You must also learn the syntax necessary to copy configuration data properly to a target device when you deploy the changeset.

Using the changeset wizard to create a changeset

The changeset wizard works like the other wizards in Enterprise Manager, and helps guide you through the process of creating a changeset.

Creating a changeset using the wizard involves four main steps:

- Specifying the source device and partition
- Selecting the object classes that you want to include
- Choosing the specific objects and their dependencies for each object class
- Reviewing the changeset details

After you create a changeset, Enterprise Manager stores the device configuration information in its database. Later, you can verify and deploy the device configuration data stored in the changeset to any compatible device in the network.

Selecting a source device and partition

The first step in creating a changeset is selecting a changeset source device. The ***changeset source*** device is the managed device in the network from which you want to copy some or all of its device configuration.

Once you select the changeset source device, you can select the device partition from which you want to copy the device configuration information.

Administrative partitions are a feature due to be introduced in BIG-IP version 9.4. ***Administrative partitions*** are logical containers containing a defined set of BIG-IP system objects and are used for access control purposes. The Enterprise Manager changeset feature is compatible with administrative partitions.

◆ **Important**

*If you are working with changesets on a device that does not support administrative partitions, select **Common** for the default partition when prompted. For devices that do not support administrative partitions, **Common** includes all partitionable BIG-IP system objects.*

To select a device and partition

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Changesets**.
   The Changeset List screen opens.

2. Above the list, click **Create**.
   The New Changeset screen opens.

3. In the **Name** box, type the name of the changeset.
   This name later appears on the changeset list.

4. In the **Description** box, type a description of the changeset.

5. From the **Source** list, select **Device** to select a specific device from which you want to copy device configuration information.

6. In the **Device** list, select the source device.

7. If the source device uses multiple partitions, in the **Partition** list, select the partition from which you want to copy objects.

8. Click **Next** to open the Step 1 of 3 screen where you can select the specific objects for the changeset.

Selecting object classes

After you specify a source device and partition, you need to select the object classes that you want to include in the changeset. An ***object class*** is the general type of network object that you want to include in a changeset. For example, a virtual server on a BIG-IP system named **www_server_one** belongs to the Local Traffic / Virtual Servers class, or the **resolv.conf** file belongs to the System / DNS class. You can select from traffic management classes or system settings, and can include any type of available object class in the changeset.

To select object classes

1. For the **Path List** setting, in the **Available** list, click a class to select it, then click the Move button (**<<**).
   The selected class moves to the **Selected** box, and is included in the changeset.
2. Repeat step 1 as necessary to add additional classes to this changeset.
3. To move to the next screen where you select specific class instances, click **Next**.

Selecting specific objects and dependencies

After you select the object classes, you must choose the specific object instances to include in the changeset. An ***object instance*** is the specific network object that you want to include in the changeset.

In the previous step, you chose object classes to include in the changeset. You can select the specific objects on the Step 2 of 3 screen. Depending on how many object classes you selected, the Step 2 of 3 screen appears once for each object class that you included in the changeset.

Enterprise Manager displays object dependencies for all objects that require dependencies. When you click the object name on the screen, you can see which objects are dependent on each object you choose, and you can modify these values if required.

To specify objects and dependencies

1. In the **Object List** box, in the **Available** list, click an object to select it, then click the Move button (**<<**).
   The selected object moves to the **Selected** list, and object dependencies appear below the **Selected** list.
2. If required, edit the details of the object or system settings.

3. To move to the next screen to review the changeset summary, or to add a different type of object instance, click **Next**.

◆ **Note**

If you are adding more than one object class to the changeset, this screen appears as many times as needed so that you can add objects for each class. When you finish adding object instances, click ***Next*** *to open the changeset summary screen.*

◆ **Important**

If you are including an iRule in a changeset, you must manually specify the dependencies for this iRule because Enterprise Manager does not automatically scan iRules to look for object dependencies.

Reviewing changeset task settings

Once you have configured the create changeset task, you can review it on the last screen of the wizard. At this stage, you can also choose whether to include dependencies in the changeset.

If you choose not to include dependencies in the changeset, you must ensure that these dependent objects are available on any device on which you may later deploy this changeset.

To review and change changeset settings

1. In the **Dependency Handling** box, select whether to include dependencies.
   The **Resources** box disappears if you choose not to include dependencies.

2. To view details of an object that you selected, in the **User Selected Objects** list, click the name of an object.
   Details about that object appear below the list in several fields, some of which are editable.

3. To change details of an object that you selected, change any of the values in the editable fields that appear when you click an object name.

4. To view details of any dependent objects, in the **Resources** list, click the name of an object
   Details about that object appear below the list.

5. Once you review and change information in the changeset, click **Finished** to save the changeset.

◆ **Tip**

If you want to manually change any details of the changeset, you can do this from the Changeset Properties screen any time after you save the changeset.

Creating a text changeset

As an alternative to using the changeset wizard, you can create a changeset by typing class and object information into the **Text** field on the New Changeset screen. While this method can produce a changeset, we recommend that you use the changeset wizard so that Enterprise Manager can generate the correct syntax and automatically gather dependency information.

When you create a device configuration on a BIG-IP system, the system stores this information in plain text in editable configuration files such as **bigip.conf**. When Enterprise Manager creates a changeset, it also stores this information in text form, ensuring compatibility with configuration files on a managed device.

The following procedure outlines the steps involved in creating a text changeset with Enterprise Manager. Following the procedure, you can learn about the proper syntax to use and rules to follow when you create a text changeset.

To create a text changeset

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Changesets**.
   The Changeset List screen opens.

2. Above the list, click **Create**.
   The New Changeset screen opens.

3. In the **Name** box, type the name of the changeset.
   This name later appears on the changeset list.

4. In the **Description** box, type a description of the changeset.

5. From the **Source** list, select **Text**.
   The Changeset Source section changes to display a **Text** box.

6. In the **Select Path** list, select a network object class and add it to the Text box by clicking **Add Path**.
   The object class path appears in the **Text** area.

7. In the **Text** box, below the object class path you just added, type the appropriate object information in a format similar to the following example:

   ```
   pool monitor_pool {
      monitor all http
      members
         10.10.10.1:http
         10.10.10.2:http
         10.10.10.3:http
   }
   ```

8. If you want to add additional classes, repeat steps 6 and 7 as necessary.

Click **Finished** to save the new changeset.

Constructing the elements of a text changeset

If you look at the text version of a changeset, you may notice that configuration settings are similar to what you may see in configuration files on a BIG-IP system. However, when Enterprise Manager creates a changeset, it uses additional directives in the text to control how the changeset is deployed to target devices.

Specifying object classes

When you include a network object in a changeset, Enterprise Manager requires that you specify a class directive so that when you deploy the changeset, Enterprise Manager knows where to write this new configuration information on the target device.

For example, if you want to include pools in the changeset, you must specify the class path in the changeset by typing the following text in the changeset:

```
#F5[Local Traffic / Pool]
```

This syntax informs the system that the object configuration that follows this text refers to Local Traffic objects, specifically pools. When you deploy this changeset, the changeset feature uses the bigpipe utility to add this configuration information as a pool configuration on the target device.

Specifying system classes

If you need to copy system settings, you must specify a system class directive in the changeset text, so that when you deploy the changeset, Enterprise Manager adds the system setting to the correct configuration file on the target device.

For example, if you want to include DNS settings in the changeset, you must specify the system class path in the changeset by typing the following text in the changeset:

```
#F5[System / DNS]
```

This syntax informs the system that the configuration data that follows this text refers to system objects, specifically DNS settings. When you deploy this changeset, the changeset feature uses the bigpipe utility to add the DNS settings to the appropriate configuration file on the target device.

Specifying unclassified objects

When you create a changeset, certain objects that you can include do not contain sufficient identification to be deployed directly to a specific configuration file on a target system.

For example, classes containing SSL certificate data require that you specify the object within the class directive. If you include SSL certificates and SSL keys in a changeset, you must specify the name of the target files. In the following example, when you deploy a changeset containing this information, the object data following these directives is copied to the **sample.crt** and **sample.key** files on the target device, respectively:

```
#F5[Local Traffic / SSL Certificate / sample.crt]
#F5[Local Traffic / SSL Key / sample.key]
```

Working with administrative partitions

In addition, if the device supports administrative partitions, Enterprise Manager includes object partition information in the changeset text. If an object belongs to the default, or **Common** partition, you must include the object class directive with the following bigpipe command:

```
shell write partition Common
```

If you include an object for a specific partition, you must precede the object class directive with the following text, where **target_partition** is the name of the partition on the target device.

```
#F5[$target_partition$]
```

This directs the system to generate a **shell write partition** bigpipe command using the partition name you specified when the system verifies or deploys the changeset.

Specifying object settings

After you specify a class path, you must specify an object configuration setting. The syntax for object information in a changeset is similar to object settings in a configuration file on a BIG-IP system. If you currently use the bigpipe utility to change configuration settings on a BIG-IP system, you should be familiar with the syntax used in a changeset.

For detailed instructions on how to create a text changeset, see *To create a text changeset*, on page 6-8.

If you type the following example into the **Text** box on the New Changeset screen, this is the first step in creating a changeset that includes both the virtual server **MyVIP** and its dependent object, the pool **MyPool**.

```
#F5[Local Traffic / Pool]
shell write partition Common
pool MyPool {
   members
     10.1.10.10:http
     10.1.10.11:http
}
#F5[Local Traffic / Virtual Server]
shell write partition Common
virtual MyVIP {
   pool MyPool
   destination 10.20.10.10:http
   ip protocol tcp
}
```

Once you create this changeset, you can then deploy it to any compatible managed device in the network. After you deploy the changeset, the target devices you selected now contain the local traffic objects **MyVIP** and **MyPool**.

Modifying a changeset

When you create a changeset, Enterprise Manager stores the changeset information in text form. The text version of the changeset is a representation of the objects and dependencies that you selected when you created the changeset.

You can modify the text version of a changeset if you need to change any details of an existing changeset. For example, if you need to change the dependencies of an object, or if you need to change details such as an IP address of an object, you can edit the changeset text instead of creating a new changeset.

In order to modify a changeset, you must manually edit the text version of the changeset. You can do this from the Changeset Properties screen.

To modify a changeset

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Changesets**.
   The Changeset List screen opens.

2. Click the name of the changeset that you want to modify.
   The Changeset Properties screen opens.

3. Modify the changeset based on your requirements:

   - To change the description of the changeset, in the **Description** box, type a new description.

   - To add objects to the changeset, in the **Select Path** list, select a network object class and add it to the text field by clicking **Add Path**, then type the object information below the class path you added.

   - To change any objects in the existing changeset, you can change any existing text in the **Text** area.

4. After you finish making changes, click **Save Changes** to save the changeset.

◆ **Tip**

If you want to verify the changeset after you make the changes, save the changeset, then click the ***Verify*** *button to start the Verify Changeset wizard. See* ***Verifying a changeset****, on page 6-12 for more information.*

◆ **Tip**

When you deploy a changeset, you also have the option to modify the text of the changeset before you distribute the configuration data to target devices.

Verifying a changeset

Before you deploy a changeset to other managed devices in your enterprise, you may want to check to see if the saved configuration settings will work when they are copied to a new device.

After you create a changeset and store it in the Enterprise Manager database, you can verify the compatibility of the changeset on any managed device before delivering a new changeset to a managed device.

When you verify a changeset, Enterprise Manager checks to see if the LTM network object classes included in the changeset can work properly with the software installed on a target BIG-IP system. However, the verify feature does not check the validity of any system settings included in the changeset.

A wizard guides you through the verify changeset process, and when you complete the task, you have the option to distribute the changeset to the managed devices on which you verified the changeset.

◆ **Note**

*The verify changeset feature uses the **BIGpipe verify merge** command to check the compatibility of changeset data that you select with target devices.*

Working with the verify changeset wizard

The verify changeset wizard works in a fashion similar to other wizards in Enterprise Manager. To configure a verify changeset task with the wizard, you must select a changeset to verify, then choose a target device and partition.

To verify a changeset

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Changesets**.
   The Changeset List screen opens.
2. Click the name of the changeset that you want to verify.
   The Changeset Properties screen opens.
3. Click the **Verify** button.
   The Step 1 of 2 screen opens.
4. In the **Device Group** box, select a device group to limit the number of devices displayed in the Compatible Devices table.
   The Compatible Devices table changes to display only devices in the device group that you selected.
5. In the **Devices** box, select an option to limit the number of devices displayed in the Compatible Devices table.
   The Compatible Devices table changes to display only devices that meet the criteria you specified.

6. In the Compatible Devices table, check the Select box next to any device for which you want to verify the current changeset.
7. Click **Next**.
   The Step 2 of 2 screen opens, listing the devices you selected and provides an option to select a partition for each.
8. In **Partition** column in the table, select a partition for each device. Enterprise Manager verifies the changeset on this partition for each device you selected on the Step 1 screen.
9. Click **Verify Changeset** to start the task.
   The Verify Changeset task properties screen opens, displaying the verification status of each device that you selected.

◆ **Tip**

*After you verify a changeset, you can immediately start a deploy changeset task using the devices and changeset you selected for the verify task. When you click **Deploy** on the Verify Changeset task properties screen, the Deploy Changeset wizard opens on the Step 3 of 5 screen where you can select the partitions. See **Deploying a changeset**, on page 6-14 for more information.*

Deploying configuration data and settings to target devices

After you create and verify a changeset, you can deliver the device configuration data and settings to any managed device in the network. As an alternative, you can take a current snapshot of a configuration data on managed device and deliver that device configuration data to another managed device.

Depending on whether you want to deliver current data or saved changeset data, you can choose between two wizards to deploy device configuration data.

Deploying a changeset

After you create a changeset, you can copy it to any compatible managed device in the network. The changeset wizard works in a similar manner to other wizards in Enterprise Manager and lets you select compatible devices, partitions, task options, and review your options before you start the task.

If you want to test whether a changeset will work on a managed device before deploying it, you can use the Verify Changeset wizard to test the configuration data before you deploy it. See *Working with the verify changeset wizard*, on page 6-12 for more information.

When you deploy configuration data to a managed device, Enterprise Manager delivers this data to the managed device, overwriting existing settings in configuration files on each managed device. Before Enterprise Manager overwrites this information, it creates a backup of the original configuration settings on each device, which provides you with the option to restore the original configuration if needed.

Selecting a changeset

The first step in delivering a changeset to other devices is selecting the changeset. Once you select the changeset, you can start the wizard from the changeset properties screen.

To select a changeset

1. On the Main tab of the navigation pane, expand **Enterprise Management**, then click **Changesets**.
   The Changeset list screen opens.
2. In the list, click the name of the changeset that you want to deploy to other devices.
   The changeset general properties screen opens.

3. Below the Changeset Text table, click the **Deploy** button to open the deploy changeset wizard.

◆ **Note**

*On the changeset properties screen, you can modify the objects in the changeset, before you distribute it, by changing the text in the **Text** area before you click **Deploy** to start the deploy changeset wizard.*

Choosing compatible target devices

After you select a changeset to deploy, you must select the devices on which you want to copy the changeset data. Like other wizards in Enterprise Manager where you select target devices, the system provides a list of compatible devices from which to select.

To select target devices

1. In the **Device Group** box, select a device group to limit the number of devices displayed in the Compatible Devices table.
2. In the Compatible Devices table, check the Select box next to any device to which you want to distribute the current changeset.
3. Below the table click **Next** to move to the next screen where you select the specific partitions on the devices you selected.

Selecting target partitions

After you select target devices for the configuration change data, you can select specific partitions for each of these devices.

To select device partition targets

1. In the Target Partition Table, in the **Partitioned Object Target** list, accept the default partition currently selected for each target device, or select a new one.
2. Below the table, click **Next** to move to the task options screen.

Setting task options

After you specify the partitions for the change configuration data, you can set options for the task. These options take effect when you start the task, and they determine what actions the system takes during the task.

If the system encounters an error during the task, you can choose to stop the task, or to continue distributing the configuration data on devices. If you choose to continue, the task runs until it deploys the changeset data on as many devices as possible. If you choose to stop the task, an error message appears to assist in reconfiguring the task.

When you deploy a changeset, you may want the option to rollback to a previous device configuration if you later encounter issues on the device. You can choose to create a UCS archive for each target device before the deploy changeset task begins.

When you copy changeset data, you can also choose whether or not to include private SSL keys in the changeset configuration data. If you do not include this data in the changeset, you must add the SSL keys to each target device.

To set task options

1. For the **Device Error Behavior** setting, choose the action that you want Enterprise Manager to take if it encounters an error during the distribute changeset task.
2. For the **Rollback UCS Archive(s)** setting, you can choose to create a UCS archive for each target device before Enterprise Manager distributes the changeset to the managed device.
3. For the **Configuration Archive** setting, you can choose to include private SSL keys in the changeset data or not.
4. Click **Next** to move to the task review screen.

Reviewing task settings

After you have selected the target devices and partitions, and set the task options, you can review all of the settings before you start the Deploy Changeset task. If you need to, you can edit the task name, or you can manually edit the changeset text.

To review or change task settings

1. If you want to change the name of the task, in the **Task Name** box, type a new task name.
   This name appears on the task list when you start the task.
2. If you want to edit the objects included in the changeset, in the Changeset table, click the **Edit** link.
   The Changeset Details screen opens.
   a) In the **Text** area, you can edit the text to modify the objects included in the changeset.
   b) Click **Save Changes** to save changes to the changeset and return to the Task Review screen.
3. After you have reviewed or edited the changeset, you have two options:
   - If you want to verify the changeset, click **Verify Changeset**.
     This runs the **BIGpipe verify** command without committing the configuration change data set.

- If you want to start the task, click **Start Task**. The deploy changeset task starts, and a status screen opens.

Delivering a current device configuration

As an alternative to distributing saved changeset data to managed devices, you can deliver current device configuration data and settings to other devices.

You can create this task using the main task wizard, in a fashion similar to creating a changeset, and then distributing the changeset.

Refer to the procedures for creating a changeset in *Using the changeset wizard to create a changeset*, on page 6-4 to create a current snapshot configuration change data. Then, use the procedures for deploying a changeset in *Deploying a changeset*, on page 6-14. For specific assistance on a screen, consult the online help.

7

Managing Software Images

- Managing software images
- Installing software on managed devices
- Monitoring software and hotfix tasks

Managing software images

Installing a software or hotfix upgrade on individual devices can be a time-consuming task involving downloading an upgrade image, logging on to individual devices, configuring each upgrade task, and monitoring the job as it completes.

With Enterprise Manager as your software image management system, you can catalog and store several versions of software and hotfixes on the Enterprise Manager system, and use these images to perform upgrades to as many managed devices in the network as necessary.

By storing and cataloging all upgrade images in one location, the central repository makes it easier to manage the upgrading of a wide range of managed devices in the network.

After you add software images to the repository, you can then deploy software and hotfix images from the repository to one or more managed devices in the network.

When you set up an automated upgrade process, you can elect several options such as choosing the install location and reboot location. Once you start an upgrade task, you can monitor the progress of each device upgrade on the task list.

Working with the software repository

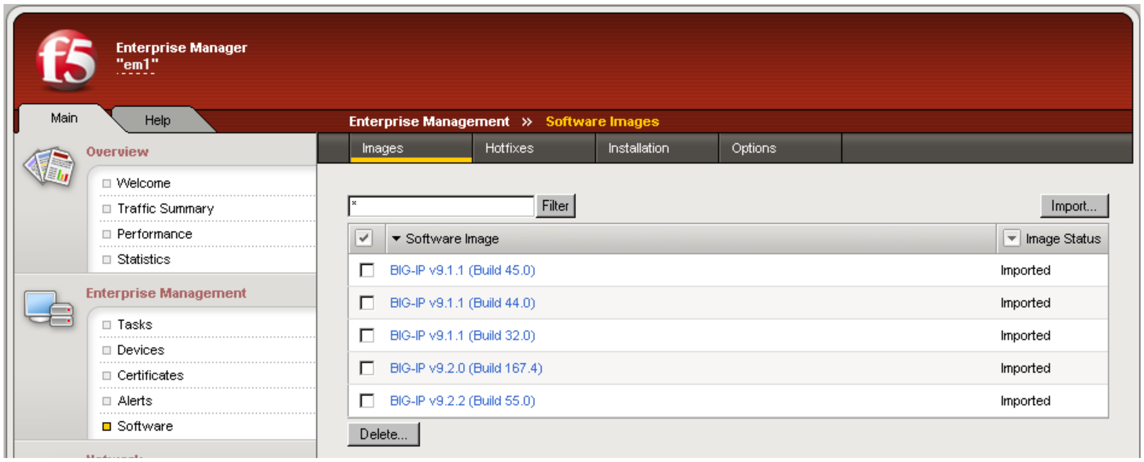
The Enterprise Manager software repository provides a central location where you can store all software upgrade and hotfix installation images. Once you download software or hotfix images from the F5 Networks FTP server, you can store all of the necessary images in the Enterprise Manager repository, enabling you to more efficiently manage the upgrading of devices in the network.

Adding software images to the repository

From the Enterprise Management screen, you can view and deploy multiple software images to as many managed devices in the network as you require.

If additional images become available, you can add them to the software repository for deployment at a later time.

Each image that you add to the repository includes an MD5 signature that you can use to manually check the validity of the software image.



☑	▾ Software Image	▾ Image Status
□	BIG-IP v9.1.1 (Build 45.0)	Imported
□	BIG-IP v9.1.1 (Build 44.0)	Imported
□	BIG-IP v9.1.1 (Build 32.0)	Imported
□	BIG-IP v9.2.0 (Build 167.4)	Imported
□	BIG-IP v9.2.2 (Build 55.0)	Imported

Figure 7.1 The software image list displays the software images stored in the Enterprise Manager software repository

To add software to the software image list

Once you download a software image from the F5 Networks FTP server to your Enterprise Manager system, you can add it to the software repository.

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Software**.
   The Software Images screen opens, displaying all available software update packages.

2. Above the software image list, click **Import**.
   The Import Software Updates screen opens.

3. In the **File Name** box, click **Browse** to search for the image using a directory or folder view.

4. After you enter the path and file name, click **Import**.
   The Software Update List opens and the image name appears in the list with the status of **Importing**. When the importation completes, you can deploy the software to managed devices.

◆ **Important**

When you import a software image, you must leave the browser window open on the file import screen. If you close the window or navigate away from the import screen, this terminates the file transfer. If you need to perform other management tasks, you can open a new browser window.

To add hotfix images to the hotfix list

You manage hotfixes on a separate list from the software upgrade list, but you import hotfix images in a similar fashion.

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Software**.
   The Software Images screen opens, displaying all available software update packages.
2. On the menu bar, click **Hotfixes**.
   The Software Hotfixes screen opens, displaying all available hotfix update packages.
3. Click **Import**.
   The New Hotfix screen opens.
4. In the **File Name** box, click **Browse** to search for the image using a directory or folder view.
5. After you enter the path and file name, click **Import**.
   The Hotfix List opens and the image name appears in the list with the status of Importing. When the importation completes, you can deploy the hotfix to managed devices.

◆ **Important**

When you import a hotfix image, you must leave the browser window open on the file import screen. If you close the window or navigate away from the import screen, this terminates the file transfer. If you need to perform other management tasks, you can open a new browser window.

Removing images from the software repository

If you no longer need to keep software or hotfix images in the software repository, you can delete them from their respective list screens. Once you remove an image from the list, Enterprise Manager deletes the image from its database. If you need to deploy this image in the future, you must re-import it to the software repository.

To delete software or hotfix images

From the software image list, or the hotfix image list, check the box to the left of the image name and click **Delete** below the list.
After you confirm the deletion, Enterprise Manager deletes the software or hotfix image from its database and removes it from the image list.

Installing software on managed devices

Using Enterprise Manager, you can deploy software or hotfix images to multiple managed devices in the network. Instead of logging on to each individual device, you can configure Enterprise Manager to upgrade multiple devices in a software upgrade task. A ***software upgrade task*** is a series of jobs that you configure to upgrade managed devices with software stored in the Enterprise Manager software repository. Each job consists of one individual device upgrade.

A software upgrade wizard streamlines the task of software upgrades while providing enough flexibility so that you can set custom options on each device you plan to upgrade. The wizard guides you through the process of selecting devices to upgrade, including which of the upgrade image or hotfixes to install, which boot location is upgraded, and which boot location is used during the reboot.

You can use the device groups feature to further enhance the upgrade process in that you can deploy a software or hotfix upgrade to an entire device group at once. Then, all of the members of the device group are upgraded during the upgrade task.

Working with multiple boot locations

BIG-IP systems feature a multiple boot capability, which means that you can install the software on multiple disk boot locations on each managed device. A ***boot location*** is a portion of a drive with adequate space required for a software installation (this was previously referred to in other documentation as a boot ***slot***). The BIG-IP 1500, BIG-IP 3400, BIG-IP 6400, BIG-IP 6800, BIG-IP 8400, and BIG-IP 8800 platforms support this functionality, and if you manage any of these systems with Enterprise Manager, you can select the boot location for software upgrades when configuring an upgrade task.

Installing software to high availability systems

To minimize the risk when performing a installation to a system in a high availability configuration, we recommend that you configure only one device in the pair per upgrade task. For example, for an active-standby pair, instead of adding both the active and standby devices to the installation list when configuring the task, upgrade only the software on the standby device. Then, when the upgrade completes, you can switch the device to active mode to test whether the upgrade works properly. Once you confirm that the upgrade works as expected, you can configure a task to upgrade the second device of the pair.

◆ **Important**

If you include both the active and standby systems in the same upgrade task and the upgrade does not work properly on the first device of a high availability pair, you cannot cancel the upgrade on the second device.

Installing software on devices in a tiered configuration

Although Enterprise Manager supports a network topology that features a tiered configuration where a top-tier BIG-IP system load balances requests to multiple lower-tier BIG-IP systems, the software upgrade wizard does not indicate which devices exist on which tier.

If your network topology features a tiered configuration, we recommend that you do not schedule devices on both tiers for upgrade in the same upgrade task. This ensures that Enterprise Manager can maintain a connection to all devices in the network throughout an upgrade task.

Installing software on Enterprise Manager systems

In addition to installing software and hotfixes on managed devices, you can install software and hotfixes to Enterprise Manager systems, including the system you are working on. This means that Enterprise Manager can upgrade itself, as long as you added Enterprise Manager software to the software repository.

When you configure a software upgrade or hotfix installation task, any Enterprise Manager systems in your network appear among the list of devices that you can upgrade (if you elected to discover Enterprise Manager devices in the network). You can configure an upgrade task for Enterprise Manager in the same way that you do for any managed device.

◆ **Note**

Certain options may not be available when you are configuring an Enterprise Manager system for a software upgrade task. For example, if you are installing software on the same system on which you are configuring the upgrade task, you cannot specify a different boot location. Consequently, you may notice that some options are not available when configuring a self-install task.

Performing software version rollbacks

Although the name suggests otherwise, you can use the software upgrade wizard to install previous versions of software on managed devices in the network.

You can configure software version rollbacks, or downgrades, in the same way that you configure software upgrades. However, because of the way the software management process operates, this may cause issues during a software downgrade.

After a typical software installation, Enterprise Manager applies the current device configuration to the newly installed software. After a downgrade task, it is possible that the current device configuration is no longer compatible with the software version. Because of this, we recommend that you manually reconfigure the device after completing a downgrade task.

Installing software to one or more devices

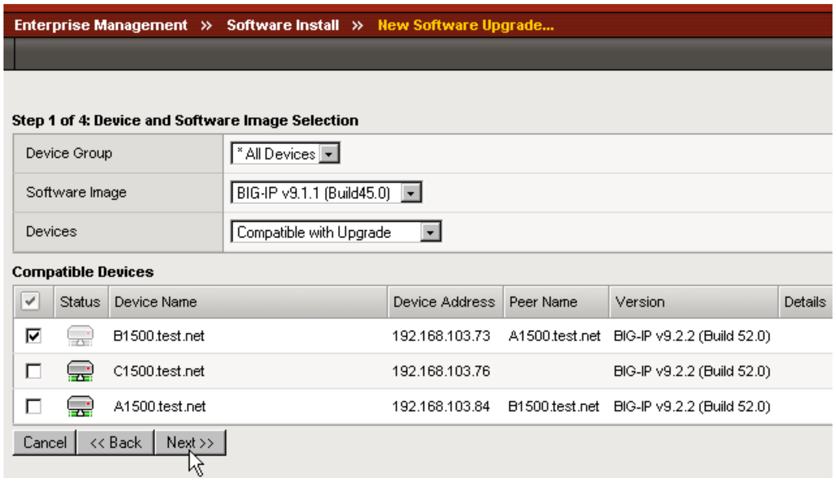
The simplest method of installing software to a device is through the software upgrade wizard. The software upgrade wizard provides four steps to guide you through all the configuration options necessary to start an upgrade task. When you perform a software upgrade, you have the option to include hotfixes in addition to the software.

To start a software image upgrade task

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Software**.
   The Software Images screen opens, displaying all available software update packages.
2. On the menu bar, click **Installation**.
   The software update wizard opens, prompting you to choose a software upgrade or hotfix-only installation.
3. Select **Software Upgrade** and click **Next**.
   The Step 1 of 4 screen opens where you select devices to install to, and the software image to install.
4. Follow the steps on the following pages to work through the wizard screens to install software upgrades.

◆ **Note**

If you want to install hotfixes only, select Hotfix Installation and click ***Next****. See* ***Installing hotfixes to one or more devices*** *on page 7-9 for information on installing hotfixes.*



Enterprise Management » Software Install » New Software Upgrade...

Step 1 of 4: Device and Software Image Selection

Device Group	* All Devices
Software Image	BIG-IP v9.1.1 (Build45.0)
Devices	Compatible with Upgrade

Compatible Devices

☑	Status	Device Name	Device Address	Peer Name	Version	Details
☑		B1500.test.net	192.168.103.73	A1500.test.net	BIG-IP v9.2.2 (Build 52.0)	
☐		C1500.test.net	192.168.103.76		BIG-IP v9.2.2 (Build 52.0)	
☐		A1500.test.net	192.168.103.84	B1500.test.net	BIG-IP v9.2.2 (Build 52.0)	

Figure 7.2 *You can select software and devices in Step 1 of the software upgrade wizard*

To select a software image and devices for the upgrade task

You can select a software image to install, and the devices to install the image to, in Step 1 of 4 of the software upgrade wizard.

1. In the **Device Group** box, select an option to narrow the list of devices:

   - If you want to install to a device group, select the device group name.

   - If you want to install to specific devices, select **All Devices** to see a list of all devices compatible with the upgrade image you select.

2. In the **Software Image** box, select the version that you want to use to upgrade devices.
   The Compatible Devices table changes to show only devices that you can upgrade with the image you selected.

3. In the **Devices** box, choose to display which devices are compatible, or which devices are not compatible, with the software image you selected in the Compatible Devices table,
   The Compatible Devices table changes based on the option you select.

4. In the **Compatible Devices** table, check the Select box to the left of the devices that you want to upgrade with the software you selected in the **Software Image** box.

5. To move to the Step 2 of 4 screen, where you can select any hotfixes that you want to install during the upgrade, click **Next**.

◆ **Note**

If a device does not appear in the Compatible Devices table, check the software version on the device to ensure that you can use the software image you selected for an upgrade.

◆ **Note**

*If a software image does not appear in the **Software Image** box, ensure that the image was imported correctly. You can view this information on the Software Images screen.*

To select hotfix upgrades to include in the upgrade task

You can select hotfix images to include in the upgrade process in Step 2 of 4 of the software upgrade wizard. This screen displays available hotfixes that are compatible with the software you selected on the previous screen.

1. In the hotfix table, check the Select box to the left of one or more hotfixes that you want to install during this upgrade.
   ***Note**: If no hotfixes appear in the table, there are no available hotfixes in the Enterprise Manager repository that are compatible with the software you selected. It is possible that you may not have imported a compatible hotfix image to the software repository.*
2. To move to the next screen, where you can select installation and task options, click **Next**.

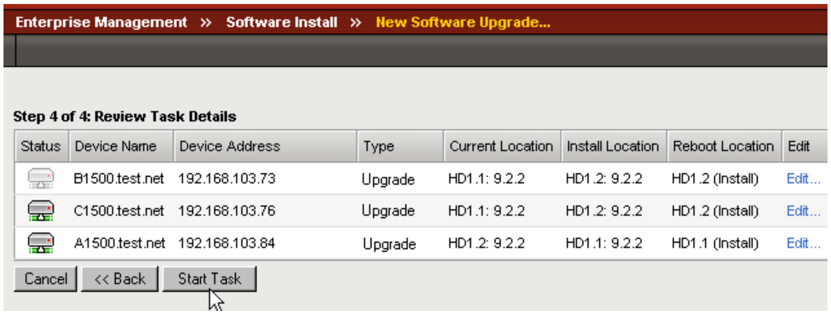
To select installation and task options for the upgrade task

You can specify the install location and select a reboot option in Step 3 of 4 of the software upgrade wizard.

1. In the **Install Location** list, select where you want to install the software upgrade.
   The default is any empty boot location, or the location that hosts the oldest installed software version. If you select **Active Location**, the new software is installed over the software on the currently active boot location.
2. In the **Post Installation** list, select which boot location to use for rebooting the device upon completion of the upgrade process.
3. To move to the Step 4 of 4 screen, where you can review the details of the upgrade task you configured, click **Next**.

◆ **Note**

If you do not select to reboot the managed device using the new software installation, the device reboots using the current default location, which may not be the same as the install location.



Enterprise Management » Software Install » New Software Upgrade...

Step 4 of 4: Review Task Details

Status	Device Name	Device Address	Type	Current Location	Install Location	Reboot Location	Edit
	B1500.test.net	192.168.103.73	Upgrade	HD1.1: 9.2.2	HD1.2: 9.2.2	HD1.2 (Install)	Edit...
	C1500.test.net	192.168.103.76	Upgrade	HD1.1: 9.2.2	HD1.2: 9.2.2	HD1.2 (Install)	Edit...
	A1500.test.net	192.168.103.84	Upgrade	HD1.2: 9.2.2	HD1.1: 9.2.2	HD1.1 (Install)	Edit...

Cancel
<< Back
Start Task

Figure 7.3 *You can review the upgrade options in Step 4 of the software upgrade wizard*

To review the details of the upgrade task

You can review the details of the upgrade task you just configured in Step 4 of 4 of the software upgrade wizard. The Task Details table list the devices selected for upgrade, the current boot location on each device, the install location you selected, and the location that the device will boot to when the upgrade process completes.

1. Review the information on the table.
2. If you want to adjust any options for a specific device, click the **Edit** link to the right of the device boot location information.
   The edit task general properties screen opens, allowing you to change the install or reboot location for the device.
3. When the details look correct, click **Start Task** below the list.
   The Task Properties screen opens, displaying details relevant to the task that you configured.

To open the task list screen

The task properties screen displays information about the task you started, including a detailed list of all the devices you configured a software upgrade on, and the progress of each installation.

- Below the Task Properties table, click the **Exit to Task List** button.
  The task list screen opens, displaying a list of all running tasks on the Enterprise Management system.

Installing hotfixes to one or more devices

Because you may install hotfixes on devices in your network more often than you install full software upgrades, it is important to have a simple method of deploying hotfixes to many devices at once. You can use the hotfix installation wizard to create a hotfix installation task. A ***hotfix installation task*** is a series of jobs that you configure to upgrade one or more managed devices with hotfixes stored in the Enterprise Manager hotfix repository. Each job consists of one individual hotfix installation per device. When you install hotfixes to one or more devices, you can only install on a managed device's currently active boot location.

To start a hotfix installation task

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Software**.
   The Software Images screen opens, displaying all available software update packages.
2. On the menu bar, click **Hotfixes**.
   The Software Hotfixes screen opens, displaying all available hotfixes.
3. Verify that the hotfix that you want to install is available in the list, then on the menu bar, click **Installation**.
   The software update wizard opens, prompting you to choose a software upgrade or hotfix-only installation.
4. Select **Hotfix Installation** and click **Next**.
   The Step 1 of 3 screen opens where you select the hotfix images to install.

◆ **Important**

*If the hotfix image that you want to install is not available in the hotfix list, you may need to import it. See **Adding software images to the repository** on page 7-1.*

To select a hotfix image to install

You can select a hotfix image in Step 1 of the hotfix installation wizard.

1. From the **Product Version** list, select the product version that the hotfix you are planning to install applies to.
   The Available Hotfixes table changes to display hotfixes compatible with the software version you selected.
2. In the Available Hotfixes table, check the Select box to the left of any hotfix that you want to install.
3. To move to the next screen where you select devices to install the hotfix to, click **Next**.

To select devices to install the hotfix to

You can select which devices to install the hotfix to in Step 2 of the hotfix installation wizard.

1. In the **Device Group** list, if you want to install to a device group, select the device group name, otherwise select **All Devices** to see a list of all devices compatible with the hotfix you selected.
2. In the Compatible Devices table, check the Select box to the left of the devices that you want to upgrade with the hotfixes you selected on the Step 2 of 3 screen.
3. To move to the last screen, where you can review the options you set in this hotfix upgrade task, click **Next**.

◆ **Note**

If a device does not appear in the Compatible Devices table, check the software version on the device to ensure that you can use the hotfix.

To review hotfix installation options

You can review and elect to remove a device from the hotfix installation task in Step 3 of the hotfix installation wizard.

1. Review the information on the table.
2. If you want to remove a device from the install task:

   a) Click the **Edit** link to the right of the device boot location information.
   The device task general properties screen opens

   b) Below the Task Details table, click the **Remove** button.
   The Scheduling Review screen opens after you confirm the removal of the device from the hotfix installation task.
3. When the details look correct, click the **Start Task** button below the list.
   The Task Properties screen opens, displaying details relevant to the task that you configured.

To open the task list screen

The task properties screen displays information about the task you started, including a detailed list of all the devices you configured a hotfix installation on, and the progress of each installation. The section *Monitoring software and hotfix tasks*, on page 7-12, provides additional information about the task list and how to work with tasks in the list.

- On the Task Properties screen, below the Task Properties table, click the **Exit to Task List** button.

Monitoring software and hotfix tasks

When you start a software upgrade or hotfix installation, the task properties screen appears automatically to give you details of how much of the task is complete, and if the process is successful. You can also view an overview of the tasks running, or the details of a particular task.

The task list displays an overview of all tasks on Enterprise Manager, including running and completed tasks. When all the install or upgrade jobs in a task finish, the task name and description remains in the task list until you delete it.

Working with software upgrades on the task list

Once you start a software upgrade or hotfix installation, the task is added to the Enterprise Manager task list. If you start more than one upgrade task, additional tasks also appear in the task list.

The progress bar on the task list indicates the overall progress of the task. For example, if you scheduled ten devices for a hotfix installation, the progress bar will indicate 60% when 6 of those devices have completed the hotfix installation.

If you click the name of a task, the task properties screen opens, giving additional details about a task, and providing the opportunity to cancel any pending installations remaining in the task. See the following section for information about modifying a running task.

Once a task finishes, and you no longer need a record of the task, you can delete the task from the task list.

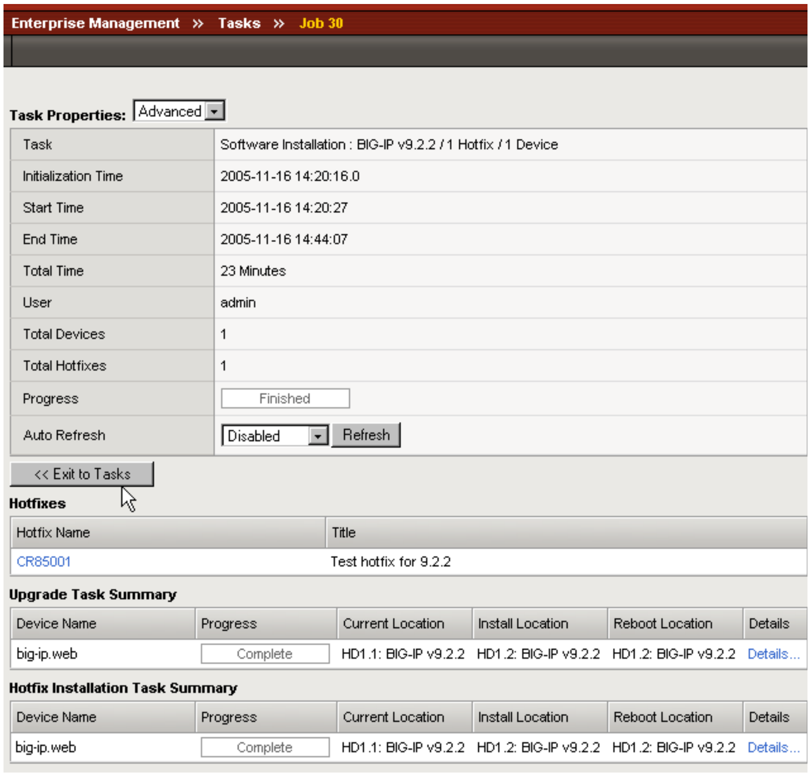
To delete a task from the task list

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens, displaying all running tasks in Enterprise Manager.
2. Check the box to the left of the task that you want to delete, and click **Delete** below the list.
   The task is removed from the list, and the record is deleted from the Enterprise Manager database.

Cancelling pending tasks

You can cancel pending jobs in tasks that are already running by using the task properties screen. Whenever you start a software upgrade or hotfix installation task, the task properties screen opens. Alternately, you can click a task name in the task list to open the task properties screen.

The task properties screen displays details about a running task. For example, if you start an upgrade task on 10 devices, the properties screen displays the overall process and the progress per device.



Task Properties: Advanced

Task	Software Installation : BIG-IP v9.2.2 / 1 Hotfix / 1 Device
Initialization Time	2005-11-16 14:20:16.0
Start Time	2005-11-16 14:20:27
End Time	2005-11-16 14:44:07
Total Time	23 Minutes
User	admin
Total Devices	1
Total Hotfixes	1
Progress	Finished
Auto Refresh	Disabled

Hotfixes

Hotfix Name	Title
CR85001	Test hotfix for 9.2.2

Upgrade Task Summary

Device Name	Progress	Current Location	Install Location	Reboot Location	Details
big-ip.web	Complete	HD1.1: BIG-IP v9.2.2	HD1.2: BIG-IP v9.2.2	HD1.2: BIG-IP v9.2.2	Details...

Hotfix Installation Task Summary

Device Name	Progress	Current Location	Install Location	Reboot Location	Details
big-ip.web	Complete	HD1.1: BIG-IP v9.2.2	HD1.2: BIG-IP v9.2.2	HD1.2: BIG-IP v9.2.2	Details...

Figure 7.4 *The task properties screen displaying details of a software upgrade with hotfix installations*

To cancel pending upgrade tasks

On the task properties screen, click the **Cancel Pending Items** button below the task summary table(s).
After the current device completes its upgrade, Enterprise Manager cancels any software installations or hotfix upgrades for all devices listed in the Task Summary table as **Pending**.

◆ **Important**

You cannot cancel an upgrade once the individual upgrade job starts.

To view details of a specific upgrade or installation

On the task properties screen, in a task summary table, click the **Details** link to the right of any software upgrade or hotfix installation job.
The task details screen opens, providing additional details specific to that job, including any suggestions if the job failed.

8

Managing User Account Data

- Managing user accounts
- Copying user configuration information
- Changing user account passwords

Managing user accounts

When you manage a large number of BIG-IP systems, you usually create and manage user accounts individually on each of these devices. When managing users on individual devices, it may be time consuming to keep track of each user and their privileges on each device.

Using Enterprise Manager as a user management proxy can save valuable time by providing you lists of all users in your network, and each device on which they have access privileges.

Additionally, you can view user accounts in the context of device groups to see which users have access to which devices in a custom device group.

See the *Managing User Accounts* chapter in the ***BIG-IP® Network and System Management Guide*** for information on managing user accounts, understanding user account types and user roles, and managing an authentication source.

Working with the user list

The ***user list*** displays all users configured on all managed devices in the network. The user list also displays how many devices or device groups the user has access to.

When you use the user list and the user details screens linked from the user list, you do not need to log on to individual devices to review all user accounts in the network.

To open the user list

On the navigation pane, expand **Enterprise Manager** and click **Users**.

On the user list screen, numbers in the Devices and Device Group columns indicate how many devices or device groups a user has access to. Each of these numbers is a link that opens a screen that displays the specific devices or device groups, including the user's roles on each.

To view user-specific roles on devices or device groups

On the user list screen, select what you want to view:

- If you want to view a list of devices that a user has access to, click either the user name or the number in the Devices column.
- If you want to view a list of device groups that a user has access to, click the number in the Device Groups column.

Regardless of which option you choose, the user properties list opens, listing the user's web access and shell (or console) access roles on each device or device group.

◆ **Note**

On the user-specific device groups screen, a role may be labeled as ***Mixed****. This indicates that the user has different roles on at least two unique devices that are members of that device group.*

To view a user's roles within a device group

If you are viewing the device group user properties list, you can further drill down to view a user's roles on each member of the device group.

From the user properties list screen, click the user role in either the Web Role or Shell role column.
The device group user access screen opens, listing all of the members of the device group and the user's role on each device.

Viewing users on a device

In addition to viewing all users, or users in device groups, you can view users in the context of a device.

To view a list of user accounts on a device

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Devices**.
   The device list screen opens.
2. Click the name of the device for which you want to view a user list.
   The device properties screen opens.
3. On the menu bar, click **Launch Pad**.
   The Launch Pad screen opens.
4. In the Device Settings table, in the Type column, click the **Users** link.
   The device user list opens to display all the users on the currently selected device.

Configuring user account information on managed devices

On some user screens, Enterprise Manager provides a link to the managed device's Configuration utility. You can use this link to manage a specific user account on the managed device.

To manage account information on a managed device

On the user properties list screen, or the device group user access screen, click the **Launch** link to open the managed device's configuration utility to manage the adjacent user account.

Copying user configuration information

When you configure user account information on a BIG-IP system, you can set parameters, such as a user's web interface and root access privileges and specify an authentication source. When you configure these BIG-IP systems individually, you have to configure this information on each device.

However, if you use the Enterprise Manager Copy User Access Configuration wizard, you can copy user account information from one device to as many devices as you require, easily adding new users or user account information to BIG-IP systems in the network.

The configuration data that you can copy includes user names and passwords, shell access information, and authentication source information.

By using the Copy User Access Configuration Wizard, you can save valuable time by creating a common user account configuration on one source device, then copying that configuration data to other devices in the network.

Working with the Copy User Access Configuration wizard

The Copy User Access Configuration wizard functions in a manner similar to the software installation wizard. Basically, you select a source device that contains the user account data that you want to copy, then choose destination devices where you want to copy the information, set task options, and start the task.

Once you start the copy configuration task, the task appears in the task list where you can monitor its progress.

Starting a copy configuration task involves four main steps: starting the wizard, selecting a target and source device, setting task options, and reviewing task settings before starting the task.

To start a copy device configuration task

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Tasks**.
   The task list screen opens.

2. Above the list, click the **New Task** button.
   The New Task screen opens.

3. On the New Task screen, select the **Copy User Access Configuration** option and click **Next**.
   The Step 1 of 3 screen opens where you can select source and destination devices, and choose what type of configuration data to copy.

4. Follow the steps on the following pages to work through the wizard screens to copy user access configuration data.

To select devices and configuration data

Once you start the copy configuration wizard, you can select a source device, the type of data you want to copy, and the devices on which to copy the data.

1. In the **Source Device** box, select the device that you want to use as the data source for user configuration data.
2. For **Configuration Data**, check the Select box next to each type of user configuration data that you want to copy from the source device: **Users**, **Shell Access**, **Authentication**.
3. In the **Device Group** list, select an option to narrow the list of target devices in the Compatible Devices table:
   - If you want to copy to devices in a device group, select the device group name.
   - If you want to install to specific devices, select **All Devices** to see a list of all devices compatible with the configuration data you selected.
4. In the **Devices** box, select an option to view a list of target devices that are compatible or not compatible with the configuration data you selected.
5. In the **Compatible Devices** table, check the Select box next to each device that you want to copy configuration data to and click **Next**. The Step 2 of 3 screen opens where you can specify task options.

To set task options

You can specify task options on the Step 2 of 3 screen of the wizard.

1. In the **Device Users** box, select an option for copying user accounts to a destination device:
   - **Add users not already present on the device** - adds users from the source device to the user list on each destination device without changing any user account information already configured on the destination device
   - **Replace users on device** - copies the entire user account list from the source device to the destination device, overwriting any user accounts currently existing on the destination device.
2. In the **Device Error Behavior** box, select an option to determine how the system handles errors during the task:
   - **Continue task on remaining devices** - the task continues until the system finishes copying device configuration data to destination devices that you selected. Specific errors appear on the task properties screen.

- **Cancel task on remaining devices** - the task stops after the first error occurs. Specific errors appear on the task properties screen. You must configure a new task to copy data to devices that were canceled.

3. Click **Next** to open the task review screen.

To review task options

You can review task options and start the task on the Step 3 of 3: Task Review wizard screen. This screen summarizes the task, including the source device, the configuration data to be copied, and the destination devices.

- If you need to remove any user accounts from the configuration copy task, in the Configuration Data table, click the **Details** link adjacent to the Users entry.
  The Configuration Data screen appears where you can specify users to include in the task.
- If these settings look correct, click **Start Task**.
  The Task Properties screen opens and displays information about the configuration copy task.

Using the Launch Pad to start a user configuration copy task

In addition to the Copy Device Configuration wizard, you can initiate a configuration copy task for a specific device from the device Launch Pad screen. The Launch Pad screen provides an overview of user accounts, shell access settings, and authentication information for a device.

From the Launch Pad, you can start a copy task to copy the device's user configuration data to another device, or you can open the device's Configuration utility.

To start a copy task from the Launch Pad

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Devices**.
   The device list screen opens.
2. Click the name of the device that contains user configuration data that you want to copy to another device.
   The device properties screen opens.
3. On the menu bar, click **Launch Pad**.
   The Launch Pad screen opens.
4. In the Device Settings table, check the Select box next to each device setting that you want to copy.

5. Below the list, click **Copy**.
   The Step 1 of 3 screen of the Configuration Copy wizard opens with the **Source Device** and **Configuration Data** settings already selected.

◆ **Tip**

If you want to select specific users to copy during the copy configuration task, click the ***Users*** *link in the Device Settings table to open the device user list where you can select specific user accounts to include in the task.*

Changing user account passwords

If you manage user accounts on individual devices, certain tasks can become time consuming if you have a large number of devices. For example, if you need to change a user's password on multiple devices in your network, this may require logging on to each device in succession to manage a single user's account.

However, with Enterprise Manager as your user management proxy, you create a task to automate the password change process for any user on any managed device in the network. This can save you a good amount of time when managing user passwords, while ensuring that you when you change a password, the new password is identical on each device that you select.

Working with the Change User Password wizard

Enterprise Manager provides a wizard to assist you with changing user passwords. The Change User Password wizard works in a way similar to other wizards in Enterprise Manager. It involves four main steps presented on subsequent screens in the wizard:

- Selecting the user whose password you want to change and specifying the devices on which you want to change the password.
- Specifying the new password.
- Setting task options.
- Reviewing the task settings.

To start a copy device configuration task

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Tasks**.
   The task list screen opens.
2. Above the list, click the **New Task** button.
   The New Task screen opens.
3. On the New Task screen, select the **Change User Password** option and click **Next**.
   The Step 1 of 4 screen opens where you can select the user and the devices on which you want to change the user's password.

Follow the steps on the following pages to work through the wizard screens to change a user's password.

To select a user and devices

Once you start the change user password wizard, you can select a user account, and the devices on which to change the user's password.

1. In the **User Name** box, select the user whose password you want to change.

2. In the **Device Group** list, select an option to narrow the list of devices in the Compatible Devices table:
   - If you want to select from a list of devices in a device group, select the device group name to see a list of devices in that group on which the user has an account.
   - If you want to select from a list of all devices, select **All Devices** to see a list of all devices on which the user has an account.
3. In the **Devices** box, select an option to change the list of devices to devices displayed in the table:
   - **Compatible Devices** - Select this option to display devices on which the user account exists.
   - **Incompatible Devices** - Select this option to display devices on which the user account does not exist.
4. In the Compatible Devices table, check the Select box next to each device for which you want to change the user's password, and click **Next**.
   The Step 2 of 4 screen opens where you can specify the new user password.

To specify a new password

1. For the **Authentication** setting, in the **Password** box type the new user password.
2. In the **Confirm** box, re-type the password.
3. Click **Next** to move to the Task Options screen.

To set task options

Task options direct the system to take an action when a task is running.

1. In the **Device Error Behavior** box, select an option to determine how the system handles errors during the task:
   - **Continue task on remaining devices** - the task continues until the system finishes changing the user password on as many devices that you selected. Specific errors appear on the task properties screen.
   - **Cancel task on remaining devices** - the task stops after the first error occurs. Specific errors appear on the task properties screen. You must configure a new task to change a user password on devices that were cancelled.
2. Click **Next** to open the task review screen.

To review task settings

You can review task options and start the task on the Step 4 of 4: Task Review wizard screen. This screen summarizes the task, including the user account for which you are changing the password, and the devices on which you are changing the user's password.

1. If you need to change the password you specified on the Step 2 screen, click the **Details** link adjacent to the **User Name** entry.
   The Edit Task Item screen appears where you can specify a new password for the task.
2. If these settings look correct, click **Start Task**.
   The Task Properties screen opens and displays information about the password change task.

9

Monitoring and Alerting

- Monitoring device status
- Monitoring management tasks
- Configuring custom alerts

Monitoring device status

When you use Enterprise Manager to manage devices in the network, you can get a general overview of the status of devices from the device list screen. You can view the device list by clicking the **Devices** link in the **Enterprise Management** section of the Main tab on the navigation pane.

If you need to notify individuals in your organization about certain conditions in the network, you can configure custom alerts for managed devices in the network. This can help you improve response time when a certificate expires on a managed device, or if a managed device becomes unreachable. Additionally, you can configure these alerts to work with any existing network management servers in the network.

Understanding status icons in the device list

Status icons offer the quickest insight into the state of managed devices in the network. The icons indicate whether Enterprise Manager can successfully communicate with managed devices and, if the devices are part of a high availability system, their active or standby failover state.

If Enterprise Manager might not be able to communicate with a managed device, the status icon changes so that a red X appears in the middle of the device icon. There are a variety of reasons that Enterprise Manager might not be able to communicate with a managed device: the device is rebooting, the management cable became disconnected, or the iControl port was closed or blocked. If you notice a device unreachable icon, you can try to remotely log into the device to further investigate the device's status.

State	Status Icon
Enterprise Manager can contact the device, and the device is in Active Mode	🟩
Enterprise Manager can contact the device and the device is in Standby Mode	⬜
Enterprise Manager cannot currently contact the device	❎

Table 9.1 *The three types of status icons provide a basic overview of device status in the device list*

Monitoring management tasks

One of the advantages of using Enterprise Manager as a device management appliance is that you can monitor the progress of several management tasks at once. You can use the task list to survey the status of running, completed, and pending tasks.

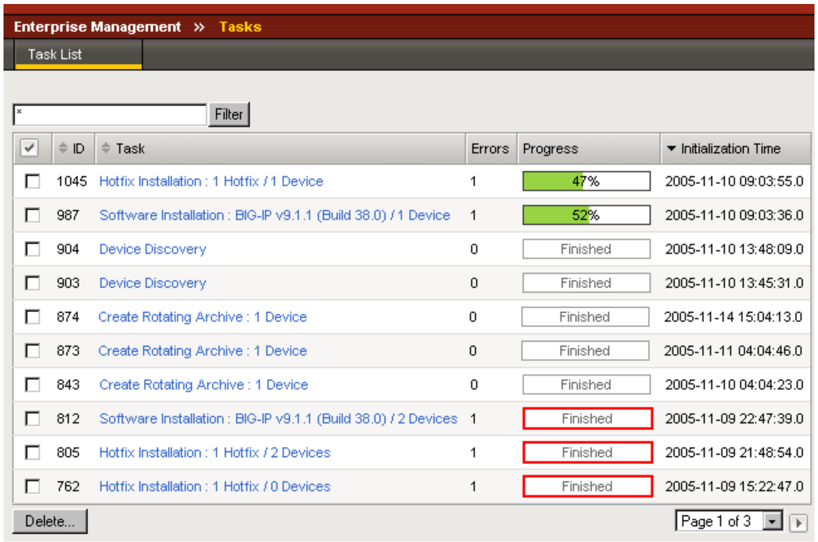
You can also use the task list as a starting point to finding additional information about a particular task, or for setting up new tasks such as a software upgrade or rotating archive schedule.

Using the task list

The task list provides an overview of all tasks initiated by Enterprise Manager. You can also use the task list as a starting point for software upgrades and for scheduling rotating archives.

To open the task list

In the navigation pane, expand **Enterprise Management** and click **Tasks**.



☑	ID	Task	Errors	Progress	Initialization Time
□	1045	Hotfix Installation : 1 Hotfix / 1 Device	1	47%	2005-11-10 09:03:55.0
□	987	Software Installation : BIG-IP v9.1.1 (Build 38.0) / 1 Device	1	52%	2005-11-10 09:03:36.0
□	904	Device Discovery	0	Finished	2005-11-10 13:48:09.0
□	903	Device Discovery	0	Finished	2005-11-10 13:45:31.0
□	874	Create Rotating Archive : 1 Device	0	Finished	2005-11-14 15:04:13.0
□	873	Create Rotating Archive : 1 Device	0	Finished	2005-11-11 04:04:46.0
□	843	Create Rotating Archive : 1 Device	0	Finished	2005-11-10 04:04:23.0
□	812	Software Installation : BIG-IP v9.1.1 (Build 38.0) / 2 Devices	1	Finished	2005-11-09 22:47:39.0
□	805	Hotfix Installation : 1 Hotfix / 2 Devices	1	Finished	2005-11-09 21:48:54.0
□	762	Hotfix Installation : 1 Hotfix / 0 Devices	1	Finished	2005-11-09 15:22:47.0

Figure 9.1 *The task list provides an overview of running and completed tasks.*

The task list provides information relevant to the task, including the overall progress of the task, and the task initialization time. If you click the name of a task, the task properties screen opens to provide additional task details and options.

When a task completes, a record remains in the task list to assist you in tracking when upgrades, device discoveries, and configuration archive management tasks occurred. These records remain in the list until you delete them.

To remove a task from the task list

Check the Select box to the left of a completed task name, and click the **Delete** button below the list.
Enterprise Manager deletes the task from the Enterprise Manager database, and removes the task from the task list.

◆ **Note**

Although deleting a task from the list removes the record, Enterprise Manager maintains the audit record of all tasks initiated by Enterprise Manager.

Working with the task properties screens

When you click a task name in the task list, the task properties screen opens. This screen gives you additional details about the task you selected. Depending on the type of task you are looking at, the task properties screen can display the status of each individual device in a discovery task, software upgrade, or hotfix installation.

If errors occur in the task, you can click the **Details** link in the Task Summary table to view even more detailed information and find suggestions about a particular job.

If there are pending jobs in the task, you can cancel any pending jobs by clicking the **Cancel Pending Items** button below the Task Summary table.

Configuring custom alerts

Using Enterprise Manager as your network management appliance gives you custom alerting options to help you better maintain the health of your network. You can configure custom alerts to notify you or others if a device becomes unreachable by Enterprise Manager, the completion or failure of a software or hotfix installation, and if a device system clock differs from the Enterprise Manager clock.

When you configure custom alerts, you can apply them to individual devices, or to a device group.

You can also create alerts for the Enterprise Management device itself so that you can maintain the health of your management system.

Setting up alert defaults

Before you create alerts, you can configure alert defaults for an alert email recipient and you can specify the address of a remote syslog server for alerting.

When an alert is triggered, if you define a default email address, Enterprise Manager can send an alert notification to this address. Optionally, Enterprise Manager can send a syslog event to a remote syslog server that you specify when an alert is triggered.

◆ **Important**

*For information on setting up system settings required to enable alerting features such as sending email messages or SNMP traps, see **Setting alerting system options**, on page 3-12.*

To set alert default options

1. In the navigation pane, expand **Enterprise Management**, and click **Alerts**.
   The Device Alerts list screen opens.

2. On the menu bar, click **Options**.
   The Alert Options screen opens.

3. In the **Email Recipient** box, type the default email address to use when you select email as an alert action.
   ***Note**: You can specify an email address different from the default when you create a custom alert.*

4. In the **Syslog Server Address** box, type the IP address of the remote syslog server if you want to use syslog events for alerting.

5. In the **Alert History** box, type the number of history entries that Enterprise Manager stores in the Alert History list.

◆ **Tip**

If you want to send email to more than one person when an alert is triggered, you can use an alias as the default email address, then you can configure multiple addresses on your mail server.

Configuring system alerts

To help maintain the health of the Enterprise Manager device, you can configure system alerts to notify you when CPU, disk, or memory usage meets or exceeds a particular threshold. You can set these options on the EM Alerts screen.

To set system alerts

1. In the navigation pane, expand **Enterprise Management**, and click **Alerts**.
   The Device Alerts list screen opens.
2. On the menu bar, click **EM Alerts**.
   The EM Alerts screen opens.
3. Depending on which metrics that you want to track with alerts, change the values in the **CPU Usage**, **Disk Usage**, or **Memory Usage** boxes.
4. In the **Action** box, select the type of action that you want Enterprise Manager to take when the values you specified in the **CPU Usage**, **Disk Usage**, and **Memory Usage** boxes are met or exceeded.

◆ **Note**

Because the CPU or memory usage may spike repeatedly during certain Enterprise Management tasks, many alerts may be triggered, which could result in multiple emails, SNMP traps, syslog events, or alert history entries.

Understanding the types of device alerts

Enterprise Manager can take actions on a wide variety of alerts that can assist you in managing your F5 Networks devices. The alerts that you can set include:

- Device unreachable by Enterprise Manager
- Certificate expired or near-expiration
- Completed software installations or hotfix upgrades
- Failed software installations or hotfix upgrades
- Clock skew between the Enterprise Manager and managed devices
- Failed rotating archive creation

Alerting for Device Unreachable

If Enterprise Manager loses the connection to a managed device, the status icon in the device list changes to indicate this problem. However, if you need to immediately notify someone as soon as Enterprise Manager loses a connection to a managed device, you can configure a custom alert to notify you or others. Recipients of this alert email can then take the necessary action to get your managed device back online. This is a continuous alert that checks the connection every 10 minutes and triggers another alert if the device is unreachable.

Because Enterprise Manager authenticates itself to managed devices on the iControl port through a certificate that it creates when it first discovers a device in the network, there are a variety of reasons that the connection could be interrupted.

The connection could be interrupted if the managed device is rebooting, or if someone closed the management port or removed the management cable. It is also possible that a system clock differential between Enterprise Manager and a managed device caused the management certificate to expire.

◆ **Note**

The device refresh interval takes precedence over the continuous checking done by this alert. That is, if the refresh interval is set higher than 10 minutes, this alert checks for a connection within the refresh interval.

Warning of expired or near-expired certificates

Because it is likely that you have a large number of certificates defined on managed devices in the network, you may want a way to automatically monitor these certificates and warn you when they near expiration.

Although you can use the certificates list to view a broad overview of certificates on devices in the network, you can create a custom alert to notify a specific user when a certificate expires or is within a specific number of days of expiration.

When you define the alert, you can specify a notification to repeat at specified intervals until the certificate expires.

Notifying of completed installations and upgrades

When you start a software upgrade or hotfix installation task, you may not be able to monitor the overall status of the task. If you start an upgrade of multiple devices, it may not be feasible to manually check to see if a particular device is upgraded. You can create a custom alert to notify you or others when a device completes an upgrade or installation task.

Alternately, you can use the Task List to get a broad overview of all running tasks. If you click the name of a task on the task list, it opens the task properties screen where you can view detailed information about devices involved in the task, including which devices have completed the upgrade or installation.

Alerting on failed installations and upgrades

Because you can upgrade multiple devices in a software upgrade or hotfix installation, you may not be able to closely monitor each job. You can create a custom alert to notify you or others if an upgrade or installation job fails. The user that receives the alert email can then investigate why the upgrade or installation failed, make corrections, and schedule a new task.

You can also use the Task List to find running tasks that encountered errors during an upgrade or install process.

Warning of clock skew between the Enterprise Manager and managed devices

When Enterprise Manager adds a device to the managed device list, it creates a certificate that it uses to authenticate itself to the managed device. If the system clock of Enterprise Manager gets too far out of sync (15 minute difference between system clocks) with a managed device, this invalidates the management certificate, and can result in Enterprise Manager losing management privileges on a device.

To prevent this scenario, you can set an alert that will notify you or others whenever the Enterprise Manager and managed device system clocks skew too far out of sync. Then, whoever receives the alert can log on to the managed device and make sure the system clock is closely matched with Enterprise Manager. This is a continuous alert that checks the clock skew every 10 minutes, and triggers another alert if the systems clocks are out of sync.

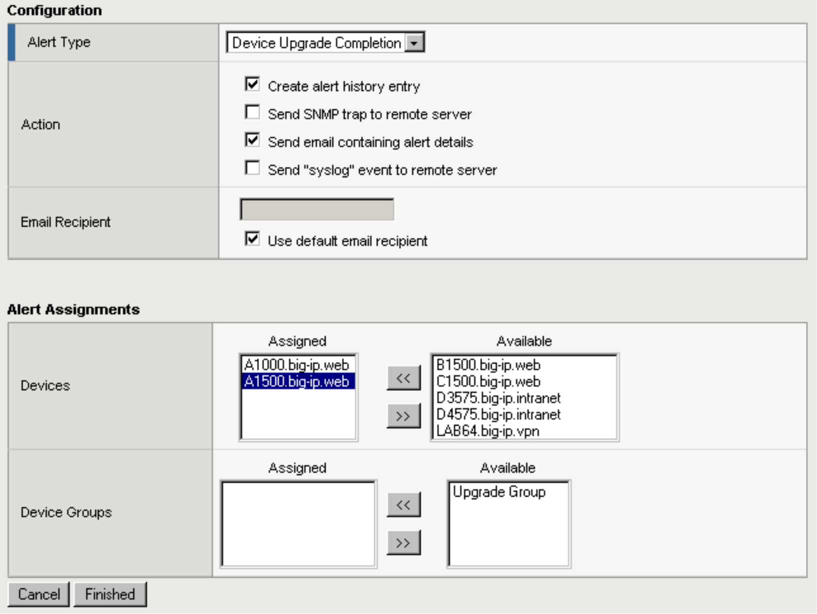
Notifying of a failed rotating archive creation

When you configure a rotating archive schedule, Enterprise Manager creates a device configuration at the interval you specified. Because this is an automated process, you may not know if the configuration archive was created properly.

You can create a custom alert to notify you or others whenever a scheduled configuration archive process encounters an error. A user who receives an alert email can investigate why an archive was not created or can manually create a configuration archive.

Creating alerts for devices or device groups

Creating an alert for a device or device group involves naming the alert, defining the alert condition, setting the alert action, and assigning the alert to one or more devices. You can do this from one screen, the New Alert screen.



Configuration

Alert Type	Device Upgrade Completion
Action	☑ Create alert history entry ☐ Send SNMP trap to remote server ☑ Send email containing alert details ☐ Send "syslog" event to remote server
Email Recipient	☑ Use default email recipient

Alert Assignments

	Assigned	Available
Devices	A1000.big-ip.web A1500.big-ip.web	B1500.big-ip.web C1500.big-ip.web D3575.big-ip.intranet D4575.big-ip.intranet LAB64.big-ip.vpn
Device Groups		Upgrade Group

Figure 9.2 *Defining the alert type and actions, then assigning devices to the alert on the New Alert screen*

To create an alert for a device or device group

1. In the navigation pane, expand **Enterprise Management**, and click **Alerts**.
   The Device Alerts list screen opens.

2. Above the alert list, click the **Create** button.
   The New Alert screen opens.

3. In the General Properties section, in the **Name** box, type a name for the alert. Once you create the alert, you cannot change the name. The name appears in the alert list on the Device Alerts screen.

4. In the Configuration section, in the **Alert Type** box, select the alert condition.
   Depending on the type you select, the section may change to provide additional options.

5. If the alert type requires a threshold, in the **Condition** box, specify a threshold value.

6. For **Action**, check the box next to the actions that you want Enterprise Manager to take when the alert is triggered.

7. If you selected to send an email, then for **Email Recipient**, you can choose to use the default email recipient, or type the email address of a specific user:

   a) To send an email to the default email recipient listed on the Alert Options screen, check the Select box.

b) To send an email to an alternate recipient, clear the Select box and type a new email address.

8. If you selected to log a remote syslog event, then for **Syslog Server Address**, you can choose to use the default syslog server address, or type the server address of a different remote server:

    a) To log an event on the default syslog server listed on the Alert Options screen, check the Select box.

    b) To log an event on an alternate server, clear the Select box and type a new syslog server address.

9. In the Alert Assignments area, assign this alert to devices or device groups:

    a) In either the **Devices** or **Device Groups** box, click a device or device group in the **Available** box to select it.

    b) Click the Move button (<<) to move the selected devices or device groups to the **Assigned** box.
    The alert now applies to devices and device groups listed in the **Assigned** box.

10. Click **Finished**.
    The Device Alerts screen opens, and the new alert appears in the list.

Modifying or deleting alerts

Once you create an alert, the alert definition is flexible enough to easily apply to additional devices and device groups. Conversely, you can remove devices and device groups from a particular alert. You can also change the alert actions or email recipients of an alert, on the alert properties screen. From the Device Alerts screen, clicking the name of an alert opens the alert properties screen.

To modify an alert

1. In the alert list, click the name of the alert that you want to modify. The Alert Properties screen opens.
2. Change any of the values in the Configuration section, or add or remove devices and groups from the alert in the Alert Assignments sections.
3. Click **Save Changes** to save your changes.

See the online help for additional details about changing specific properties of an alert.

If you no longer need an alert, you can delete the alert using the Device Alerts screen. Once you remove an alert from the alert list, it no longer applies to any devices or groups that you assigned.

To delete an alert

From the Device Alerts screen, in the alert list, check the Select box to the left of an alert, and click the **Delete** button below the list.

10

Managing Device Certificates

Working with device certificates

Because the BIG-IP Local Traffic Manager (LTM) can control your SSL traffic, you may have a large number of SSL and web certificates on many different LTM devices your network.

Enterprise Manager can provide a quick overview of all the server certificates and web certificates on each managed device in the network. You can use Enterprise Manager to monitor which certificates are nearing their expiration date, and which ones have expired. Using this overview can save you time over monitoring certificate expiration dates on individual LTM devices.

Monitoring device certificates

When Enterprise Manager adds a device to the device list, you have the option to monitor the expiration status of all the certificates on the managed device. You can view the status of both traffic certificates and system certificates. ***Traffic certificates*** are server certificates that a managed device uses in its traffic management tasks. ***System certificates*** are the web certificates that allow client systems to log into the BIG-IP system Configuration utility.

Enabling certificate monitoring

By default, certificate monitoring is enabled for all managed devices, however, you may specify which specific device or device groups you want to monitor. If you choose to monitor a device group, you automatically monitor all of the certificates on all of the devices that are members of the device group.

To enable certificate monitoring

You can control which devices or device groups participate in certificate management from the same screen.

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Certificates**.
   The Traffic Certificates list screen opens.
2. On the menu bar, click **Options**.
   The Certificate Options screen opens.
3. For the **Devices** or **Device Groups** settings, in the **Disabled** box, click the name of a device or device group.
4. Click the Move (<<) button.
   The selected device or device group moves to the **Enabled** box.
5. Click **Save Changes**.
   Enterprise Manager now monitors certificates defined on the devices and device groups that you moved to the **Enabled** box.

If you no longer want to monitor certificates on a device or device group, you can disable a device or device group's participation on the same screen that you enable it. If you disable certificate monitoring for a device, certificates for the device no longer appear on certificate lists, and certificate expiration alerts for this device no longer apply.

To disable certificate monitoring

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Certificates**.
   The Traffic Certificates list screen opens.
2. On the menu bar, click **Options**.
   The Certificate Options screen opens.
3. In the **Devices** or **Device Groups** row, in the **Enabled** box, click the name of a device or device group.
4. Click the Move (>>) button.
   The selected device or device group moves to the **Disabled** box.
5. Click **Save Changes**.
   Enterprise Manager no longer monitors certificates defined on the devices and device groups that you moved to the **Disabled** box.

Working with the certificate list screens

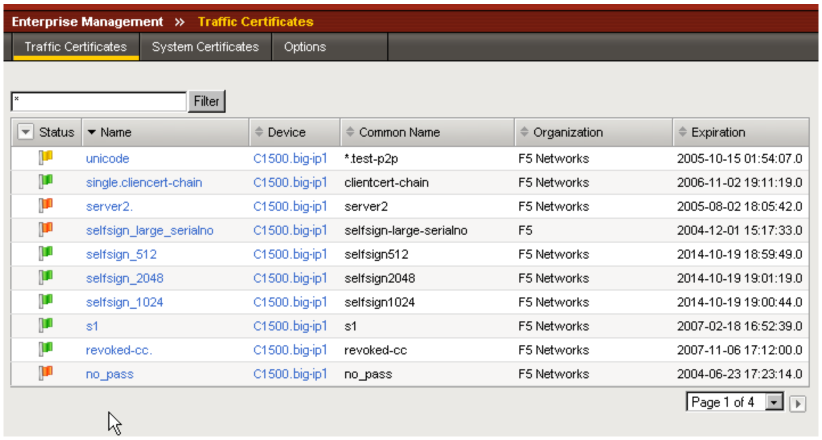
You can view either traffic certificates or system certificates on their own certificate list screens. These screens provide a quick overview of vital certificate information such as the expiration status, name, the device the certificate is configured on, the common name, and expiration date and time.

Status flags offer the quickest view on the status of a certificate. Table 10.1 outlines the status flags.

Status Flag	Expiration Status
🟥	The Red Status Flag indicates that the certificate has expired. When client systems require this certificate for authentication, the client receives an expired certificate warning.
🟨	The Yellow Status Flag indicates that a certificate will expire in 30 days or less. The certificate is still valid, but you should take action to prevent certificate expiration.
🟩	The Green Status Flag indicates that a certificate is valid and will remain valid for at least 30 more days.

Table 10.1 *Certificate status flags*

When working with the certificate list screens, you can sort the list by clicking the respective column headings, or you can filter the list to display only certificates with a particular status flag.



Status	Name	Device	Common Name	Organization	Expiration
🟨	unicode	C1500.big-ip1	*.test-p2p	F5 Networks	2005-10-15 01:54:07.0
🟩	single.cliencert-chain	C1500.big-ip1	clientcert-chain	F5 Networks	2006-11-02 19:11:19.0
🟧	server2.	C1500.big-ip1	server2	F5 Networks	2005-08-02 18:05:42.0
🟧	selfsign_large_serialno	C1500.big-ip1	selfsign-large-serialno	F5	2004-12-01 15:17:33.0
🟩	selfsign_512	C1500.big-ip1	selfsign512	F5 Networks	2014-10-19 18:59:49.0
🟩	selfsign_2048	C1500.big-ip1	selfsign2048	F5 Networks	2014-10-19 19:01:19.0
🟩	selfsign_1024	C1500.big-ip1	selfsign1024	F5 Networks	2014-10-19 19:00:44.0
🟩	s1	C1500.big-ip1	s1	F5 Networks	2007-02-18 16:52:39.0
🟩	revoked-cc.	C1500.big-ip1	revoked-cc	F5 Networks	2007-11-06 17:12:00.0
🟧	no_pass	C1500.big-ip1	no_pass	F5 Networks	2004-06-23 17:23:14.0

Figure 10.1 *The Traffic Certificates screen outlines important certificate information*

To filter the list by status flag

1. In the Status column, click the down arrow.
   A menu appears indicating the status flags.

2. From the menu, choose a status flag.
   The table changes to display only certificates that match the status flag you selected.

To view detailed certificate information

If you want to view additional details about a particular certificate, click the name of a certificate to open the certificate properties screen.

Creating alerts for certificate expiration

If you require more precise notification of certificate expiration dates, you can create a custom alert. When you create a custom alert on the New Alert screen, in the **Alert Type** box, select **Certificate Expiration**. Once you select this type of alert, you can configure an alert based on the number of days until the certificate expires. For detailed instructions on how to create alert instances and configure alert actions, see *Configuring custom alerts*, on page 9-4.

◆ **Note**

You cannot configure certificate-based alerts on devices or device groups until you enable certificate monitoring on those devices or device groups.

11

Auditing Enterprise Manager System Events

Working with Enterprise Manager system logging

Enterprise Manager provides a comprehensive set of auditing features so that you can track what types of enterprise management tasks were initiated from a particular Enterprise Manager system.

Viewing and managing log messages each provides you with continuous information about system events. Some events pertain to general operating system events, and some are specific to the Enterprise Manager system, such as the starting or stopping of a task, a software importation, or a device discovery.

The mechanism that the Enterprise Manager system uses to log events is the same as the BIG-IP system uses: the Linux utility **syslog-ng**. The **syslog-ng** utility is an enhanced version of the standard UNIX and Linux logging utility **syslog**.

The types of events that the Enterprise Manager system logs are:

- **System events**
  System event messages are based on Linux events, and are not specific to the Enterprise Manager system.

- **Local traffic events**
  Local-traffic event messages pertain specifically to the local Enterprise Manager system.

- **Audit events**
  Audit event messages are those that the Enterprise Manager system logs as a result of changes to the Enterprise Manager system configuration. Logging audit events is optional.

Because Enterprise Manager is based on TMOS, the system logging feature works the same way as BIG-IP system logging, and the Enterprise Manager system logs all of the same information that the BIG-IP system does. You can review logging features, log types, and how to set log levels in the *Logging BIG-IP System Events* chapter in the ***BIG-IP Network and System Management Guide***. You can use the procedures in that chapter to configure logging on the Enterprise Manager system. The following section describes additional processes that the Enterprise Manager system logs.

Understanding the specific processes logged by the system

The Enterprise Manager system introduces four processes to TMOS that enable the system to manage other F5 devices in the network. The four processes are:

- **discoveryd**
  This process enables the device management features such as device discovery, managing device groups, performing high availability functions, and refreshing device status information.

- **swimd**
  This process enables the software image management features, including importing software or hotfix images to the software repository, and deploying software or hotfixes to managed devices

- **emalertd**
  This process enables the custom alerting features for managed devices, including creating alert instances, assigning alert actions, and logging alert events.

- **emfiled**
  This process enables the features required to manage device configuration archives, including scheduling a rotating archive schedule, and maintaining pinned archives.

For each of these processes, Enterprise Manager can log a variety of events, including device discovery, software installations, alerts for managed devices, and tasks involving managed device configuration archives. When you enable audit logging, the process name appears in the system log along with a more specific description of the event.

Understanding the differences in logging options

Although the system event logging works in the same way as it does for a BIG-IP system, there are certain logging options that differ. Because the logging feature is designed to assist in traffic management, some of the logging options specific to traffic management may not apply to Enterprise Manager. When you set local traffic logging options, some of the events that you can choose to log may not produce logging, because Enterprise Manager does not deal with the same kind of traffic as a BIG-IP Local Traffic Manager system.

The Enterprise Manager system logs the messages for these events in the file **/var/log/em**.

Enabling audit logging

By default, the auditing feature that logs system events is not activated. If you want to log system events, you must enable audit logging. Audit logging logs messages that pertain to configuration changes that users or services make to the Enterprise Manager system configuration.

Audit logging logs messages whenever a Enterprise Manager system object, such as a software image or a device group, is created, modified, or deleted. There are three ways that objects can be configured:

- By user action
- By system action
- By loading configuration data

You can choose one of four log levels for audit logging. In this case, the log levels do not affect the severity of the log messages; instead, they affect the initiator of the audit event.

The log levels for audit logging are:

- **Disable**
  This turns audit logging off. This is the default value.
- **Enable**
  This causes the system to log messages for user-initiated configuration changes only.
- **Verbose**
  This causes the system to log messages for user-initiated configuration changes and any loading of configuration data.
- **Debug**
  This causes the system to log messages for all user-initiated and system-initiated configuration changes.

To enable audit logging

1. On the Main tab of the navigation pane, expand **System**, and click **Logs**.
   The System Logs screen opens.
2. On the menu bar, click **Options**.
   The Options screen opens.
3. In the Audit Logging section, in the **Audit** list, select a log level.
4. Click **Update**.

Viewing system logs

You can find the Enterprise Manager system log in the same location as you can find it on the BIG-IP system. On the Main tab of the navigation pane, expand **System**, and click **Logs**. You can then choose a log type from the menu bar, depending on the type of log that you want to view.

Glossary

administrative partitions

Administrative partitions are logical containers containing a defined set of BIG-IP system objects and are used for user management purposes.

boot location

A boot location is a portion of a drive with adequate space required for a software installation. This was previously referred to in other documentation as a *boot slot*.

changeset

A changeset is a user-defined collection of configuration data that enables you to archive and distribute an extended device configuration of one BIG-IP system.

changeset source

The changeset source device is the managed device in the network from which you want to copy some or all of its device configuration and store it in a changeset.

ConfigSync

See *configuration synchronization*.

configuration synchronization

Configuration synchronization is the task of duplicating the BIG-IP system or Enterprise Manager system configuration data onto its peer unit in a redundant system.

Configuration utility

The Configuration utility is the browser-based application that you use to configure the BIG-IP system.

dependency

A dependency indicates additional network object data or resource required for the primary network object to function correctly.

device list

The device list catalogs all devices that Enterprise Manager remotely manages. Adding devices to the device list is the first step in centrally managing the devices in the network.

device group

A group of devices that you can manage as a collection rather than individually is called a device group. For example, you can create an alert for a device group so that the alert applies to all devices that are members of the device group.

failover

Failover is the process whereby a standby unit in a redundant system takes over when a software failure or a hardware failure is detected on the active unit. See also *redundant system*.

hotfix installation task

A hotfix installation task is a series of jobs that you configure to upgrade one or more managed devices with hotfixes that are stored in the Enterprise Manager hotfix repository.

interfaces

The interfaces on the Enterprise Manager or other F5 Networks systems are the physical ports that you use to connect each system to other devices on the network.

iRule

An iRule is a user-written script that controls the behavior of a connection passing through the LTM system. iRules™ are an F5 Networks feature and are frequently used to direct certain connections to a non-default load balancing pool. However, iRules can perform other tasks, such as implementing secure network address translation and enabling session persistence.

managed device

A managed device is an F5 Networks device, such as a BIG-IP system, that is managed by Enterprise Manager.

management interface

The management interface is a special port on the BIG-IP system, used for managing administrative traffic. The management interface, named MGMT, does not forward user application traffic, such as traffic slated for load balancing. See also *TMM switch interface*.

object class

An object class is the general type of network object that you want to include in a changeset. See also *object instance*.

object instance

An object instance is the specific network object that you want to include in the changeset. See also *object class*.

pinned archive

A pinned archive is a UCS archive (that you create or move from the rotating archive list) that is saved in the Enterprise Manager database until you remove it. See also *user configuration set (UCS)*.

redundant system

A redundant system is a pair of BIG-IP systems configured for failover. In a redundant system, there are two units, often with one running as the active unit and one running as the standby unit. If the active unit fails, the standby unit takes over and manages connection requests.

rotating archives

Rotating archives are UCS archives created at a regular interval according to the schedule that you set in Enterprise Manager. See also *user configuration set (UCS)*.

SNAT (Secure Network Address Translation)

A SNAT is a feature you can configure on the BIG-IP system. A SNAT defines a routable alias IP address that one or more nodes can use as a source IP address when making connections to hosts on the external network.

SNMP (Simple Network Management Protocol)

SNMP is an industry-standard protocol that gives a standard SNMP management system the ability to remotely manage a device on the network.

software upgrade task

A software upgrade task is a series of tasks that you complete to upgrade managed devices with a software image stored in the Enterprise Manager software repository. Each job consists of one individual device upgrade.

syslog-ng

The **syslog-ng** utility is an enhanced version of the standard UNIX and Linux logging utility, **syslog**. Enterprise Manager uses this utility to log system events.

system certificates

System certificates are the web certificates that allow client systems to log into the BIG-IP system Configuration utility.

TMM switch interface

TMM switch interfaces are those interfaces that the BIG-IP system uses to send or receive application traffic, that is, traffic slated for load balancing. See also, *management interface*.

traffic certificates

Traffic certificates are server certificates that a managed device uses in its traffic management tasks.

user configuration set (UCS)

A user configuration set is a backup file that you create for the BIG-IP system or Enterprise Manager system configuration data. When you create a UCS, the system assigns a **.ucs** extension to the file name.

warm backup

A warm backup is a system that duplicates the configuration information of its peer device, and can perform all of the functions of its peer, but requires manual intervention to maintain the integrity of the backup configuration information.

Index