Enterprise Manager™ Administrator Guide

version 1.6

MAN-0223-05

Product Version

This manual applies to product version 1.6 of the Enterprise Manager.

Publication Date

This manual was published on March 20, 2008.

Legal Notices

Copyright

Copyright 2008, F5 Networks, Inc. All rights reserved.

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, Acopia, Acopia Networks, Application Accelerator, Ask F5, Application Security Manager, ASM, ARX, Data Guard, Enterprise Manager, EM, FirePass, FreedomFabric, Global Traffic Manager, GTM, iControl, Intelligent Browser Referencing, Internet Control Architecture, IP Application Switch, iRules, Link Controller, LC, Local Traffic Manager, LTM, Message Security Module, MSM, NetCelera, OneConnect, Packet Velocity, Secure Access Manager, SAM, SSL Accelerator, SYN Check, Traffic Management Operating System, TMOS, TrafficShield, Transparent Data Reduction, uRoam, VIPRION, WANJet, WebAccelerator, and ZoneRunner are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

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).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation <http://www.apache.org/>.

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

Table of Contents

1
Introducing Enterprise Manager

Working with Enterprise Manager 1-1
Working with compatible managed devices 1-2
Using Enterprise Manager features 1-5
Installing and setting up the system 1-6
Discovering devices 1-6
Grouping devices 1-6
Archiving and restoring device configurations 1-7
Managing device configuration data 1-7
Software, hotfix, and attack signature upgrades 1-8
Managing user accounts in the network 1-8
Monitoring the network and creating custom alerts 1-8
Monitoring certificate expiration dates 1-9
Auditing Enterprise Manager system events 1-9
Working with the Enterprise Manager interface 1-9
Navigating object list screens 1-10
Using general properties screens 1-11
Using the Menu bar 1-11
Understanding status icons 1-12
Finding user assistance 1-13
Contents of the Administrator Guide 1-13
Stylistic conventions 1-15
Finding documentation and technical support resources 1-16

2
Installation and Setup

Installing Enterprise Manager in the network 2-1
Choosing a network topology 2-1
Working with different network configurations 2-3
Working with a NAT configuration 2-4
Working with a tiered network configuration 2-5
Working with a tiered configuration using a SNAT 2-6

3
Licensing and Configuring the System

Setting up Enterprise Manager for the first time 3-1
Licensing the Enterprise Manager software using the Configuration utility 3-1
Creating the platform management configuration 3-3
Platform setup screen settings 3-4
Rerunning the Setup utility 3-6
Configuring the enterprise management network 3-6
Using the Basic Network Configuration wizard 3-7
Configuring Enterprise Manager defaults and preferences 3-8
Configuring Enterprise Manager as a high availability system 3-8
Changing the device refresh interval 3-12
Changing the device archive options 3-13
Setting alerting system options 3-14
Setting up SNMP options 3-15
Configuring internal email options 3-15
Managing user accounts 3-19
Working with the user list 3-19
Selecting the authentication source 3-21

Managing user roles 3-22
Working with role permissions 3-22

4
Discovering and Managing Devices

Working with Enterprise Management features 4-1
Understanding device types 4-1
Discovering and adding devices 4-2
Discovering devices 4-2
Adding devices using an imported file 4-4
Managing the refresh interval 4-5
Deleting devices from the device list 4-6
Performing basic device management 4-6
Setting device communication properties 4-7
Testing communications between devices and Enterprise Manager 4-7
Working with high availability systems 4-8
Rebooting managed devices remotely 4-10
Working with device groups 4-12
Managing device group members 4-13
Managing device memberships to a device group 4-14
Software upgrades and alerts on device groups 4-14
Managing device licenses 4-15
Using the License Device wizard 4-15
Acquiring support information 4-19
Using the Support Information wizard 4-19
Maintaining devices 4-22
Using maintenance mode 4-23
Replacing a device 4-24

5
Managing UCS Archives

Working with device archives 5-1
Managing Enterprise Manager device archives 5-1
Managing rotating archives 5-4
Managing rotating archive schedules 5-4
Modifying or deleting configuration archives 5-7
Saving device configuration archives 5-8
Restoring device archives 5-10
Comparing UCS archives 5-11
Configuring an archive comparison task 5-11
Reviewing configuration comparisons 5-13
Searching device configurations 5-14

6
Managing Device Configurations with Changesets

Managing device configurations 6-1
Introducing changesets 6-1
Understanding changesets 6-2
Working with changesets 6-2
Using changesets when adding new devices 6-2
Deploying new standards with changesets 6-3
Configuring new applications using changesets 6-3
Performing simple configuration changes using changesets 6-3
Understanding dependencies 6-4
Creating a changeset for a device 6-5
Using the Changeset wizard to create a changeset 6-5
Using a managed device source for a changeset 6-6
Creating a changeset based on a template 6-12
Creating a text changeset 6-13
Modifying a changeset 6-17
Verifying a changeset 6-17
Deploying configuration data and settings to target devices 6-18
Deploying a changeset 6-18
Delivering a current device configuration 6-19
Viewing device configurations 6-20

7
Working with Device Configuration Templates

Introducing templates 7-1
Working with templates and staged changesets 7-1
Understanding changesets and templates 7-2
Working with templates 7-2
Publishing templates 7-2
Using templates when adding new devices 7-3
Working with variables 7-3
Working with standard templates 7-7
Using a standard template for common tasks 7-8
Creating a template 7-9
Using the Template wizard to create a template 7-9
Working with the template list 7-16
Managing template properties 7-16
Modifying a template 7-18
Importing and exporting templates 7-20

8
Working with Staged Changesets

Staging configuration changes 8-1
Staging a changeset after creating a new changeset 8-1
Staging a changeset from the template properties screen 8-1
Staging a changeset using the Staged Changeset wizard 8-2
Verifying and deploying staged changesets 8-5
Verifying a staged changeset 8-6
Deploying a staged changeset 8-8

9
Managing Software Images

Managing image and file updates 9-1
Downloading software, hotfix, and attack signature images 9-1
Working with the image repository 9-5
Installing software on managed devices 9-8
Working with multiple boot locations 9-8
Installing software on devices in a tiered configuration 9-9
Installing software on Enterprise Manager systems 9-9
Performing software version rollbacks 9-9
Installing software to one or more devices 9-10
Installing hotfixes to one or more devices 9-13
Working with attack signatures 9-16
Managing signature updates 9-16
Installing attack signatures to one or more devices 9-19
Monitoring installation tasks 9-22
Working with software upgrades on the task list 9-22
Cancelling pending tasks 9-22

10
Managing User Account Data

Managing user accounts 10-1
Working with the user list 10-1
Viewing users on a device 10-2
Configuring user account information on managed devices 10-2
Copying user configuration information 10-3
Working with the Copy User Access Configuration wizard 10-3
Using the Launch Pad to start a user configuration copy task 10-5
Changing user account passwords 10-6
Working with the Change User Password wizard 10-6

11
Monitoring and Alerting

Monitoring device status 11-1
Understanding status icons in the device list 11-1
Monitoring management tasks 11-2
Using the task list 11-2
Working with the task properties screens 11-4
Configuring custom alerts 11-4
Setting up alert defaults 11-4
Configuring system alerts 11-5
Understanding the types of device alerts 11-6
Creating alerts for devices or device groups 11-9
Modifying or deleting alerts 11-11

12
Managing Device Certificates

Working with device certificates 12-1
Monitoring device certificates 12-1
Working with the certificate list screens 12-2
Creating alerts for certificate expiration 12-3
Exporting device certificate information 12-4

13
Auditing Enterprise Manager System Events

Working with Enterprise Manager system logging 13-1
Understanding the specific processes logged by the system 13-1
Understanding the differences in logging options 13-2
Enabling audit logging 13-2
Viewing logs 13-3
Searching the audit log 13-5

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, and device licensing.

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
- Manage device configuration changes through templates and staged changesets.
- Archive and restore multiple UCS archives.
- Schedule the automatic creation of UCS archives.
- Compare a current device configuration to a UCS archive, or compare two archives.
- Search through every configuration file for an object or setting.
- Install or renew device licenses for any managed device.
- Import and store multiple software, hotfix, and attack signature images in a central image repository.
- Deploy software, hotfix, and attack signature images to one or more devices.
- Synchronize device configurations between managed peer devices.
- 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.
- Gather technical information from managed devices for use by F5 Technical Support.
- Configure custom alerts to notify specific users of network events such as certificate expiration, or a completed software upgrade.
- Track and find changes made by users of Enterprise Manager.
- Monitor basic network health.

Working with compatible managed devices

Enterprise Manager version 1.6 can manage devices running the BIG-IP® 9.1.1 or later software. Additionally, Enterprise Manager can manage all Enterprise Manager devices. Enterprise Manager also supports BIG-IP Security Access Manager 8.0 or later, and WANJet 5.0 or later.

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 various managed devices.

Many new features introduced in Enterprise Manager version 1.6 are not supported by older BIG-IP software. Later versions of BIG-IP software (versions 9.3.x and 9.4.x) support new Enterprise Manager features such as device configuration management with templates and staged changesets.

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	EM v1.4.x	EM v1.6.x	WANJet v5.0.x	BIG-IP Secure Access Manager v8.0.x	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.3.x	BIG-IP v9.4.x
View all user account names in the network	X	X	X	X	X	X	X	X
View all user web roles in the network	X	X	X	X	X	X	X	X
View all user shell roles in the network	X	X	X	X	X	X	X	X

Table 1.1 *Managed device compatibility with basic user management features*

With Enterprise Manager version 1.6, you can use extended user management features that enable you to view additional user information on managed devices in the network. On later versions of managed devices, you can view details about authentication or shell access settings.

User Properties Feature	EM v1.4.x	EM v1.6.x	WANJet v5.0.x	BIG-IP Secure Access Manager v8.0.x	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.3.x	BIG-IP v9.4.x
Open user and user access configuration settings for a device using the Launch Pad screen	X	X	X	X	X	X	X	X
Single sign-on to managed devices from Launch Pad screen	X	X	X	X	-	-	X	X
View Authentication properties for user accounts on a device	X	X	X	X	-	-	X	X
View Shell Access properties for user accounts on a device	X	X	X	X	-	-	X	X

Table 1.2 *Managed device compatibility with user properties features*

Device configuration management features compatibility

The device configuration management features include the changeset features, template features, and staged changesets features. These features enable you to save, verify, and deploy an advanced set of device configuration data. These features are compatible with the latest releases of BIG-IP software (versions 9.3.x and 9.4.x), and Enterprise Manager (versions 1.4.x and 1.6.x).

Device Configuration Management Feature	EM v1.4.x	EM v1.6.x	WANJet v5.0.x	BIG-IP Secure Access Manager v8.0.x	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.3.x	BIG-IP v9.4.x
Create changeset source	X	X	X	X	-	-	X	X
Create configuration templates	X	X	X	X	-	-	X	X

Table 1.3 *Managed device compatibility with device configuration management features*

Device Configuration Management Feature	EM v1.4.x	EM v1.6.x	WANJet v5.0.x	BIG-IP Secure Access Manager v8.0.x	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.3.x	BIG-IP v9.4.x
Verify changeset data	X	X	X	X	-	-	X	X
Receive staged changeset data	X	X	X	X	-	-	X	X
View configuration differences	X	X	X	X	X	X	X	X
Browse device configurations	X	X	X	X	-	-	X	X

Table 1.3 *Managed device compatibility with device configuration management 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 the latest versions of BIG-IP system (versions 9.3.x and 9.4.x) and Enterprise Manager (version 1.4.x and 1.6.x). The Change User Password task is compatible with all managed devices.

Task	EM v1.4.x	EM v1.6.x	WANJet v5.0.x	BIG-IP Secure Access Manager v8.0.x	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.3.x	BIG-IP v9.4.x
Install Software Image	X	X	X	X	X	X	X	X
Install Software Hotfix	X	X	X	X	X	X	X	X
Copy User Access Configuration	X	X	X	X	-	-	X	X
Deploy Device Configuration	X	X	X	X	-	-	X	X
Change User Password	X	X	X	X	X	X	X	X
Renew device license	X	X	X	X	X	-	X	X

Table 1.4 *Managed device compatibility with task features*

High availability management compatibility

You can use Enterprise Manager to perform basic configuration and failover tasks for most high availability devices in the network. These tasks include using the ConfigSync feature to synchronize device configurations between redundant pairs, or changing the failover state between active and standby.

High Availability Management Feature	EM v1.4.x	EM v1.6.x	WANJet v5.0.x	BIG-IP Secure Access Manager v8.0.x	BIG-IP v9.1.1	BIG-IP v9.2.x	BIG-IP v9.3.x	BIG-IP v9.4.x
Synchronize configurations between peer devices	X	X	-	X	X	X	X	X
Change the active or standby state of a peer device	X	X	-	X	X	X	X	X

Table 1.5 *Managed device compatibility with high availability management 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 completing 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, manage 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 4-12.

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*** can store all the configuration data on a BIG-IP Local Traffic Manager system that is required to manage traffic, including information about system settings and network objects.

You can also use ***configuration templates*** to further enhance your device configuration management options. Configuration templates give you the ability to create specific configuration change guidelines that use variables so that you can re-use a configuration template to perform the configuration changes on multiple devices.

Using Enterprise Manager, you can store configuration information in changesets or configuration templates, and deploy it to one or more additional BIG-IP systems in your network through staged changesets. ***Staged changesets*** place a device configuration change in a staged state where a user can review and approve the changes prior to deployment.

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 wizards to create templates and changesets, or to stage changesets using an existing changeset or template as the source. 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 with changesets see Chapter 6, *Managing Device Configurations with Changesets*. For information about using templates, see Chapter 7, *Working with Device Configuration Templates*. To learn about using staged changesets, see Chapter 8, *Working with Staged Changesets*.

Software, hotfix, and attack signature upgrades

After you have set up 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 software, hotfix, and Application Security Manager attack signature images. Once you add these images to the repository, you can deploy an upgrade to one device, or configure multiple device upgrades. If you choose to configure device groups, you can create an upgrade task that installs upgrades to all compatible 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, hotfix, or attack signature definition upgrade, you can choose multiple upgrade options, including the installation location and reboot location on each device. For detailed information about managing images and upgrades see Chapter 9, *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 10, *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 11, *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 12, *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 13, *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.

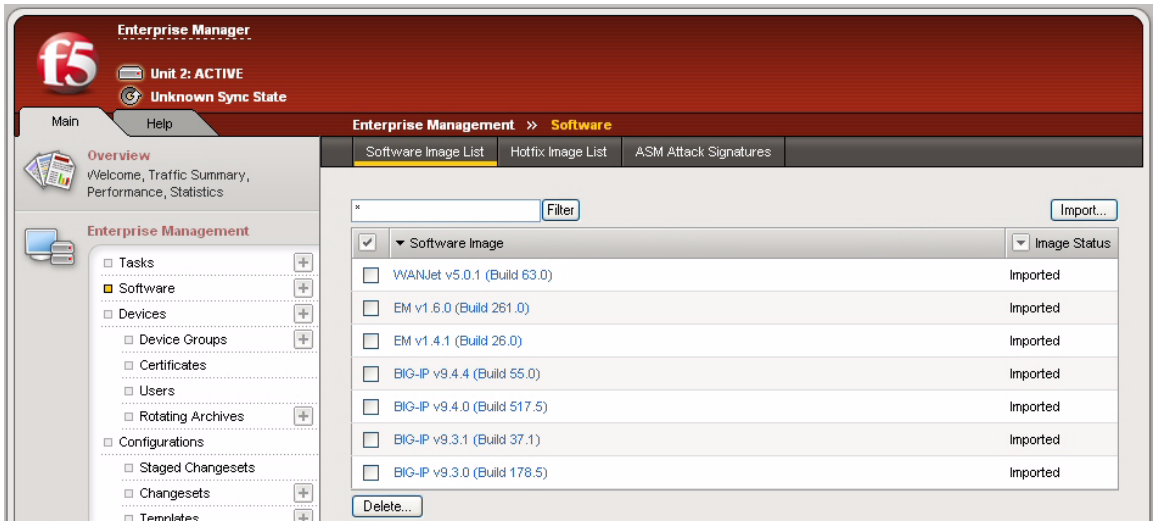

Figure 1.1 *Enterprise Management: Software Images object list screen*

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, preceding, 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, preceding,

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 bar, you can select options to enable specific management tasks, depending on the device, task, alert, or software image you are working with.

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.

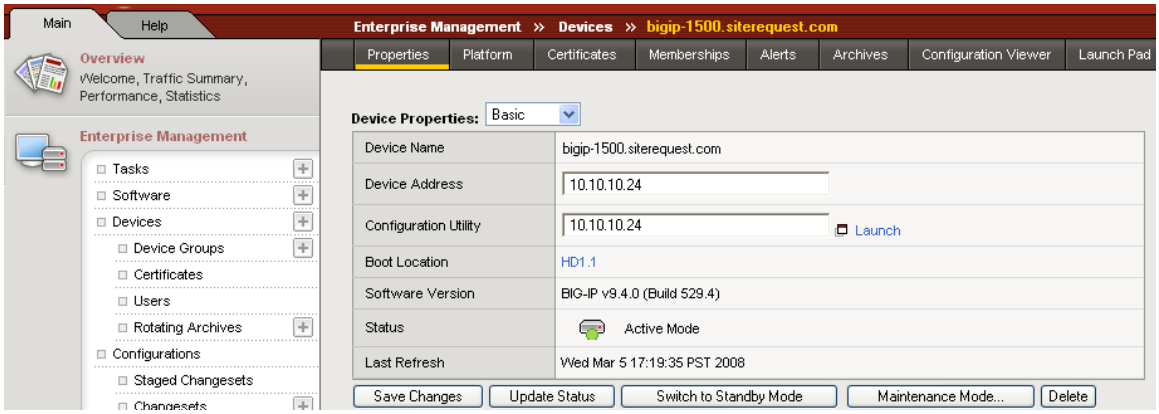

Figure 1.2 *A device general properties screen with menu bar*

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 1.6 *Status icons for managed devices*

Icon	Connection Condition
	Impaired (communication error; device can still receive updates)
	Maintenance Mode (communications between Enterprise Manager and the managed device are disabled)
	Replacement Mode (a modified version of Maintenance Mode for the purpose of replacing the managed device)

Table 1.6 *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 4-7.

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 With Changesets**
  This chapter describes the concept of managing device configurations using changesets.
- **Working With Device Configuration Templates**
  This chapter introduces the concept of configuration templates and how to use them to extend your device configuration management options.
- **Working With Staged Changesets**
  This chapter explains how to use staged changesets to manage device configuration changes using standard changesets and configuration templates.
- **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 9, *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 1.7 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 1.7 *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*** and ***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 Ask F5^{SM} Knowledge Base, **https://support.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 Ask F5[SM] Knowledge Base, **https://support.f5.com**, provides the latest release notes, technical notes, answers to frequently asked questions, updates for the Administrator Guide (in PDF format).

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.

Important

Although we recommend using the management interface, the hardware limitations of the Enterprise Manager 500 platform may adversely affect performance during device discovery or other management tasks. To avoid encountering possible performance degradation on the 500 platform, we recommend using the TMM switch ports on the Enterprise Manager 500 system to connect to managed devices.

Note

If you configure an Enterprise Manager redundant system, we recommend that you use the TMM interface on each Enterprise Manager peer device. We recommend a TMM port instead of the management port because a TMM port can support both static and floating self IP addresses. Use of a floating self IP address is necessary to ensure that the managed devices can communicate with active device of an Enterprise Manager redundant system. See ***Configuring Enterprise Manager as a high availability system****, on page 3-8* *for more information.*

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 the *Configuring the BIG-IP Platform and General Properties* chapter 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. That 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 4-7, 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 4-7, 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 4-7, 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 4-7, 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
- Managing user roles

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.

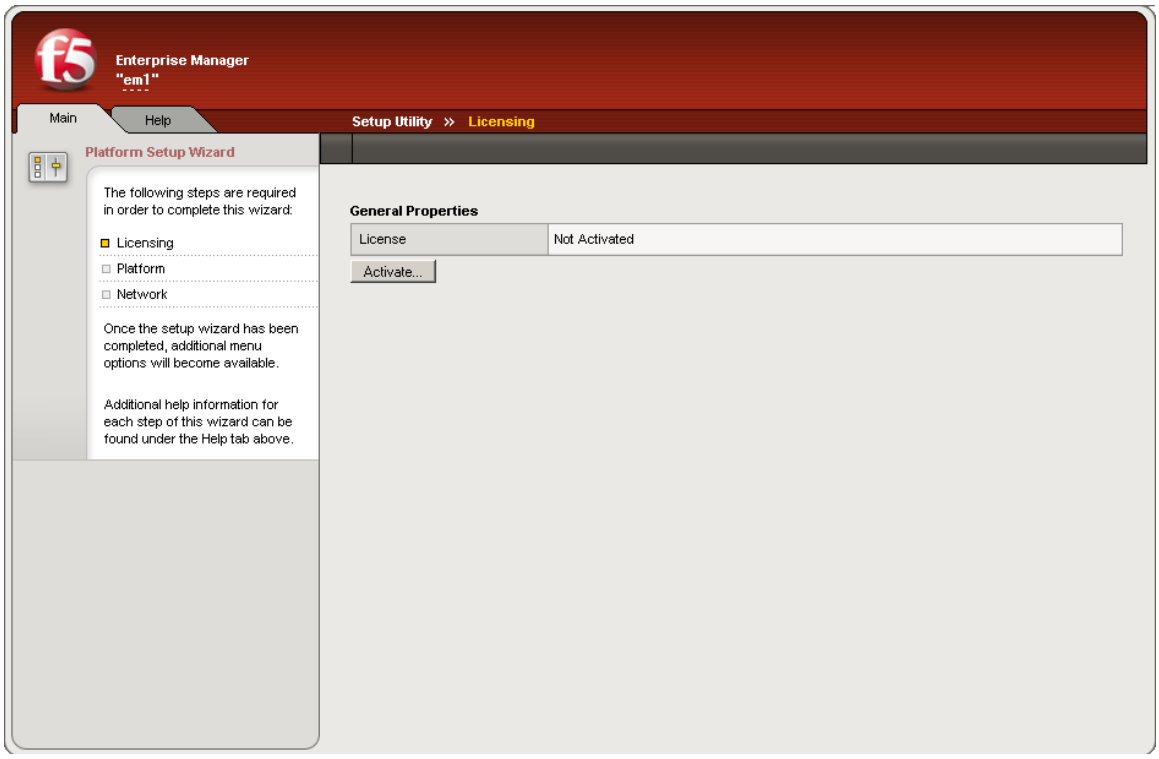

Figure 3.1 *The Licensing screen in the Setup utility*

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

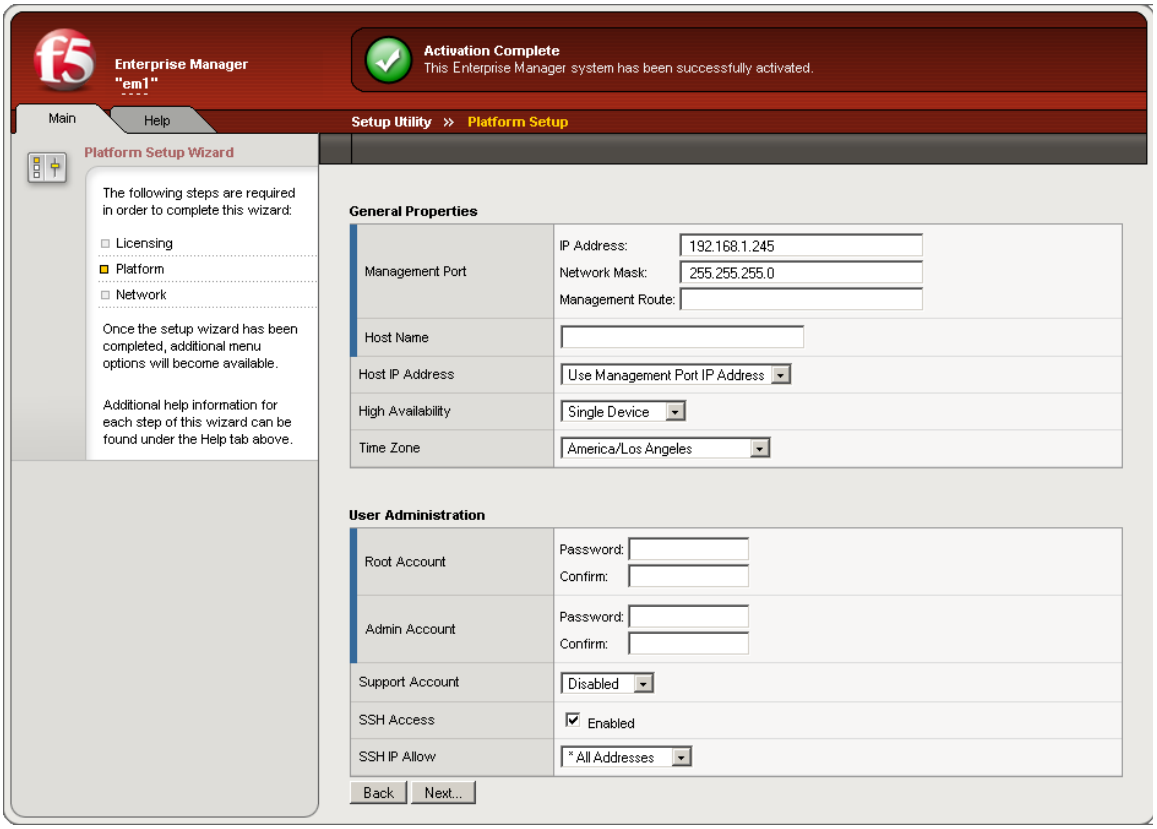

Figure 3.2 *The Platform Setup screen*

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.*

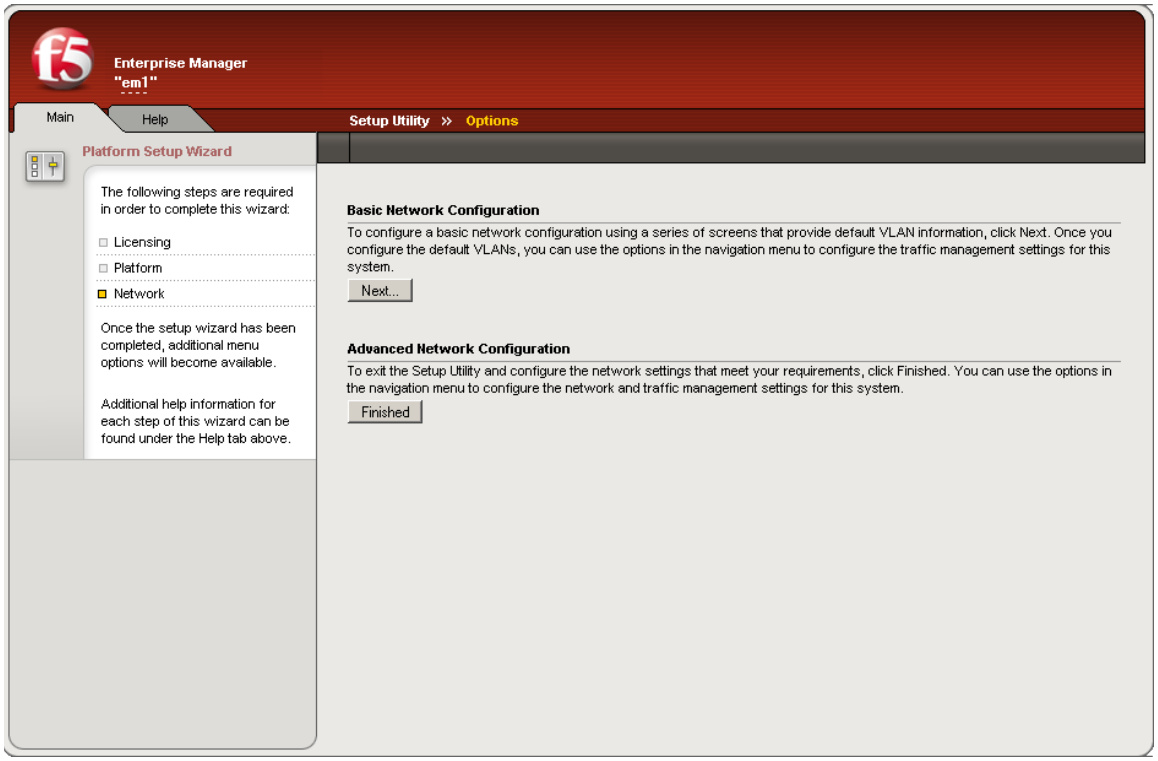

Figure 3.3 *The Options screen for configuring the enterprise management network*

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 IP addresses.

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 4-8 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 five 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 may incur 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.

Setting up a high availability Enterprise Manager system

Because of the differences with Enterprise Manager in a high availability configuration when compared to a BIG-IP system, Enterprise Manager may encounter issues unless you connect the devices according to certain guidelines.

In order for Enterprise Manager to work properly in a high availability configuration, you must configure the Enterprise Manager redundant systems to manage devices through a TMM port instead of the management port because a TMM port can support both static and floating self IP addresses. Use of a floating self IP address is necessary to ensure that the managed devices can communicate with the active device of an Enterprise Manager redundant system.

Configuring the network topology for high availability

An Enterprise Manager system manages information about other systems, so it requires some changes to the network topology to work successfully with certain tasks such as software upgrades. In order for two peer systems to communicate information about managed devices properly, follow these guidelines before you start configuring initial settings for the high availability system:

1. Configure at least one static self IP address (instead of using the MGMT interface to connect the devices).
2. Create at least one floating (shared) self IP address on the same network.
3. Configure a default gateway or route on the same network as each of the two self IP addresses that you configured.

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.

Scheduling automatic configuration synchronization

In order to ensure that your Enterprise Manager high availability system is synchronized, you may want to set up an automatic synchronization schedule. You can configure Enterprise Manager to run an automatic ConfigSync process at a regular interval, on the same screen where you can perform a manual synchronization.

To configure a scheduled ConfigSync

1. On the Main tab of the navigation pane, expand **System** and click **High Availability**.
   The System Redundancy Properties screen opens.
2. On the menu bar, click **ConfigSync**.
   The System ConfigSync screen opens.
3. In the Scheduled Configuration Sync table, for **Schedule**, select an option to determine how often you want the system to automatically synchronize its configuration with its peer:
   - **Disabled**: specifies there is no Scheduled ConfigSync task
   - **Daily**: specifies you schedule a ConfigSync at the same time each day
   - **Weekly**: specifies you select a day each week, and a time to run a scheduled ConfigSync
   - **Monthly**: specifies you select a day each month to run a scheduled ConfigSync
     The table changes to show additional options for **Day of the Week** or **Day of the Month**, depending on your choice.
4. 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 start the ConfigSync.
5. Click **Update** to save your changes.

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 60 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 **Rotating Archives**.
   The Rotating Archive Schedule screen opens.
2. On the menu bar, click **Options**.
   The Rotating Archives 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 11, *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 viewing 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.

To verify DNS resolution

1. Log on 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. For **Password**, in the **New** and **Confirm** boxes, type the password for the user you just entered and confirm the password.
5. From the **Role** list, select **Administrator**, **Advanced Operator**, or **Operator**.

6. From the **Partition Access** list, select an option to determine which administrative partitions the new user can access.
   The default is **All** partitions.
7. if you want to allow the user to access the command console, from the **Terminal Access** list, select **Enabled** to permit the user to access the Enterprise Manager device from the command line.
8. To add a new user, click **Repeat**, and repeat steps 3 through 7.
   The system adds the user settings you just configured, then clears the **User Name** and **Password** boxes.
9. To return to the user list screen, click **Finished**.

Important

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

For more information about user roles and permissions, see *Managing user roles*, on page 3-22.

To update user account properties

You can update user passwords and permissions from the user account properties screen.

1. On the Main tab of the navigation pane, expand **System** and click **Users**.
   The Users List screen opens.
2. In the user list, click the name of the user that you want to modify.
   The user account properties screen opens.
3. To change the user password, for **Password**, in the **New** and **Confirm** boxes, type the new password for the user, and confirm the password.
4. To change the user role, from the **Role** list, select **Administrator**, **Advanced Operator**, or **Operator**.
5. To change the user's partition access setting, from the **Partition Access** list, select an option to determine which administrative partitions the new user can access.
   The **Partition** box indicates the current setting for this user's partition access.
6. If you want to allow the user to access the command console to change the user's terminal access setting, from the **Terminal Access** list, i, select **Enabled** to permit the user to access the Enterprise Manager device from the command line.
7. Click **Update** to save changes to the user account properties.

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.

Managing user roles

With the addition of user role functionality, you can determine which users can perform different types of device management tasks. Enterprise Manager classifies user roles in three main types: Administrator, Advanced Operator, and Operator.

An Administrator-level user can perform all management functions available in Enterprise Manager, including managing other user accounts and roles.

Restricted user types (Advanced Operator and Operator) can, by default, perform fewer management tasks on the system. However, you can select certain types of actions that users assigned to one of these roles can perform. You do this by assigning permissions, or privileges, to user roles. Then, when you assign a user to a specific role, the user inherits the permissions that you granted to that role.

You can use the user roles feature to control the types of users who can perform device configuration management tasks. For example, if you want ***UserOne*** and ***UserTwo*** to manage device configurations differently, you do all of the following tasks:

- Assign different permissions to Advanced Operator and Operator.
- Assign ***UserOne*** to the Advanced Operator role.
- Assign ***UserTwo*** to the Operator role.

Because each user is assigned a different role, you can manage their permissions by changing the permissions for the role.

Working with role permissions

User role permissions determine the management tasks that users with a particular role can perform using Enterprise Manager. The two types of restricted user role permissions that you can modify are Advanced Operator and Operator. Administrators can perform all management tasks on the Enterprise Manager system.

For each type of restricted user role, you can manage up to eight permissions for each role. The main limitation that Enterprise Manager imposes is that you cannot assign any user-management permissions to restricted user types. Otherwise, you can permit a variety of management tasks for whichever user role you choose.

Table 3.1, on page 3-23, outlines all of the user role permissions that you can assign to Advanced Operators or Operators.

Permission	Management task
Archive Device Configurations	Users can create and manage UCS archives for all managed devices.
Browse Device Configurations	Users can view device configuration settings using the Enterprise Manager configuration browser.
Compare Device Configuration Archives	Users can compare two UCS configuration files for a managed device.
Stage Changesets for Deployment	Users can create a new staged changeset from published templates.
Deploy Staged Changesets	Users can deploy a staged changeset, whether it was created by that user or another user.
Administer Device Groups	Users can manage device group members.
Synchronize Device Configuration with Peer	Users can initiate a ConfigSync task to synchronize a managed redundant system.
Failover Devices	Users can start a fail over process from one managed device to the device's failover peer. Additionally, users can initiate a fail back process for an active-active configuration.

Table 3.1 *User role permissions for Enterprise Manager*

To specify user role permissions

1. On the Main tab of the navigation pane, click **Roles**.
   The Roles screen opens.
2. For each user role listed, check or clear the Select box next to the permission you want to modify.
3. Click **Apply** to save the changes to the user role permissions.

Important

By default, only certain staged changeset permissions are enabled for each user type: Operators can deploy staged changesets and Advanced Operators can stage changesets. In order to fully implement user role access control, you must enable roles on the Roles screen prior to assigning users device configuration management tasks.

4

Discovering and Managing Devices

- Working with Enterprise Management features
- Discovering and adding devices
- Performing basic device management
- Working with device groups
- Managing device licenses
- Acquiring support information
- Maintaining devices

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, or 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 a network 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, including BIG-IP product modules, such as Local Traffic Manager™, Global Traffic Manager™, Link Controller™, and Application Security Manager™.

Important

Enterprise Manager cannot currently manage BIG-IP software running on the VIPRION™ platform.

WANJet systems

The F5 Networks WANJet® appliance increases distributed application performance by optimizing, thus reducing, the amount of data that is transferred over the WAN. Enterprise Manager can manage WANJet appliances version 5.0 and later.

BIG-IP Secure Access Manager

The BIG-IP Secure Access Manager is a software component of the BIG-IP hardware platform that provides remote users with secure access to corporate networks, using most standard Web browsers. Enterprise Manager can manage BIG-IP Secure Access Manager, version 8.0.x. 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. After Enterprise Manager identifies these devices and logs on to 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, IP subnet, or by importing a list of devices. During a discovery task, 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.

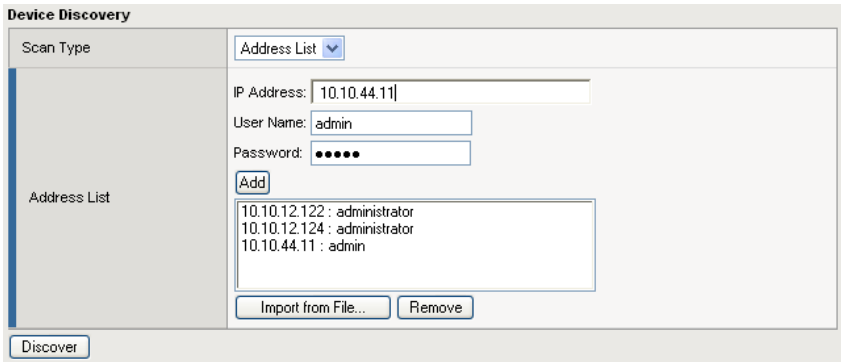

Figure 4.1 *Adding individual device addresses on the Device Discovery setup screen*

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, for the **Scan Type** setting, 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.*

Adding devices using an imported file

In addition to using Enterprise Manager to automatically discover devices in the network, you can also add devices to the device list by importing a file containing values that specify the IP address, user name, and password of each device. Enterprise Manager uses the information from this file to connect to the devices, log on using a user name/password combination, and set up device management.

For WANJet systems, we recommend importing a CSV file that contains device information. ***CSV*** stands for comma-separated values and refers to a text file (with a **.csv** file extension) that stores tabular data in a comma-delimited format.

Note

For discovering BIG-IP systems in the network, we recommend using the automatic device discovery feature of Enterprise Manager instead of the file import method.

Importing CSV files

If you choose to import a file for device discovery, Enterprise Manager uses the CSV file you import to determine the device IP address, user name, and password. When you create a CSV file to use for device discovery, use the following format with each unique device represented on its own line:

<device>, **<username>**, **<password>**

The variable **<device>** refers to the IP address of the device to discover, **<username>** is the user name that you want Enterprise Manager to use to log on to the device, and **<password>** is the password for the user name.

For example, if you have a list of five devices to discover, your import file may have the following entries:

```
10.10.10.1,admin,pass001
10.10.10.2,admin,pass002
10.10.10.3,admin,pass003
10.10.10.4,admin,pass004
10.10.10.5,admin,pass005
```

To import a CSV file

When you import a CSV file with device information, ensure that the file is hosted on your local system.

1. On the Main tab of the navigation pane, expand **Enterprise Management,** and click **Devices**.
   The Devices screen opens.
2. Above the device list, click **Discover**.
   The Device Discovery screen opens.
3. Click the **Import From File** button.
   The Import Address List screen opens.
4. Click the **Browse** button.
   A dialog box opens.
5. In the dialog box, browse to the location of the file that you want to import, and click the name of the file to select it.
6. Click **Open**.
   The path and file name appear in the **File Name** box.
7. Click **Import**.
   The screen changes to display the import status. When the importation finishes, the Device Discovery screen opens, and a list of imported IP addresses and user names appears in the **Address List** box.
8. Click **Start Task** to start the discovery task to add the devices in the Address List box to the Enterprise Manager device list.

Managing the refresh interval

Enterprise Manager polls managed devices at a default interval of 60 minutes. In each polling cycle, Enterprise Manager collects information about device status, peer synchronization, software installed on a device, and 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 list or a 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 information related to the device.

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.

◆ Note

*If a managed device cannot communicate with Enterprise Manager, the message **Device cannot contact EM** appears in the **Details** column next to a device name on the device list.*

To test a managed device's connection to Enterprise Manager

1. Log on to 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 managed devices that are part of a redundant pair and displays each device's failover state.

A ***redundant system*** is a pair of F5 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***, or the ***WANJet Appliance Administrator 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 BIG-IP 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 from active to standby

You can change the failover state of an active device from the Device Properties screen.

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**.
   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.

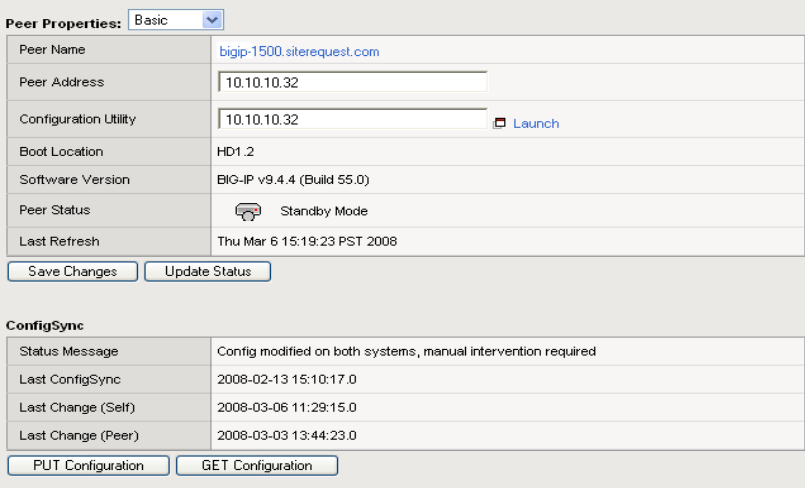

Figure 4.2 *Peer information on the device general properties screen*

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

On some managed devices, you can install different software versions on different boot locations. This gives you the opportunity to test different software or hotfix versions on a device before fully upgrading a device. If you have one software version installed on one boot location on a managed device, and a different software version installed on another boot location, you can use Enterprise Manager to reboot the device using the other 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 **Platform**.
   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.

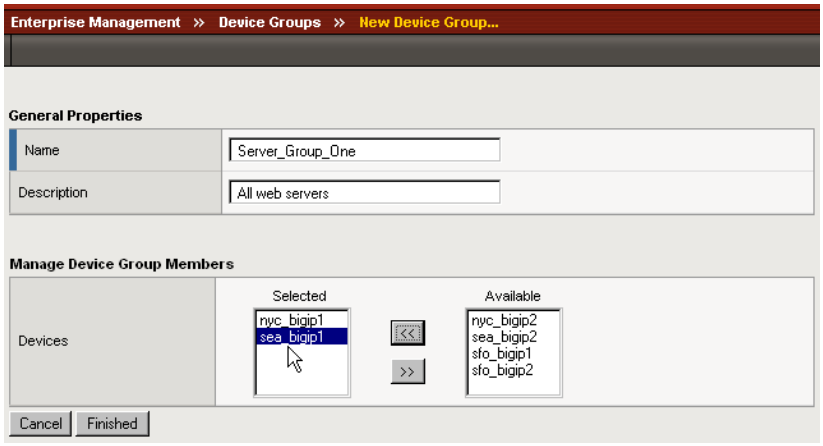

Figure 4.3 *Adding members to a new device group*

To create a device group

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Device Groups**.
   The Device Groups list screen opens.
2. Click the **Create** button.
   The New Device Group screen opens.
3. 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.
4. In the **Description** box, type information that can help identify the group when it appears on the Device Groups list screen.
5. In the Manage Device Group Members section, you can add devices to the device group. Devices listed in the **Selected** box are members of the current device group, and devices listed in the **Available** box can be added to the current device group.
   - 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 **Selected** box.

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

6. 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 **Device Groups**.
   The Device Groups list screen opens.
2. Click the name of the device group whose members that you want to manage.
   The Device Group general properties screen opens.
3. Below the General Properties table, click the **Manage** button.
   The Manage Device Group Members screen opens.
4. On the Manage Group Members screen, you can add devices to, or remove devices from the device group. Devices listed in the **Selected** 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 **Selected** box.
   b) To remove devices from the group, select a device in the **Selected** box and click the Move button (**>>**) to move the device name to the **Available** box.
5. Click **Finished** 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 device list 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 Membership** box.
   The current device is a member of device groups listed in the **Active Membership** 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.

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 that are compatible with the upgrade. 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 9, *Managing Software Images*. For detailed information about working with alerts and device groups, see Chapter 11, *Monitoring and Alerting*.

Managing device licenses

Two of the more time consuming tasks of managing multiple devices are renewing the device license on each device, or acquiring an initial license. You can use Enterprise Manager to automate the licensing process and save time over logging onto each device to initiate a licensing task. Enterprise Manager provides several automated features to expedite the licensing process for all managed devices in the network.

Enterprise Manager automatically determines which devices need to be licensed and displays this information on the device list screen. You can then configure a task using the License Device wizard that can license or renew a license on as many devices as you need.

The License Device wizard automates the entire licensing process. It retrieves the license dossier from the managed device, sends it to the F5 Networks licensing server, acquires a new license from the server, and provides you the opportunity to back up the device configuration before renewing the license.

Using the License Device wizard

Enterprise Manager uses a wizard to assist you in renewing the license on one or more managed devices. Using the wizard, you can select the devices that you want to license, view and accept the End User License agreement (EULA) for each device (if required), and start a task that updates the license on the devices you select.

Configuring a License Device task involves four or five main steps:

- Selecting the devices for licensing
- Contacting the licensing server to retrieve license information
- Reading and agreeing to a new EULA (if required)
- Setting task options
- Reviewing task settings before starting the task

To start a device licensing task

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens.
2. Above the Task List, click **New Task**.
   The New Task screen opens
3. In the **Licensing** section, select **License Device**.
4. Click **Next**.
   The Device Selection screen (Step 1) opens where you can select devices to include in the licensing task.
5. Follow the steps on the following pages to work through the wizard screens to license the devices that you select.

To select devices for licensing

On the Step 1 screen of the Licensing wizard, you can select devices.

1. In the **Device Group** box, select an option to narrow the list of devices:
   - If you want to license devices in a specific device group, select the device group name.
   - If you want to view all managed devices, select **All Devices**.
2. For **Device Filter**, select an option to display all compatible devices, devices in standby mode, unlicensed devices, or devices requiring a licensing hotfix.
   The device list table below **Device Filter** changes based on the option you select.
3. In the device list table, check the Select box next to each device that you want to license.
4. Click **Next** to move to the Step 2 screen where the system retrieves license information from the license server.

◆ Note

Due to some licensing issues involving iControl communications, certain devices may require a software upgrade in order to successfully re-license the device. See ***SOL7702: Enterprise Manager will verify the service check date and may require a license reactivation before marking a system eligible for an upgrade*** *on the Ask F5 Knowledge Base (****https://tech.f5.com****) for information about these licensing issues.*

To retrieve device license information

On the Step 2 screen, the system retrieves device license information, including the End User License Agreement (EULA) from the F5 licensing server. Once the system retrieves the license information for each device that you selected on the previous screen, you can move to a screen to license devices (or to accept EULAs, if required).

While the system retrieves license information from the licensing server, a progress indicator appears on the screen, and the screen refreshes at regular intervals until all of the license information is retrieved.

If you want to stop the screen from refreshing, in the **Auto Refresh** box, click **Stop**. To manually refresh the information on the screen, in the **Auto Refresh** box, click **Refresh**.

After the system retrieves license information, the system indicates which devices are ready for licensing by displaying a **Licence ready** message next to the device. Alternately, the message may indicate **EULA required**.

To move to the next screen, click **Next**.
If any of the messaged in the Details field indicate **EULA required**, then a Review EULAs screen opens. If no EULA is required, then the Task Options screen opens.

◆ Note

*Generally, when you first accept an End User License Agreement, you do not need to accept it again to renew a device license. However, if the EULA changes, you must accept the new EULA for each device that you want to re-license. When the system retrieves license information from the server, it displays a **EULA required** message next to each device for which you must accept a new EULA. If you follow the previous steps to select devices, the License Device wizard presents a Review EULAs screen next. If you do not need to accept EULAs for this task, skip to **To set task options**, on page 4-18.*

To accept EULAs for devices

If you need to read and accept an End User License Agreement for one or more devices that you selected, the Review EULAs screen opens.

The Review EULAs screen presents all available license agreements, and you can switch between these agreements if there are more than one. You can also choose to accept all EULAs for all devices for a specific EULA.

1. To view a different EULA (if available), in the **EULA** list, select a different EULA.
   The **Applies to Device(s)** box changes to display the devices to which the EULA applies.
2. To accept the EULA for all devices listed in the **Applies to Device(s)** box, check the Select box next to **Accept all EULAs and continue with device licensing**.
3. Repeat the previous two steps if you have additional EULAs listed in the EULA list.
4. Click **Next** to move to the Task Options screen.

◆ Note

*The **Next** button is unavailable until you accept an End User License Agreement for all devices in the licensing task.*

To set task options

After you select the devices for licensing, you can set task options. These options direct the system to take certain actions during the licensing task. You can specify what actions to take if the system encounters an error, and you can choose whether to create a UCS archive of each managed device before licensing the device.

1. To set an error handling option for this task, in the **Device Error Behavior** list, select an option.
2. To specify whether to create a UCS archive for each device before renewing the license, in the **Create Archives** box select an option.
3. To change whether Enterprise Manager includes private SSL keys in a UCS archive created before the system licenses the managed device, in the **Archive Options** box, change the value.
4. For **Post Licensing**, select an option to select whether to reboot the managed device after licensing (**Reboot Device** is the default option).

   ***Note**: We recommend that you accept the default option to reboot each device after licensing.*
5. Click **Next** to move to the Task Review screen.

To review task settings

Enterprise Manager presents an overview of the settings you specified on the previous screens so that you can review them prior to starting the task. You can change the name of the task (as it appears on the task list) from this screen, or you can use the **Back** button to move back to change options for the task.

To change the name of the task, in the **Task Name** box, type a new description before clicking **Start Task**.

To start the licensing task, click the **Start Task** button.

Acquiring support information

Using Enterprise Manager, you can collect information from any managed device that is useful in the event that you need to contact F5 Technical Support. A support case typically requires that you provide basic system and configuration information in order to properly diagnose and address any issues.

You can use Enterprise Manager to assist in gathering this information, which can save you time over logging on to each individual device to copy configuration files and device information.

The Support Information wizard helps you gather vital information about each managed device, and produces a report that you can submit to F5 Technical Support, if necessary.

Important

This section presumes that you have already initiated a support case with F5 Technical Support, and that your support representative has assigned a case number to you. This task requires entering a case number. Enterprise Manager uses that case number to associate the support information gathered with the existing case number already assigned.

Using the Support Information wizard

Enterprise Manager uses a wizard to assist you in collecting important support data from one or more managed devices. Using the wizard, you can select the devices from which you want information, and attach additional information about the configuration (if required), and start a task that gathers information from any device that you select.

Gathering support information requires four or five main procedures:

- Specifying a case number
- Adding device data
- Attaching additional information
- Setting the upload destination
- Sending the support information

To start a support information gathering task

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens.
2. Above the Task List, click **New Task**.
   The New Task screen opens
3. In the **Support** section, select **Gather Support Information**.

4. Click **Next**.
   The Task Properties screen (Step 1) opens where you provide a case number and additional information about the task.

To specify a case number and notes

The Step 1 wizard screen appears after you select the **Gather Support Information** option on the New Task screen.

1. In the **Case Number** box, type the case number assigned to the support case.
2. In the **Additional Information** box, type notes or information about the case.
   These notes can assist support engineers in diagnosing and solving your support case.
3. Click **Next** to move to the Device Data screen where you provide information about devices in this case.

To add device data

You can add device data and attachments to the support information on the Step 2 wizard screen that appears after you specify a case number and notes.

1. Above the Device Data table, click **Add**.
   The Add Devices screen appears.
2. For **Device Group**, select an option to limit the devices displayed by device group membership.
3. For **Device Filter**, select whether to view **Devices in Standby Mode** or **All Devices**.
   The device table changes to display devices that match your selection.
4. In the device table, check the Select box next to each device from which you want to collect support information.
5. Click **Retrieve Device Data**.
   The Gathering Device Support Information screen opens and displays a status of support information collection. The system may require several minutes to retrieve data from a managed device.
6. After the system collects the device data, click **Finished**.
   The Step 2 wizard screen opens again so that you can include attachments, if necessary.

◆ Note

*If your technical support representative requires **qkview** parameters for the support case, the representative provides the value. Then, for **Add Devices**, select **Advanced** to display the **qkview Parameters** box to enter the information.*

To include attachments with the device data

On the Step 2 wizard screen, you can include attachments such as screen shots, error messages, or log files with the support data. When you send this information to F5 Technical Support, Enterprise Manager includes the attachments.

1. Above the File Attachments table, click **Attach**.
   The Import Attachment screen opens.
2. In the **File Name** box, type the path and file name of the file, or click the **Browse** button to open a dialog box to visually search for the file.
3. Click **Import** to import the attachment.
   The screen changes to indicate file importation status. After the file imports, the Step 2 wizard screen opens again.
4. From the Step 2 wizard screen, click **Next** to open the Step 3 wizard screen.

To set the upload destination

On the Step 3 wizard screen, you can review the device information and attachments that you are gathering, and you can select an upload destination for the support information. Depending on your selections, the screen may change to prompt you for additional information.

1. In the **Destination** box, select a destination:
   - **Default F5 Support site**: this selects the standard F5 support server, and uploads the information to a directory that matches the case number.
   - **Custom Location**: this provides the option to specify a custom FTP server destination, and prompts you for more information.
   - **Local Download**: this saves the gathered support information in a compressed file on your local client system. If you select this option, you do not need to specify any additional settings.
2. If you selected **Default F5 Support Site**, review the **Email Address** box to ensure that the email address matches the email associated with the case number assigned to this support case.
3. If you selected **Custom Location**, type the following information in the appropriate boxes:
   - **FTP Server**: the FQDN or IP address of the FTP server to which you are sending support information
   - **FTP Port**: the port number of the FTP server
   - **FTP Login Name**: the user name that the system uses to log on to the FTP server
   - **FTP Login Password**: the password for the user name that the system uses to log on to the FTP server

- **Destination Directory**: the default directory on the remote system, where you send the support information. By default, the directory name corresponds to the support case number.

4. Review the data in the Devices and Attachments tables.
5. Click **Next** to move to the Step 4 wizard screen where the system prepares and sends the support information to the server you specified.

To send support information

The Step 4 wizard screen automatically prepares and sends the support information you collected to the destination you specified on the Step 3 wizard screen. The screen refreshes at a regular interval until the support information is sent.

If you selected **Local Download** on the previous screen, this screen provides a link. Click the link to save the save the data in a compressed file on the local client system.

Click **Finished** to return to the New Task screen.
After you click Finished, Enterprise Manager removes the collected support data from its database.

◆ Note

*If the system does not successfully transmit support information to F5, click **Back** to return to the Step 3 screen so that you can ensure that the FTP information or **Email Address** is correct.*

Maintaining devices

In certain cases, you may need to perform maintenance on a managed device in the network or even replace a device. You can use Enterprise Manager to switch a device into maintenance mode. ***Maintenance mode*** is a device state in which communications between Enterprise Manager and the managed device are disabled for the purpose of performing maintenance on the managed device.

When a device is in maintenance mode, Enterprise Manager communications are suspended so that you do not receive unnecessary alerts or configure tasks for a managed device that you know is offline.

Using maintenance mode

When you use Enterprise Manager to manage devices, it maintains a connection with the device in order to monitor device status or trigger alerts. However, when you take a managed device offline to perform maintenance, Enterprise Manager continues to attempt to communicate with the device, and may trigger unintended alerts due to the managed device's offline state.

To avoid this scenario, you can use maintenance mode to temporarily interrupt management communications between Enterprise Manager and a managed device. While a device is in maintenance mode, Enterprise Manager does not refresh device information, nor trigger alerts for the device. Additionally, you cannot include in a management task any device in maintenance mode.

Important

Maintenance mode does not disable any communications on the managed device itself. Maintenance mode only disables communication between Enterprise Manager and a managed device.

To enable maintenance mode

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The device list screen opens.
2. In the device list, click the name of the device that you want to switch to maintenance mode.
   The device general properties screen opens.
3. Below the General Properties table, click **Maintenance Mode**.
   The Maintenance management screen opens.
4. For **Mode**, select **Maintenance Mode**.
5. In the **Reason** box, type a note to indicate the reason for activating maintenance mode.
   This text appears on the device list and is logged in the Enterprise Manager audit log.
6. Click **Save Changes**.
   The general properties screen opens and the device state changes to Maintenance mode and the status icon on the screen and on the device list changes to indicate the new state.

To exit maintenance mode

You can turn off maintenance mode for a device from the same general properties screen that you used to enable maintenance mode.

1. On the general properties screen for a device, below the general properties table, click the **Maintenance Mode** button.
   The Maintenance management screen opens.
2. For Mode, select **Maintenance/Replacement Mode Off**.

3. In the **Reason** box, type a note to indicate the reason for de-activating maintenance mode.
   This text is logged in the Enterprise Manager audit log.
4. Click **Save Changes**.
   The device state changes to the state that the device was in prior to maintenance mode.

Replacing a device

In certain cases, you may need to replace a device. You can use Enterprise Manager to assist you in tracking the steps required to replace the device. Once you enable device replacement mode, Enterprise Manager provides a checklist that you can use to perform the steps necessary for replacing a device.

To start a device replacement task

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Devices**.
   The device list screen opens.
2. In the device list, click the name of the device that you want to switch to maintenance mode.
   The device general properties screen opens.
3. Below the General Properties table, click **Maintenance Mode**.
   The Maintenance management screen opens.
4. For Mode, select **Device Replacement Mode**.
5. In the **Reason** box, type a note to indicate the reason for activating Replacement mode.
   This text appears on the device list and is logged in the Enterprise Manager audit log.
6. Click **Save Changes**.
   The Device Replacement Checklist screen opens.

◆ Note

The Device Replacement Checklist appears instead of a device general properties screen once you set a device to replacement mode.

Working with the device replacement checklist

When you change the state of a device to Replacement mode, the Device Replacement Checklist screen appears instead of the general properties screen for a device. The device replacement checklist is a list of common tasks for replacing a device in the network.

The checklist contains several tasks. Before you select the check box next to each task, ensure that you complete the necessary tasks to successfully replace the device. Tracking device replacement tasks assists you by making the state of the overall replacement task visible.

- **Put device into Device Replacement Mode**
  When you replace a device, you must place it into maintenance mode so that Enterprise Manager does not attempt to perform management tasks.
- **Create UCS archive**
  When you replace a device, you should create an archive of the existing configuration so that you can use the same configuration on the replacement system. Click the **Create UCS archive** link to open the Devices: Archives screen to create an archive.
- **Replace physical hardware**
  Check the box after you replace hardware in the device, or the device itself.
- **Discover Replacement Device**
  When you add a replacement device to the network, you must discover the device before Enterprise Manager can manage it. Click the **Discover Replacement Device** link to open the New Device screen where you can configure a discovery task for the new device.
- **Set host name on replacement device**
  Set the host name on the new device. When you later restore the UCS archive to the new device, this restores the additional general properties (such as IP address, time zone, and HA settings).
- **Licensing**
  Depending on the type of replacement that you are performing, you have several licensing options:
  - **New Device / RMA** - Select this option when you are adding a new device or replacing a returned device. You can select to use the registration key on the new device.
  - **Repurpose similarly licensed device** - Select this option when you use the device for a different purpose in the network and you plan to use the currently licensed features.
  - **Repurpose different licensed or unlicensed device using EXISTING registration key** - Select this option when you use the device for a different purpose in the network and you plan to use different licensed features with the registration key currently assigned to the device. You can optionally select to use the existing registration key (with F5 Technical Support assistance) and you can re-license the device.
  - **Repurpose different licensed or unlicensed device using NEW registration key** - Select this option when you use the device for a different purpose in the network and you plan to use different licensed features with a new registration key. You can optionally set the new registration key (with F5 Technical Support assistance) and you can re-license the device.

- **Install software and hotfixes**
  After you license the new device, you can install software or hotfix upgrades, as needed.
- **Restore UCS archive** (without license)
  Restoring the UCS archive that you archived earlier ensures that the device configuration matches the device that you replaced.
- **Exit device replacement mode**
  Clicking the **Exit device replacement mode** link sets the device to active mode and opens the device properties screen.

5

Managing UCS Archives

- Working with device archives
- Managing rotating archives
- Saving device configuration archives
- Restoring device archives
- Comparing UCS archives
- Searching device configurations

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 3-13.

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 on 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 on 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.

Managing rotating archive schedules

After Enterprise Manager adds devices to the device list, you can set up a rotating archive schedule for any managed device that you select (or all managed devices). If you need to set up a custom schedule for any devices, you can do that individually for each device. You can create as many rotating archive schedules as you need, and you can assign any number of devices to each schedule. This provides flexibility to ensure that you can create device configurations for different devices at different intervals.

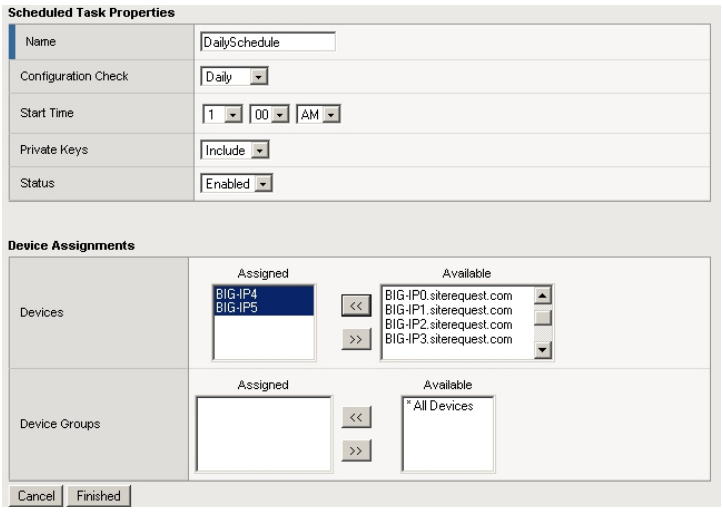

Figure 5.1 *Adding devices to a rotating archive schedule on the New Scheduled Task screen*

To configure a rotating archive schedule

You can configure a rotating archive schedule for one device, a device group, or as many individual devices as required.

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Rotating Archives**.
   The Rotating Archives list screen opens.
2. Above the table, click **Create**.
   The New Scheduled Task screen opens.
3. In the **Name** box, type a name for the rotating archive schedule. This name appears in the Rotating Archives list.
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.
6. In the **Private Keys** list, select whether you want to include private SSL keys in the rotating archive.
7. In the **Status** list, select whether you want to enable or disable the rotating archive schedule after you create it.
8. In the Device Assignments table, for the **Devices** or **Device Groups** setting, in the **Available** list, select a device or device group.
9. Click the Move button (**<<**) to move the selected devices or device groups from the **Available** to the **Assigned** list.
10. When you finish adding devices or device groups to the **Assigned** list, click **Finished**.
    The configuration archive list screen opens and the new rotating archive schedule appears in the list.

After you set up a rotating archive schedule, then whenever a device configuration in the **Assigned** list 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.

Modifying rotating archive schedules

Once you create a rotating archive schedule and add devices or device groups, you can further manage the schedule. You can modify elements of the schedule, including the interval and its enabled state, making these changes affect all the devices subscribed to that schedule. Additionally, you can manage individual device or device group memberships to a particular schedule.

To modify a rotating archive schedule

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Rotating Archives**.
   The Rotating Archives list screen opens.
2. In the list, click the name of a schedule.
   The Scheduled Task Properties screen opens.
3. If you want to change the archive interval, 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.
4. 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.
5. If you want to change whether to include private SSL keys in the rotating archive, in the **Private Keys** list, select an option.
6. If you want to change the state of the rotating archive schedule, in the **Status** list, select an option:
   - **Enabled**: Activates the scheduled task to check for configuration changes and create archives at the specified interval for all devices in the **Assigned** list.
   - **Disabled**: De-activates the scheduled task and stops checking for configuration changes or creating archives for all devices in the **Assigned** list.
7. If you want to add devices or device groups to this rotating archive schedule:
   a) In the Device Assignments table, for the **Devices** or **Device Groups** setting, in the **Available** list, select a device or device group.
   b) Click the Move button (**<<**) to move the selected devices or device groups from the **Available** to the **Assigned** list.
8. If you want to remove devices or device groups from this rotating archive schedule:
   a) In the Device Assignments table, for the **Devices** or **Device Groups** setting, in the **Assigned** list, select a device or device group.
   b) Click the Move button (**>>**) to move the selected devices or device groups from the **Assigned** to the **Available** list.
9. To save changes to the rotating archive schedule, click **Save Changes**.

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 the archives table, check the Select box next to the name of the archive(s) that you want to delete.
5. Below the 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 the 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 before implementing important changes such as a software upgrade or hotfix installation. This ensures that you can restore a saved configuration from any specific point in time.

In addition to saving archives for any individual device, you can use the device groups feature to pin an archive for each device in a device group.

To create a new pinned archive

You can create a new UCS archive from a Device Archives 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 archives table (below the Rotating Archive Summary 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. For **Private Keys**, choose an option to determine whether Enterprise Manager stores private key data in the UCS archive.
8. Click **Create**.
   Enterprise Manager creates a UCS archive of the current device and the archive appears in the archive table when the Device Archive screen opens.

To pin an existing configuration archive

You can save a UCS archive from the Device Archives 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 archives table, check the box to the left of an archive name to select it.
5. Click **Pin Archive** below the table.
   The archive status changes to **Pinned** and it remains in table until you delete it.

To work with device groups

Using steps similar to the preceding procedures, you can use the pinned archive feature with device groups as you would for an individual device. The difference between the steps involves first selecting a device group.

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Device Groups**.
   The Device Groups list screen opens.
2. Click the name of the device group for which you want to manage archives.
   The Device Group properties screen opens.
3. On the menu bar, click **Archives**.
   The Device Groups Archives screen opens.

From the Device Groups Archives screen, you can manage archive schedules and pinned archives in the same way you do for individual devices.

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 Device Archives screen opens.
4. In either the device archive 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.

Comparing UCS archives

When you manage multiple versions of UCS archives, you may encounter situations where you need to compare the differences between device configuration archives. Comparing archives can assist in troubleshooting issues related to restoring archives or upgrading software. When you compare archives, Enterprise Manager highlights the differences between two archives so that you can easily identify configuration changes.

Configuring an archive comparison task

Enterprise Manager provides the Compare Device Configurations wizard to assist you in configuring an archive comparison task. It works in a fashion similar to other wizards in Enterprise Manager. You can choose to compare either the current configuration to an archive, or two UCS archives.

Comparing device configurations using the wizard involves two main steps:

- Specifying the source device
- Choosing to compare the current configuration to an archive or to compare two archived configurations

Starting an archive comparison task with the Task wizard

After you start the task, the first step requires that you select a source managed device, then the type of comparison you want to perform.

To start an archive comparison task

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens.
2. Above the Task List, click **New Task**.
   The New Task screen opens.
3. In the **Configuration Archives** section, select **Compare Archive**
4. Click **Next**.
   The Compare Device Configurations screen opens, where you select a device and comparison type.

To select a device and comparison option

After you start the archive comparison task, the Step 1 screen appears, prompting you to select the source device and the type of comparison that you want to do. Although, you can only compare UCS archives for one device, you can compare the current configuration to an archive, or you can compare two existing archives.

1. For **Device**, select the managed device for which you want to compare device configurations.
2. For **Comparison**, select an option depending on the type of comparison that you want to do:
   - **Current configuration to an archive**
     Select this to compare the current configuration of the device you selected in the **Device** box to one of the archived configurations listed in the Configuration archives table.
   - **Two configuration archives**
     Select this to compare two archived configurations.
3. Your next action is based on what you selected for **Comparison**.
   - If you are comparing the current configuration to an archive, in the Configuration Archives table, select the option button next to the archived configuration that you want to compare.
   - If you are comparing two archived configurations, in the Configuration Archives table, check the Select box next to two archives that you want to compare
4. Click **Next** to advance to the Task Review screen.

To review the comparison task options

After you configure the options, you can review the options before starting the task, or change the task name on the Task Review screen.

If you want to change the name of the task as it appears on the Task List screen, in the Task Name table, change the text.

To start the task, click **Start Task**.
The Task Properties screen opens, displaying details about the comparison task.

Reviewing configuration comparisons

After you start a comparison task, the task properties screen provides a summary of the task details. From this screen, you can open detailed comparison screens to view configuration differences between specific configuration files. This screen appears automatically after you start a comparison task. You can also view this screen by clicking a comparison task in the task list.

To view a detailed comparison of two configuration files

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens.
2. In the task list, click the name of an archive comparison task.
   The Task Properties screen opens.
3. In the Task Summary table, in the Comparison column, click the **View** link for the configuration files that you want to compare.
   The Task Details screen opens, displaying a detailed comparison of the configuration files, with differences between the two highlighted.

◆ Note

*In the Comparison column, the message **File Not Found** may appear in certain Compare Archive tasks. This message indicates that the system did not detect the file at the specified location, or the file does not exist. Configuration files may vary by managed device, or licensed features. Check the path and file name if you did not expect this message.*

Searching device configurations

In addition to archiving and comparing device configurations, you can search any configuration file on a managed device for specific elements. This can help you find and view particular objects or settings in any managed device in the network.

You can use the Configuration Search feature to examine all available configuration files on each managed device in the network. After you search by a particular keyword, you can filter the results to meet more specific criteria.

To search device configurations

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Configurations**.
   The Search Configuration screen opens.
2. In the **Keyword** box, type a term for which to search in each configuration file.
   You can type any alphanumeric string of characters.
3. Click **Search**.
   The Matching Objects table changes to display configuration files that contain instances that match the string you typed in the **Keyword** box.
4. In the **Matching Objects** filter box, type a string of characters and click the adjacent **Filter** button to filter the list of configuration files.
   A list of configuration files that match the filter you applied appears in the Matching Objects list.
5. To view the contents of a configuration file, in the Matching Objects list, click the name of the configuration file.
   The configuration file text appears in the Object Text table.
6. To clear the configuration file list, click **Reset**.

◆ Tip

*The preceding procedure searches every device configuration for a keyword before you limit the matching objects, and may take a long time if you have a large number of managed devices. If you want to limit your search to only a specific device or set of configuration files, you can type a character string in the **Matching Objects** filter box above the Matching Objects list before typing anything in the **Keyword** box. Then, when you subsequently search by keyword, the system searches only configuration files already listed in the Matching Objects list.*

6

Managing Device Configurations with Changesets

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

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 system specific configuration files
- 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 system device configuration settings that allows you to copy all or part of the device's configuration settings to a separate system. Enterprise Manager uses changesets to provide enhanced device configuration management.

Introducing changesets

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 create and then 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.

For more information on how you can use changesets, see *Working with changesets*, on page 6-2.

Understanding changesets

Although changesets and UCS files each represent 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, in 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, you typically 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 task to deploy the changeset, 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 generally want to 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 as resource objects 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 when you choose a managed device as the configuration source:

- Specifying the changeset source
- 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.

◆ Note

The wizard screens that appear in the Changeset wizard vary depending on the configuration source that you choose.

Selecting a changeset source

The first step in creating a changeset is selecting the source for the changeset. The ***changeset source*** is a managed device, configuration template, or configuration file text for which you want to copy some or all of its configuration information.

If you choose an existing managed device for the changeset source, the wizard then prompts you for object information so that you can specify the exact objects on an existing device in the network.

If you choose a configuration template for the source, Enterprise Manager uses the configuration from an existing configuration template. A ***configuration template*** is a configuration management tool that works with existing changesets to create a model device configuration framework for use in creating new changesets. If you create a template-based changeset, you can use the variables feature of the configuration template in the new changeset. See Chapter 7, *Working with Device Configuration Templates* for information about how to use configuration templates to improve changeset management.

If you choose a text source, you can manually enter configuration text, or paste configuration text from another changeset or configuration template in Enterprise Manager. Although creating a text-based changeset requires minimal steps in the wizard, you must take great care to ensure that the text information that you provide is accurate and includes proper object dependency or variable information. The Changeset wizard can automatically determine the proper object dependency information or variable information because it uses configuration information that already exists in the Enterprise Manager database.

Once you select the source type, you can select additional options depending on the type of changeset source you choose:

- For a device source, see *Using a managed device source for a changeset*, following.
- For a template source, see *Creating a changeset based on a template*, on page 6-12.
- For a text source, see *Creating a text changeset*, on page 6-13.

Using a managed device source for a changeset

Creating a device-based 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

Selecting a source device and partition

If you select a managed device as the source, you specify the device and partition from which you want to copy some or all of its device configuration.

Administrative partitions are logical containers containing a defined set of BIG-IP system objects, and are used for access control purposes. You can work with administrative partitions on managed devices running BIG-IP version 9.4.x software. 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 objects 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.

The object classes available to you vary depending on the type of managed device and the licensed features already installed on the managed device.

For Network and Local Traffic object classes, the last part of the class name is a close mapping to what type of object the changeset affects on the managed device. For example, if you include the Network / VLAN class, all objects that you affect in this class are VLANs. If you include the Local Traffic / Profiles / DNS class, all objects in this class are DNS objects. There are at least 50 total Network and Local Traffic object classes.

For System classes, the class name does not exactly specify which object is affected. Table 6.2 outlines the system class names and their related objects or settings.

System Class Name	Related object instance
System / Bind	named.conf
System / DNS	resolv.conf
System / HTTP	httpd.conf
System / LCD	lcd.showmenu setting
System / Logging	config.auditing setting
System / Net-SNMP	net-snmp_snmpd.conf
System / NTP	ntp.conf
System / Postfix / Main	main.cf
System / Postfix / Master	master.cf
System / SNMP	snmp_snmpd.conf
System / Syslog	syslog-ng.conf
System / Timezone	ntp.timezone setting

Table 6.2 *System classes and related objects allowed in changesets*

◆ Note

Starting with version 9.4.3, BIG-IP systems use a different method of managing configuration files. On 9.4.3 and later systems, only the ***named.conf****,* ***main.cf****, and* ***master.cf*** *object instances noted in Table 6.2 appear in changesets as they do for changesets based on earlier systems. To view the configuration settings for a 9.4.3 or later system to confirm compatibility with* ***bigpipe*** *commands, you can use the Configuration Viewer feature. See* ***Viewing device configurations****, on page 6-20 for instructions*

on viewing configurations. Additionally, you can find detailed information about ***bigpipe*** *commands in the* ***BIG-IP® Command Line Interface Guide****, available from the Ask F5SM Knowledge Base (****https://support.f5.com****).*

Explaining the settings for object classes is beyond the scope of this manual. For detailed information about object classes that you configure on a managed device, see the ***Configuration Guide for BIG-IP® Local Traffic Management*** manual available from the Ask F5SM Knowledge Base (**https://support.f5.com**).

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 in the wizard, you chose object classes to include in the changeset. You can select the specific objects on the Object Selection screen. The Object Selection 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 the changeset summary

Once you have selected objects to include in the changeset, you can choose whether to include dependencies, or resource objects, 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 dependency options

You can change dependency information on the Changeset Summary screen in the New Changeset wizard.

1. In the **Dependency Handling** box, select whether to include dependencies.
   The **Resource Objects** box disappears if you choose not to include dependencies.
2. To view details of an object that you selected on the Object Selection screen, 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 **Resource Objects** list, click the name of an object.
   Details about that object appear below the list.
5. Click **Next** to open the Text of Changeset screen.

Finalizing the changeset on the Text of Changeset screen

After you manage any dependencies for the changeset, you can view or modify the changeset configuration text in the final step of the Changeset wizard.

The last screen of the wizard, Text of Changeset, displays a **Text** box that contains the configuration of the changeset. In this text box, you can view the configuration changes you selected in **bigpipe** shell format. If you deploy these configuration changes, the system makes the necessary configuration changes to the appropriate configuration files. You can make changes to any of the text in the file.

Above the text box, you can select a **Basic** or **Advanced** view. If you select **Advanced**, the screen changes to display additional editing controls including the **Add Path** and **Search and Replace** buttons.

You can perform any of the four following procedures in this section on the Text of Changeset screen.

To add a new class path

To add a new class path to the changeset, in the **Select Class Path** list select a new class path and click **Add Path.**
The system generates the proper syntax for the class path, and adds it to the **Text** box.

To find an existing value and replace it with a new value

1. In the **Search For** box, type the existing value.
   You can type a user-specified value such as an IP address or object name. This value is case-sensitive.
2. In the **Replace With** box, type the new value.
3. Click **Search and Replace**.
   The system searches through the data in the **Text** box and prompts you to confirm any changes, if found.

To save the changeset

After you review or change information in the changeset, click **Finished** to save the changeset.

To stage the changeset for deployment

If you want to immediately stage this changeset for deployment, click the **Stage for Deployment** button.
The New Staged Changeset wizard opens on the Target Device Selection screen.

See *Selecting a target device for a staged changeset*, on page 8-3, for information on how to use the New Staged Changeset wizard.

◆ 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 changeset based on a template

When you create a changeset based on a configuration template, you can use the configuration and variables of that template in the changeset. When you use a template source that contains variables, you can configure the variables and allowed values in the same way that you would when you configure a configuration template. For more information about configuration templates and variables see *Working with variables*, on page 7-3.

The main difference when you configure a template-based changeset using the Changeset wizard is that you do not need to complete the steps required to select object classes and instances, as this information is already included in the configuration template source. As a result, there are only three pages in the Changeset wizard for a template source:

- The source selection screen
- The variable management screen
- The text review screen

Selecting a source template

When you select a template as the source for a new changeset, you can use the features of a configuration template in the new changeset.

A configuration template is similar to a changeset in that it can store and change device configurations for any managed device in the network. However, configuration templates provide the added capability of managing variables for a particular network configuration object.

See Chapter 7, *Working with Device Configuration Templates* for information about how to work with configuration templates.

To select a template

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 **Template**.
   The screen changes to display a table listing all available configuration templates.
6. In the template table, select the template that you want to use.
7. Click **Next** to open the template variables screen where you can configure variables for the template.

Configuring template variables

When you create a template-based changeset, you can use the advanced variables features that configuration templates use. With variables, you can essentially re-use a configuration template for different devices while maintaining valid settings on each device.

Template variables are unique values or settings required by each managed device in order to properly run the configuration change specified by the template.

To understand variables, see *Working with variables*, on page 7-3.

See *Assigning variables in a template*, on page 7-13 for instructions on how to manage variables for a template-based changeset. When you manage variables in the Changeset wizard, the procedure is the same as when you manage variables in a configuration template.

After you configure the default and allowed values of the variables in the changeset, click **Next** to move to the changeset review screen

Reviewing a template-based changeset

The last step of the Changeset wizard for a template-based changeset is the review screen. The review screen displays the text version of the changeset.

You can edit any of the configuration information in the **Text** box.

Once you confirm that the configuration information for the changeset is accurate, do one of the following:

- To add the changeset to the changeset list, click **Finish**.
- To start the New Staged Changeset wizard to stage this changeset, click **Stage 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.
9. 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 or other utilities 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
```

When you construct the changeset text to include an object that can be targeted to a specific partition, 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 6-14.

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 the virtual server **MyVIP**, which references its pool, **MyPool**.

```
#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.

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 after you stage the deployment. To learn how to work with staged changesets, see *Staging configuration changes*, on page 8-1.

When you verify a changeset, Enterprise Manager checks to see if the local traffic management 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 all possible system settings included in the changeset.

A wizard guides you through the stage changeset process, and when you finalize the settings, you have the option to verify the staged changeset on the target devices. For more information about the Staged Changeset wizard, see *Verifying and deploying staged changesets*, on page 8-5.

Note

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

Deploying configuration data and settings to target devices

After you create a changeset, you can deliver the device configuration data and settings in the changeset to any managed device in the network. As an alternative, you can take a current snapshot of a configuration on a 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 ways 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. You do this by using the New Staged Changeset wizard to stage the data for deployment. After you do this, you can deploy the data to target devices that you select using the Deploy Staged Changeset wizard. Each wizard works in a similar manner to other wizards in Enterprise Manager, and lets you select compatible devices, partitions, and task options, and then review your options before you start the task.

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.

See *Staging configuration changes*, on page 8-1, for information on how to create a new staged changeset. See *Verifying and deploying staged changesets*, on page 8-5, for information on how to verify and deploy the configuration changes in a changeset.

Selecting a changeset for deployment

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 **Stage for Deployment** button to open the Deploy Staged Changeset wizard.

For more information about the staged Changeset wizard, see *Selecting a staged changeset source*, on page 8-3.

Delivering a current device configuration

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

You can do this by completing a series of tasks:

1. Create a changeset using the New Changeset wizard.
2. On the last screen of the New Changeset wizard, Text of Changeset, click the **Stage for Deployment** button.
   The New Staged Changeset wizard opens using the changeset you just created as the source.
3. Create a New Staged Changeset.
4. On the last screen of the New Staged Changeset wizard, click the **Deploy Staged Changeset Now** button.

Refer to the procedures for creating a changeset in *Using the Changeset wizard to create a changeset*, on page 6-5, to create a current snapshot configuration change data. Then, use the procedures for creating a staged changeset in *Deploying a staged changeset*, on page 8-8. For specific assistance on a screen, consult the online help.

Viewing device configurations

When you manage a device with Enterprise Manager, you can view specific elements of a device configuration file. Enterprise Manager provides a configuration viewer so that you can specify configuration settings for any object on a device.

Using the configuration viewer can save you time. Normally, to find specific configuration information in the configuration files on each managed device, you have to open a text configuration file and manually search for specific elements. Viewing configurations for objects may also assist you in creating changeset configurations.

To view object configurations for a device

1. On the Main tab of the navigation pane, expand **Enterprise Management**, then click **Devices**.
   The Devices screen opens.
2. In the device list, click the name of the device for which you want to view a configuration.
   The device general properties screen opens.
3. On the menu bar, click **Configuration Viewer**.
   The Configuration Viewer opens.
4. In the **Partitions** list, click the name of the partition that you want to view.
   The **Modules** list changes to display all modules available on the managed device.
5. In the **Modules** list, click the type of system configuration that you want to view.
   The **Paths** list changes to display all object classes available on the managed device.
6. In the **Paths** list, click the class of network object that you want to view.
   The **Objects** list changes to display all object instances of the class you selected.
7. In the **Objects** list, click one or more network objects.
   The screen changes to display a text view of the object configuration you selected.

7

Working with Device Configuration Templates

- Introducing templates
- Working with templates
- Working with standard templates
- Creating a template
- Working with the template list
- Modifying a template
- Importing and exporting templates

Introducing templates

To further expand your device configuration management options, you can use configuration templates. A ***configuration template*** is a configuration management tool that works with existing changesets to create a model device configuration framework for use in creating new changesets. Configuration templates assist you in managing specific elements of a device configuration when managing multiple devices through the use of variables.

A configuration template is similar to a changeset in that it can store and change device configurations for any managed device in the network. However, configuration templates provide the added capability of managing variables for a particular network configuration object. Through the use of variables, you can create a model configuration change for a device using an existing device's configuration, then use it to update a different device by setting variables to values compatible with the target device.

For example, if you want to create a template to enable a virtual server, you can create a basic configuration template that will enable a virtual server on any device you choose, as long as you include the required information (such as the virtual server name or address) for each device. Then, you can use the template information to create a changeset in order to deploy the configuration change to managed devices.

For more information on how you can use templates, see *Working with templates*, on page 7-2.

Working with templates and staged changesets

When you create a template, you are creating it for use in a staged changeset. A ***staged changeset*** is a device configuration changeset that is ready to be deployed. When you stage a changeset, the system prepares a configuration change but it requires additional information before deploying the change. You can control how users stage and deploy changesets based on their user roles. See *Working with role permissions*, on page 3-22, for more information on how to employ user roles to manage templates.

A staged changeset is similar to a standard changeset that is ready to be deployed to a specific set of devices. The difference is that a staged changeset can be saved in its ready state for later use.

When you create a changeset, or a staged changeset, you can use a template as the configuration source. When you do this, your choice adds the variable functionality to the changeset or staged changeset.

For more information about staged changesets and templates, see *Staging configuration changes*, on page 8-1. For more information about creating standard changesets, see *Creating a changeset for a device*, on page 6-5.

Understanding changesets and templates

Although changesets and templates each represent a collection of configuration files that you can use for managing device configurations, changesets and templates differ in three primary ways. The following table outlines the main differences.

Changesets	Templates
Contain a set of configuration data for a specific device.	Organized so that a user can manage the individual elements of configuration data that vary from device to device.
Are designed so that you can deploy a specific set of configuration data to other devices without changing any values in the configuration.	Are designed to use variable values to create device-specific changesets, or to stage configuration changes from a generalized set of configuration data to devices with varied configurations.
Can be used for a wide variety of tasks, including setting up a device, maintaining consistent configurations on multiple devices, and creating new applications.	Can be used to stage individualized configuration changes to multiple devices.

Table 7.1 *Differences between changesets and templates*

Working with templates

In many cases, you can use templates in a fashion similar to the way you use changesets. Because templates offer you the ability to set variables for use with different devices in the network, you can use templates in conjunction with changesets to help streamline and standardize common network configuration tasks.

Publishing templates

When editing a template, you can choose to publish the template. By publishing a template, you make the template available to other users for use in creating staged changesets. By default, new templates are unpublished.

If you create a prototypical configuration setting using a template, you can permit other Enterprise Manager users to use this template for their own changesets by publishing it. For example, if you use a template to create a standard virtual server that includes the necessary configuration information for other similar virtual servers, other users may benefit from using your template.

If a template is not published, restricted users such as Operators and Advanced Operators cannot use it to stage a changeset (Administrators can use any template in the system except Standard Templates).

This adds an additional layer of control to device configuration management when combined with the requirement that all staged changesets must be verified before they are deployed.

Using templates when adding new devices

When you add a new device to the network, you can use a changeset to deploy common configuration elements (including profiles, monitors, iRules, and network objects) to the new device. For information about using a changeset when adding a new device to the network, see *Using changesets when adding new devices*, on page 6-2.

If you use a prototypical device as the model for new devices in your network, you can extend the usefulness of changesets by using templates to manage variables for new devices.

For example, if you manage devices in multiple data centers that reside in multiple time zones, you may want to create a template to set the time zone on a device. To do this, create a template that sets the time zone, and make the time zone setting a variable. Then, edit the allowed values for the variable to include all the necessary times zones. See *Creating a template*, on page 7-9, for more information on how to create a template.

Once you save the template, you can use it in either a standard changeset or a staged changeset. When you configure the changeset using the template as the source, you can select a time zone appropriate for the devices in your network.

Working with variables

While changesets require that you manage network object dependencies, configuration templates usually require that you manage template variables in order to successfully use templates as a device configuration management tool. ***Template variables*** are unique values or settings required by each managed device in order to properly run the configuration change specified by the template.

Because a template is essentially a guideline for a configuration change that you can apply to multiple independent devices, you must specify network object information specific to the device that you are managing. This information can include such data as virtual server names, node addresses, or other network object address and port information.

When you use a template in a staged changeset, you can deploy the same device configuration change to multiple independent managed devices. This can help you avoid creating additional changesets for common configuration changes. For example, if you create a template to disable a node on a managed device and you want to disable more than one node, you do not

need to create separate changesets to disable each node. Instead, you can create one changeset that disables a node at a variable IP address. Then, you can stage a changeset using this template, and you can choose a unique IP address each time you stage and deploy the changeset.

For more information about staged changesets and templates, see *Staging configuration changes*, on page 8-1.

Understanding the elements of template variables

In order to successfully manage template variables with Enterprise Manager, you must understand the different elements of the variable that you can control. There are six main elements of a variable that you can customize:

- **Variable name**
  Usually, the system chooses a variable name, but in some cases, you can specify a different name for the variable. The name you choose appears in the template configuration text. This name also appears in a staged changeset if you do not specify a variable description.
- **Default variable value**
  When you assign a variable, you can assign a default value, or specify a collection of allowed values for the variable. If you assign a default value, the system uses this value for the variable when you deploy a changeset based on this template (although the user deploying the changeset can change the value).
- **Variable description**
  Because only the variable name is visible in the template text, and is usually system-assigned, it is helpful to assign a description to the variable. This can help other users properly use the variable when they stage or deploy a changeset based on this template.
- **Whether the variable is editable**
  When you create a template as an Administrator-level user, you can determine whether a restricted user such as an Operator or Advanced Operator can change a variable when they use the template to stage a changeset.
- **Visibility of the variable**
  If you restrict a user's ability to edit the value of a variable, you then have the option to hide the variable setting from restricted users when they use the template to stage a changeset.
- **Allowed variable values**
  Although you can specify a default value for the variable, you can also specify what values are allowed in the variable. By doing this, you can ensure that any user staging a changeset with this template sees a list of values rather than simply specifying a value (which can prevent errors).

When you create a configuration template with variables, you can modify these elements before you save the template. Additionally, you can modify these settings by clicking the **Manage Variables** button on a template properties screen.

Understanding variable syntax

Typically, when you create a template, you use a wizard to construct the template from network objects on a managed device in your network. The wizard prompts you for the necessary information, and automatically generates the proper text syntax for the template. See *Using the Template wizard to create a template*, on page 7-9, for more information.

As you create the template using the Template wizard, or when you view the general properties of an existing template, you can view the text version of the template.

When you add a variable to the template, the Enterprise Manager system adds a line to the text version of the template. You can also create a variable name and add it to the template manually. When you add a variable to a template, you must use the following format, where **<variable_name>** is the name of the variable in the network object.

```
@define <variable_name>
```

Enterprise Manager uses the leading at symbol (@) to distinguish a variable from static configuration information in a template. (The at symbol is not required, but it ensures that a variable name is unique and easily identified when you read the configuration text.) Additionally, the **@define** text flags the line as a variable, and prompts the system to replace the variable with a value when deployed. When you deploy a staged changeset created with a template, the system replaces the variable information from any line that begins with **@define** when it writes new information to the target device's configuration files.

For example, if you create a template to disable a node, you can write the following in the **Text** box on the Template Variable Properties screen:

```
@define @node_ip
#F5[Local Traffic / Node]
#F5[$target_partition$]
node @node_ip {
    session disable
}
```

In the preceding example, the first line specifies the variable **@node_ip** after the variable flag **@define**. The second line indicates the Object Class and instance. The third line indicates the partition. The fourth line starts the command to disable the node, and runs the **session disable** command on the node indicated by the variable **@node_ip.**

◆ Note

*When Enterprise Manager creates a variable automatically, it may write the variable with **@replace** before the variable name. Although this is also a valid variable flag, it is much more granular than **@define**, which directs the system to look for a variable term.*

Understanding dependencies

As with changesets, in order to successfully copy a network object from one BIG-IP system to another using templates, 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 template.

Because you can use templates in a more granular fashion compared to changesets, you may not need to include dependencies in templates. For example, if you create a template simply to enable or disable a virtual server, you do not need to include dependencies because the action you are taking (enabling or disabling the virtual server) is the important part of the configuration change. When you deploy a staged changeset to a device to enable or disable a virtual server, the Enterprise Manager system changes the virtual server's state, and all dependent objects are affected as if you changed the virtual server's state on the managed device itself.

Working with standard templates

Enterprise Manager features several built-in standard templates that demonstrate common device configuration tasks. A ***standard template*** is a configuration template included with Enterprise Manager that provides a simple configuration source for some common traffic management tasks.

You can use standard configuration templates as a source template to accomplish most of your common device configuration management tasks. In order to use these templates, you can use a standard template as the configuration source for a new template, changeset, or staged changeset. As an alternative, you can copy the template configuration information from the template properties screen to create a new text-based configuration templates, changesets, or staged changesets.

Currently, we provide seven standard configuration templates that cover seven basic tasks.

Template Name	Description
ltm_create_simple_http_vip_and_pool	Creates a basic HTTP virtual server and pool
ltm_pool_member_disable	Disables a local traffic pool member (allows established sessions)
ltm_pool_member_enable	Enables a local traffic pool member
ltm_pool_member_down	Sets a local traffic pool member to **down** (allowing no new connections)
ltm_node_enable	Enables a local traffic server address (all pools)
ltm_node_disable	Disables local traffic server address (for all pools, only allowing established sessions)
ltm_node_down	Sets a local traffic server address to **down** (for all pools, allowing no new connections)

Table 7.2 *Standard configuration templates and descriptions*

To view standard template properties

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Templates**.
   The Templates list screen opens.
2. To filter the list to show only Standard templates, click the down arrow at the top of the Type column, and select **Standard**.
3. In the templates list, click the name of a template.
   The template properties screen opens.

Using a standard template for common tasks

A standard template can help with common device management tasks. For example, if you need to perform maintenance on a device in your network, you need to prevent connections to nodes on device while you perform maintenance. After you complete your maintenance tasks, you enable connections. If you use a standard template, you can create a list of variables that cover all of the node addresses on the system, and use that template to create a staged changeset to **down** nodes on a device. At this time, you can create a staged changeset to enable the nodes on a device.

The following example is a procedural outline that involves many procedures detailed in this chapter and other chapters. For information about how to create a template, see *Creating a template*, on page 7-9. For information about how to create a staged changeset, see *Staging configuration changes*, on page 8-1. To learn how to deploy a staged changeset, see *Verifying and deploying staged changesets*, on page 8-5.

To use a standard template for a maintenance task

1. Create a new configuration template using the New Template wizard.
2. In the New Template wizard, select a template source for the new template, then select the **ltm_node_down** standard template.
3. On the Template Variables screen in the wizard, set the allowed values for the node IP address variable (**@NODEIP**) for the template to cover all the node IP addresses that you require.
4. Save the template.
5. Create a staged changeset using the New Staged Changeset wizard.
6. In the New Staged Changeset wizard, use a template source for the staged changeset, then select the template that you just created.
7. In the Target Device Selection screen in the wizard, select target devices for the staged changeset.
8. On the Manage Variables screen in the wizard, set the variable value.
9. Save the staged changeset.
10. Deploy the staged changeset using the Deploy Staged Changeset wizard from the New Task screen.
11. After the staged changeset sets the nodes you selected to the down state, you can perform the maintenance on the device.

You can adapt the previous example to use a standard template to enable the nodes once you complete your maintenance. Then, after you complete your maintenance, you can deploy a staged changeset to enable the nodes on the device.

Creating a template

When you create a template, you use the Template wizard. The Template wizard works in a way similar to other task wizards, such as the Changeset wizard. In most cases, you must meet the same requirements and follow the same procedures that you would when you create a changeset with the Changeset wizard.

The main difference between the Template wizard and the Changeset wizard involves adding variables. Changesets do not support variables, and templates require additional information to manage variables. When you add variables to a template, you manually type the variable code into the template text when you create the template unless Enterprise Manager automatically defines variables for your template.

Once you create a template, you can use it as a building block for a staged changeset. See *Staging a changeset using the Staged Changeset wizard*, on page 8-2 for more information.

Using the Template wizard to create a template

The Template wizard works like the other wizards in Enterprise Manager, and helps guide you through the process of creating a template. It is especially similar to the Changeset wizard.

Creating a template using the wizard involves the following main steps:

- Specifying the source device and partition
- Selecting the object classes that you want to include (if you select a device source)
- Choosing the specific objects and their dependencies for each object class (if you select a device source)
- Adding and managing variables
- Reviewing the template details

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

Selecting a source device and partition

The first step in creating a template is selecting a template source. The ***template source*** can be a managed device in the network from which you want to copy some or all of its device configuration, an existing template, or textual configuration information copied from another configuration file.

If you select the template source device, you can select the administrative partition from which you want to copy the device configuration information. ***Administrative partitions*** are logical containers including a defined set of BIG-IP system objects and are used for access control purposes. The

Enterprise Manager template feature is compatible with administrative partitions. BIG-IP system versions 9.4 and later support administrative partitions.

Important

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

If you select an existing template, you must then choose from a list of templates already defined on the Enterprise Manager system.

If you select a text source, you must paste a portion of a configuration file in the **Text** area on the following screen.

To select a source

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Templates**.
   The Template List screen opens.
2. Above the list, click **Create**.
   The New Template screen opens.
3. In the **Name** box, type the name of the template.
   This name later appears on the template list.
4. In the **Description** box, type a description of the template.
5. From the **Source** list, select one of the options for the source on which you want to base the configuration template.
   - **Device**: To use a network object or system setting from a managed device in the network.
   - **Existing Template**: To use a template that currently exists on Enterprise Manager.
   - **Text**: To copy and paste a portion of an existing configuration file.
6. Proceed according to the option that you chose for **Source**:
   - If you selected **Device**, then in the **Partition** list, select the partition from which you want to copy objects.
   - If you selected **Existing Template**, then from the template list that appears, select a template by clicking the option button next to the template name.
   - If you selected **Text**, you do not need to do anything else on this screen.
7. Click **Next** to open the next screen in the wizard.

If you select either **Text** or **Existing Template** for the **Source** in step 5, then the Template Properties screen opens next. For information about the Template Properties screen, see *Managing template properties*, on page 7-16. After you modify the template properties screen, you must then edit the variable values on the Variable Properties screen. See *Assigning variables in a template*, on page 7-13.

If you select **Device** for the **Source** in step 5, then the Class Selection screen opens next. To work with this screen, see *Selecting object classes for device-based templates*, following.

Selecting object classes for device-based templates

After you specify a source device and partition, you need to select the object classes that you want to include in the template. An ***object class*** is the general type of network object that you want to include in a template. 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 template.

Adding object classes to templates is similar to adding object classes to a changeset. See *Selecting object classes*, on page 6-7, for information about object class types and what objects they affect.

To select object classes

You select object classes on the Step 2 screen of the New Template wizard. This screen appears if you chose a device source on the Step 1 screen.

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 template.
2. Repeat step 1 as necessary to add additional classes to this template.
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 template. An ***object instance*** is the specific network object that you want to include in the template.

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

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.

To specify objects and dependencies

You select objects starting from the Step 3 screen of the New Template wizard. The screen number varies depending on the number of object classes selected; object selection screens appear as necessary so that you can select objects for each object class you selected in the Step 2 screen.

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. To move to the next screen to manage dependencies on the summary screen, or to add a different type of object instance, click **Next**.

Note

*If you are adding more than one object class to the template, 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 template summary screen where you can include dependencies.*

Important

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

Reviewing dependencies on the summary screen

Once you add objects to the template, you can choose whether to include dependencies in the template.

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

To review and change dependency information

After you select object classes and objects for a device-based template, you can review details of the objects you selected on the template summary screen.

1. In the **Dependency Handling** box, select whether to include dependencies.
   The **Resource Objects** 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.
3. 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.
4. Once you review and change information in the template, click **Next** to move to the Template Properties screen.

Assigning variables in a template

After you manage the dependency requirements for the template, you can assign variables to the template, if necessary.

Template variables are values or settings required by each managed device in order to properly run the configuration change specified by the template. Because templates include variables, you can use templates in different staged changesets to perform similar configuration changes on unique devices.

When you manage variables, you can determine the name of the variable (if it is not already set by the network object that you include in the template), the default value of the variable, and allowed values for the variable. You can also determine whether a variable is editable or visible to other users upon deployment.

◆ Note

Some network objects (such as nodes or pools) automatically generate variable information when you add them to a template. Other network objects (such as system settings) require that you manually add variable information such as the variable name and default value.

To edit template properties and variables

After you review object and dependency details, you can edit properties of the template on the Template Properties screen, including variables.

1. In the **Description** box, change the template description if necessary.
2. In the **Require verification of staged changesets** box, check the Select box to require that a user run a verify process prior to deploying a staged changeset based on this template.
3. In the **Allow staged changesets to persist** box, check the Select box to save any staged changesets based on this template in the staged changesets list after it is deployed.

4. In the **Text** box, make any necessary changes to the template as necessary:
   - To add a variable, type **@define <variable_name>** where **<variable_name>** is the name of the variable that you want to add.
   - To add a command, type the appropriate **bigpipe** command inside the brackets. The system runs this command for the network object indicated before the brackets.
   - To specify a variable for a network object, replace the network object address or value with **<variable_name>** where **<variable_name>** matches the variable you added previously.
5. Click **Next** to move to the Template Variable Properties screen where you can manage variable values in the template.

◆ Note

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

To manage variable values

The Template Variable Properties appears after the template properties screen in the New Template wizard.

1. In the Variable Properties table, in the **Default Value** box next to a variable name, type a default value for the variable. This is the value the system uses by default when the template the source of a staged changeset.
   ***Note**: If you want to specify only certain values instead of just specifying a default value, click the **Edit Allowed Values** button to add a collection of permitted values for this variable. See **To manage allowed values in a variable**, following.*
2. In the **Description** box, type a brief explanation of the variable so that a description of the variable appears when a user stages a changeset using this template.
3. If you want to permit Operators or Advanced Operators to edit this variable when they use it in a staged changeset, verify that the **Editable** Select box is checked.
4. If you choose to restrict other users from editing the variable, you can determine whether the variable is visible by checking the **Visible** Select box (it is enabled by default, but is only available if you restrict variable editing).
5. Click **Finish** to save changes to the variable.

Optionally, you can edit the allowed values for the variable. If you specify one or more allowed values for a variable, then when a user stages a changeset based on this template, he is presented with a set list of values

from which to choose. When you specify allowed values, you can control exactly which values are permitted. This may reduce the chances of the user entering an incorrect value when he stages a changeset.

To manage allowed values in a variable

In many cases, you will want to add additional control over how variables are used by users staging changesets based on this template. By creating a list of allowed values, you can specify which values users can employ for a given variable in a template.

You can manage allowed values from the Template Variables table on the template general properties screen. This screen appears in the configuration Template wizard or you can click the **Manage Variables** button from a template properties screen to view the Template Variables table.

1. In the Template Variables table, click the **Allowed Values** button. The Allowed Values screen opens.
2. For the **New Value** box in the **Values** section, type a value that matches the variable. For example, if the variable represents the state of an object, you can type **enable**, or if the variable represents the IP address of an object you can type an IP address.
3. Click **Add** to add the variable to the allowed values list. The value that you typed in the **New Value** box moves to the **Values** list.
4. Repeat steps 2 and 3 as necessary to add additional allowed values.
5. If you need to remove a variable from the list, in the **Values** list, click the name of the variable, then click **Remove**.
6. Click **Save** to save your changes to the allowed values list and return to the template properties screen.

Previewing a template with variables

After you define a variable, set its description, and manage its allowed values, you may want to preview how the variable appears when a user stages a changeset using this template.

When you preview a template, you can see how it appears on the staged changeset screen without needing to actually create or stage a changeset. This gives you the opportunity to verify that the values are accurate, and that the settings are what you expect.

The preview screen emulates the actual stage changeset form that users see when they stage a changeset using this template. It presents elements that a user sees, including target device information, and a list of the variables, and how the user can select or enter variables.

On the preview screen, the variables appear next to the description of the variable in four possible ways:

- With a list box that list includes all of the allowed values for the variable.
- With either an empty box or a box with a value, indicating that a user can change the value in the box to any variable that she requires.
- With a static value that indicates that a restricted user cannot change the variable
- With no variable listed, which means that restricted users cannot view the variable, or that no variable is defined for the template.

To preview a template variable

You can preview all variables in a template from the Template Variables screen in the Template wizard, or from the template properties screen of an existing template. This is useful to see how variables, default, and allowed values appear to other users when they stage a changeset based on this template.

1. Below the **Text** box, click **Manage Variables**.
   The Template Variable Properties screen opens, displaying a list of template variables and descriptions.
2. Below the Variable Properties table, click **Preview**.
   The Staged Changeset Variables Preview screen opens, displaying an example of how the variables appear to a user staging a changeset based on this template.

Working with the template list

After you create a configuration template, the template appears in the template list. The template list displays all of the configuration templates that are stored in the Enterprise Manager database.

You can view this list by clicking the **Templates** link on the Main tab of the navigation pane. From the template list, you can view the general properties of any template, create a new template, or delete a template.

Managing template properties

The general properties of a template give an overview of the template, including the template text. You can use the general properties as a starting point for several template-related tasks, including managing variables, or staging a changeset using this template.

To view the general properties of a template

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Templates**.
   The Templates list screen opens.
2. In the templates list, click the name of a template.
   The template properties screen opens.

Once you open the template properties screen, you can manage several aspects of the template.

Changing basic template properties

There are several elements of a template that you can modify directly on the template properties screen. This include the description, whether the template is published, whether a changeset based on this template requires verification before deployment, or whether a staged changeset based on this template is saved after deployment for later use.

Modifying the description simply changes the description text that appears on the template list screen.

Deciding whether a template is published determines whether this template appears as a source option for creating a changeset or other template. If you publish the template, other users can use the template as a source.

Requiring verification affects how users deploy staged changesets based on this template. If you choose to require verification, then a user deploying a staged changeset based on this template must run the verify process prior to deploying the changeset.

If you choose to allow the changeset to persist, this saves a staged changeset based on this template in the staged changeset list after a user deploys the changeset. When you allow changesets to persist, you can re-deploy the staged changeset from the staged changeset list, which can save you time over re-configuring a staged changeset.

To modify basic template properties

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Templates**.
   The Templates list screen opens.
2. In the templates list, click the name of a template.
   The template properties screen opens.
3. In the **Description** box, change the template description if necessary.
4. To make this template available as a source for other users creating changesets and templates, check the **Published** box.

5. To require that a user run a verify process prior to deploying a staged changeset based on this template, check the **Require verification of changesets** box.
6. To save any staged changesets based on this template in the staged changesets list after it is deployed, check the **Allow changesets to persist** box.
7. Click **Save Changes**.

Starting other template modifications from the general properties screen

If you want to change a configuration template, you can modify the template text on the general properties screen. See *Modifying a template*, following, for more information.

To modify a template from properties screen

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Templates**.
   The Templates list screen opens.
2. In the templates list, click the name of a template.
   The template properties screen opens.
3. Click the setting for the task to perform:
   - If you want to manage template variables, click the **Manage Variables** button to display the Template Variables table. See *Working with variables*, on page 7-3, for more information on how to manage template variables.
   - If you want to stage a changeset using this template as the source, click **Stage for Deployment**. See *Verifying and deploying staged changesets*, on page 8-5, for more information.

Modifying a template

When you create a configuration template, Enterprise Manager stores the template 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 template.

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

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

To modify a template

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Templates**.
   The Template List screen opens.
2. Click the name of the template that you want to modify.
   The Template Properties screen opens.
3. Above the Template Text table, select **Advanced**.
   The **Text** box expands to show additional text management tools.
4. Modify the template based on your requirements:
   - To change the description of the template, in the **Description** box type a new description.
   - To add objects to the template, 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 template, you can change any existing text in the Text area.
5. After you finish making changes, click **Save Changes** to save the template.

Important

*If you change variable definitions when you modify a template, you must update values on the Manage Variables screen by clicking the **Manage Variables** button.*

Importing and exporting templates

Because configuration templates establish a flexible basis for changing device configurations, you can share templates among Enterprise Manager devices in your network, or with other users through the F5 developer community DevCentral (**http://devcentral.f5.com**).

DevCentral is an online community featuring tools, technology, and collaboration for F5 products. After registering for free, you can access resources such as discussion forums, documentation wikis, and sample applications. In the Samples section, you can find sample templates for Enterprise Manager, and you can share templates that you create.

Importing a template is as simple as copying and pasting text from the site to the **Text** box of a new template.

You can export a template by copying template text from the Template Export screen. After you copy the text, you can use it on other Enterprise Manager systems, or share it on the DevCentral CodeShare site.

Importing template text from DevCentral

1. Log on to the DevCentral site, **http://devcentral.f5.com**.
2. Log on to your account or register for a new account.
3. Click the **Samples** link at the top of the screen.
   The samples screen opens, displaying the latest contributions to the CodeShare pages.
4. Click the **Advanced Design & Config** link.
   The Advanced Design & Config CodeShare screen opens, listing all sample code available in this category.
5. In the Sample EM Templates section, click the name of a sample template.
   A screen opens describing the purpose of the template, what platforms it has been tested on, and any additional important information about the template.
6. In the Template Text section, highlight the template text.
7. Copy the text. (On the browser menu, from the Edit menu, select Copy, or press Ctrl+C).
8. Log on to Enterprise Manager.
9. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Templates**.
   The Templates list opens.
10. Above the template list, click the **Create** button.
    The New Template screen opens.
11. In the **Name** and **Description** boxes, type an appropriate name and description for the new template.
12. For the **Source** setting, select **Text**.

13. Click **Next** to move to the Template Properties screen.
14. In the **Text** box, paste the text that you copied from DevCentral. ***Note****: If template properties such as name and description are defined in the template text, this supersedes any properties settings defined in the Template Properties table above the* ***Text*** *box.*
15. Click **Next** to move to the Template Variable Properties screen.
16. After you configure variables for the template, click **Finish**.

For detailed information about creating a template see *Using the Template wizard to create a template*, on page 7-9.

Exporting template data

The text on the Template Export screen is formatted specifically for exporting. The text includes all the necessary settings in the proper syntax so that you can use the template on another system.

1. On the Main tab of the navigation pane, expand Enterprise Management and click **Templates**.
   The Templates list opens.
2. Click the name of the template that you want to export.
   The template general properties screen opens.
3. On the menu bar, click **Export**.
   The export template screen opens.
4. In the **Text** box, highlight the template text.
5. Copy the text. (On the browser menu, from the Edit menu, select Copy, or press Ctrl+C).

After you copy the text, you can paste it into another **Text** box to create a new template, or you can submit it for inclusion on the DevCentral CodeShare site.

8

Working with Staged Changesets

- Staging configuration changes
- Verifying and deploying staged changesets

Staging configuration changes

In addition to using templates to create changesets, you can use templates as a source for a staged changeset. A ***staged changeset*** is a fully-configured device configuration change order that is ready to be deployed.

When you stage a changeset, the system prepares a configuration change, but usually awaits approval from another user before deploying the change. When a changeset is in the staged state, administrators can review and verify configuration changes before they deploy the changes.

Additionally, you can give users with an Operator or Advanced Operator role the ability to stage a changeset using published templates in Enterprise Manager. This permits you to delegate responsibility for basic configuration changes to users with different user roles. By default, only Administrator-level users can edit templates or create changesets, but user roles determine which users can use templates to create or deploy staged changesets. This ensures that only high level administrator users can modify certain elements of a template, providing more flexibility in designating template creation and staging privileges to other users in the enterprise. For more information about user roles, see *Managing user roles*, on page 3-22.

A user's role in Enterprise Manager™ determines the way that he works with staged changesets. There are three ways to stage a changeset:

- After creating a changeset using the Create Changeset wizard
- From the template or changeset properties screen
- As soon as you need to stage a configuration change using the Staged Changeset wizard

Staging a changeset after creating a new changeset

After you create a changeset using the New Changeset wizard, you can immediately stage the changeset on the final screen of the wizard.

See *Staging a changeset using the Staged Changeset wizard*, on page 8-2, for detailed instructions on creating a changeset.

Once you reach the final step of the wizard, click **Stage Changeset** to immediately stage the changeset.

Staging a changeset from the template properties screen

You can use the Staged Changeset wizard to stage a changeset based on a specific template from that template's properties screen.

To stage a changeset from a template properties screen

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

2. In the templates list, click the name of a template.
   The template properties screen opens.
3. If you want to stage a changeset using this template as the source, click **Stage for Deployment**.
   The Staged Changeset wizard opens on the target device selection screen.

Staging a changeset using the Staged Changeset wizard

The Staged Changeset wizard works in a fashion similar to other wizards in Enterprise Manager. There are five main steps involved in creating a staged changeset:

- Selecting the staged changeset source
- Choosing the target devices
- Choosing the target partitions on the devices, if applicable
- Managing the properties of a staged changeset, including the description, task options, and variable settings
- Verifying, saving, or deploying the staged changeset

Depending on your user roles, there may be more than one slightly different workflow when using the Changeset wizard. For example, administrators and other designated users can create and stage a changeset from the task list. However, if you have a non-administrator user role, that role may determine that you cannot verify and deploy the staged changeset.

For information about user roles and how they apply to the tasks involving staged changesets, see *Managing user roles*, on page 3-22.

Starting a staged changeset task

When you create a staged changeset, you use start from the Task List screen like you would start any other task. From the Task List screen, you proceed to the New Task screen where you can choose to create a staged changeset.

To start a staged changeset task

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Tasks**.
   The Task List screen opens.
2. Above the task list, click the **New Task** button.
   The New Task screen opens.
3. In the Configurations area, select **Stage a Changeset**.
   The New Staged Changeset screen opens.

Selecting a staged changeset source

After you start the task, you must select a source for the staged changeset. You can stage a changeset based on a template or changeset.

To select a changeset source

The first step in creating a staged changeset requires selecting the source for the staged changeset. You do this on the Create Staged Changeset screen, which appears after you select a **Stage a Changeset** on the New Task screen.

1. In the **Staged Changeset Source** box, select one of the following:
   - **Template** - To select an existing configuration template on which to base the staged changeset.
   - **Changeset** - To select an existing standard changeset on which to base the staged changeset.

   The table below changes to display templates or changesets depending on your selection.
2. In the table, select the option button next to the template or changeset that you want to use as the source.
3. Click **Next** to move to the device selection screen where you select target devices for the staged changeset.

Selecting a target device for a staged changeset

After you choose the staged changeset source, you can select one or more target managed devices for the staged changeset. When you deploy the staged changeset, the system makes the changes to the target devices as specified in the source configuration.

To select target devices

The Step 1 screen of the New Staged Changeset wizard appears after you select a staged changeset source.

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 staged changeset source you specified on the previous screen.
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 staged changeset, you can select specific administrative partitions for each of these devices, if the devices support administrative partitions.

To select device partition targets

1. In the Device Partition Selection table, in the **Partition 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 staged changeset properties screen.

Setting task properties

After you specify the partitions for the staged changeset, you can set properties for the task, including a description of the task that appears on the task list or staged changeset list.

When you configure a staged changeset, you can direct the system to create a UCS archive before a user deploys the staged changeset. This provides you with the option to roll back 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 deploy a staged changeset, you can also choose whether or not to include private SSL keys in the UCS archive, if you choose to create a UCS archive.

You can also specify variable values for the staged changeset if you used a template source that features variables.

To set task properties

1. In the **Description** box, type a brief note about the staged changeset. Other users can use this information when they verify or deploy the staged changeset.
2. For the **Create 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 **Archive Options** setting, you can choose to include private SSL keys in the UCS archive or not.

After you set the properties, you can manage variables for the staged changeset, verify the changeset, deploy the staged changeset, or save the staged changeset.

If you want to manage variables, see *Setting staged changeset variables*, on page 8-5.

If you want to save the staged changeset, see *Saving the staged changeset*, following.

For information about verifying and deploying staged changesets, see *Verifying a staged changeset with the Staged Changeset wizard*, on page 8-6.

Setting staged changeset variables

When you create a staged changeset with a template source that features variables, you can specify values for these variables on the staged changeset properties screen.

To set variable values

The Variable Values table displays a list of target devices. Beneath each target device, a list of configuration changes may appear. Next to certain configuration changes, a box or list appears, indicating that you can specify or select a different variable value.

To change variable values, in the Variable Values table, next to a variable, select or type a new variable value.

Saving the staged changeset

When you create a staged changeset, you can save it to deploy again later. If you anticipate re-using the staged changeset at a later date, it could save you time to retain the staged changeset so that you can deploy it again from the staged changeset list screen.

To save the changeset

To save the staged changeset, click **Save Staged Changeset**.
The staged changeset list screen appears, and the staged changeset you just created appears in the list.

Verifying and deploying staged changesets

Once you create a staged changeset, you can immediately verify or deploy the staged changeset if you have the proper user role privileges. You can also verify or deploy a staged changeset from the staged changeset list, or from the staged changesets properties screen.

◆ Tip

We recommend that you verify a staged changeset prior to deploying it to ensure that it works properly on the target device. When you create a template, if you flag the template to require verification, then all staged changesets based on the template must be verified. When this is the case, the ***Deploy*** *button appears only after you have verified the staged changeset.*

Verifying a staged changeset

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

After you create a staged changeset, you can verify the compatibility of the staged changeset on the target device before deploying it.

When you verify a staged changeset, Enterprise Manager checks to see if the network object classes included in the staged changeset can work properly with the software installed on a target system. However, the verify feature does not check the validity of every system setting included in the staged changeset.

A wizard guides you through the verify staged changeset process, and when you complete the task, you have the option to deploy the staged changeset.

◆ Note

*The Verify Staged Changeset feature uses the **bigpipe verify merge** command to check the compatibility of staged changeset data on the target devices you select.*

Verifying a staged changeset with the Staged Changeset wizard

When you create a new staged changeset, you have the option to verify the staged changeset on the last screen of the wizard. On this screen, you can also set staged changeset properties, and save the changeset.

To verify the staged changeset

1. On the Staged Changeset Properties screen (Step 3 of 3 in the New Staged Changeset wizard), at the bottom of the screen, click the **Verify** button.
   The Verify Status screen opens, displaying information about the running **bigpipe verify merge** command. The system indicates whether the staged changeset verification is successful on all target devices.
2. Once the process quits running, click the **Finished** button to return to the Staged Changeset Properties screen.

Verifying one or more staged changesets from a list

If you want to verify one or more staged changesets, you can start a verify task from the staged changeset list screen. You configure the task using a wizard to set task options and properties. When you complete the task, you can immediately deploy the staged changeset.

To verify one or more staged changesets

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Staged Changesets**.
   The Staged Changeset screen opens.
2. Check the Select box next to each staged changeset that you want to verify.
3. Click the **Verify or Deploy** button.
   The Verify Changeset Wizard opens on the Task Options screen and prompts you to choose an error behavior.

See *Using the Verify Staged Changeset wizard*, following, for instructions on working through the verify staged Changeset wizard.

Verifying a staged changeset from the properties screen

Another way that you can verify a staged changeset is to start a verify staged changeset task from the properties screen. When you do this, you can view the text configuration of a staged changeset prior to verification.

To verify a staged changeset from the properties screen

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Staged Changesets**.
   The Staged Changeset screen opens.
2. Click the name of a staged changeset.
   The Staged Changeset general properties screen opens.
3. Click the **Verify or Deploy** button.
   The Verify Staged Changeset wizard starts.

See *Using the Verify Staged Changeset wizard*, following, for instructions on working through the Verify Staged Changeset wizard.

Using the Verify Staged Changeset wizard

The Verify Staged Changeset wizard is a simple, two-screen wizard that helps you configure the verify staged changeset task.

To configure the Verify Staged Changeset wizard

The Task Options screen is step 1 of the Verify Staged Changeset wizard and prompts you to choose an error behavior for the verify task.

1. For **Error Behavior**, select the action you want Enterprise Manager to take if it encounters an error during the task:
   - **Continue task on remaining devices** - specifies that the system continues to verify staged changesets on other devices until the task finishes.

- **Cancel task on remaining devices** - specifies that the system stops the verify task when the system first encounters an invalid staged changeset.

2. Click **Next** to move to the Task Summary screen.
   The Task Summary screen opens and displays task properties and a list of target devices on which the system will verify the associated staged changeset.
3. In the **Name** box, change the verify task description if necessary.
4. Click the **Verify** button.
   The Verify Status screen opens, displaying information about the running **bigpipe verify merge** command. The system indicates whether the staged changeset verification is successful on all target devices.
5. Once the process quits running, click the **Finished** button.

Deploying a staged changeset

When you deploy a staged changeset, Enterprise Manager makes the configuration changes on the target devices that are specified in the staged changeset. When the task completes, the target devices' configurations are changed as specified in the staged changeset.

A wizard guides you through the deploy staged changeset process, and when you complete the task, you have the option to verify the staged changeset prior to starting the deploy task.

You can start a deployment task from three places in Enterprise Manager:

- Immediately after you create a new staged changeset
- From the staged changeset list
- From a staged changeset general properties screen

WARNING

We recommend that you do not deploy a staged changeset with a source created from one version of a managed device to a device with a different software version. Because of differences in configuration data syntax between different software versions, deploying a staged changeset with one version of configuration data to a different version device may cause unexpected errors. To help differentiate configuration versions, we recommend that you include this information in the changeset, template, or staged changeset description.

Deploying a staged changeset with the Staged Changeset wizard

When you create a new staged changeset from the task list, you have the option to deploy the staged changeset on the last screen of the wizard. On this screen, you can also set staged changeset properties, and save the changeset.

To deploy the staged changeset

1. On the Staged Changeset Properties screen (Step 3 of 3 in the New Staged Changeset wizard), at the bottom of the screen, click the **Deploy** button.
   The Deploy Status screen opens, displaying information about the running deployment task. The system indicates whether the staged changeset deployment task was successful on all target devices.
2. Once the process quits running, click the **Finished** button to return to the Staged Changeset Properties screen.

Deploying one or more staged changesets from a list

If you want to deploy one or more staged changesets, you can start a deployment task from the Staged Changeset list screen. You configure the task using a wizard to set task options and properties.

To deploy one or more staged changesets

1. On the Main tab of the navigation pane, expand **Enterprise Management** and click **Staged Changesets**.
   The Staged Changeset screen opens.
2. Check the Select box next to each staged changeset that you want to deploy.
3. Click the **Verify or Deploy** button.
   The deploy Changeset wizard opens on the Task Options screen opens and prompts you to choose an error behavior.

See *Using the Deploy Staged Changeset wizard*, on page 8-10, for instructions on working through the deploy staged Changeset wizard.

Deploying a staged changeset from the properties screen

Another way that you can deploy a staged changeset is to start a Deploy Staged Changeset task from the properties screen. When you do this, you can view the text configuration of a staged changeset prior to deploying.

To deploy a staged changeset from the properties screen

1. On the Main tab of the navigation pane, expand Enterprise Management and click **Staged Changesets**.
   The Staged Changeset screen opens.
2. Click the name of a staged changeset.
   The Staged Changeset general properties screen opens.
3. Click the **Verify or Deploy** button.
   The deploy staged Changeset wizard starts.

See *Using the Deploy Staged Changeset wizard*, following, for instructions on working through the deploy staged Changeset wizard.

Using the Deploy Staged Changeset wizard

The Deploy Staged Changeset wizard is a simple, two-screen wizard that is identical to the Verify Staged Changeset wizard. The wizard helps you configure the deploy staged changeset task.

To configure the Deploy Staged Changeset wizard

The Task Options screen (step 1 of the Deploy Staged Changeset wizard) prompts you to choose an error behavior for the deploy task.

1. For **Error Behavior**, select the action you want Enterprise Manager to take if it encounters an error during the task:
   - **Continue task on remaining devices** - specifies that the system continues deploying staged changesets on other devices until the task finishes.
   - **Cancel task on remaining devices** - specifies that the system stops the deployment task when the system first encounters an invalid staged changeset.
2. Click **Next** to move to the Task Summary screen.
   The Task Summary screen opens and displays task properties and a list of target devices on which the system will deploy the associated staged changeset.
3. In the **Name** box, change the deploy task description if necessary.
4. Click the **Deploy** button.
   The Deploy Status screen opens, displaying information about the running deploy task. The system indicates whether the staged changeset deployment task was successful on all target devices.
5. Once the process quits running, click the **Finished** button.

9

Managing Software Images

- Managing image and file updates
- Installing software on managed devices
- Working with attack signatures
- Monitoring installation tasks

Managing image and file updates

Installing a software or hotfix upgrade on individual BIG-IP® systems 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. Additionally, if you manage multiple BIG-IP Application Security Manager™ systems, you may have to update multiple attack signatures on a regular basis.

With Enterprise Manager™ as your software image management system, you can catalog and store several versions of software, hotfixes, and attack signature definitions 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, hotfix, or attack signature images to the repository, you can then deploy these 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.

Downloading software, hotfix, and attack signature images

You can find updated software images on the F5 Networks Downloads site, **downloads.f5.com**. To access this site, you must create an account on the site. This site uses an F5 single sign-on account for technical support and downloads.

You can use the F5 Downloads site to download software upgrades, patches, hotfixes, signature files, and other files to assist you in managing devices in your network.

◆ Tip

There are several classes and types of software updates available on the F5 Downloads site. Because you are using Enterprise Manager as your software management system, when you upgrade software, we recommend that you download ***.iso*** *images to import into the software repository. The* ***.iso*** *image files contain all of the packages necessary for the software version you are using, and there is no need to specify local or remote installation versions.*

Understanding software file types

There are four main classes of file hosted on the F5 Downloads site. Usually, the files are one of these major classes:

- **Releases**
  Releases are full product releases, and usually include a software image intended to upgrade all software on a managed device to a newer version.
- **Hotfixes**
  Hotfixes are minor updates to the current software on a managed device that fix one or more known issues.
- **Signature Files**
  Application Security Manager Attack Signature files update the system-supplied attack signatures on a BIG-IP Application Security Manager system to ensure that your applications are protected against new attacks and threats.
- **Patches**
  Patches are usually fixes for vulnerabilities.

Within each of these classes, there are multiple main file types that you can download. Each file type serves a particular purpose. For some packages, we provide both local and remote installation options.

Table 9.1, following, outlines these file types.

File Type	File Extension	Purpose
Hotfix Package	**.im**	You can use **.im** packages to install smaller fixes to managed devices. Usually, these packages update a portion of the existing software without requiring a full installation. There are usually local and remote installation versions available.
Software Image	**.iso**	You can mount an **.iso** image to perform a full upgrade of the software on a managed device. The **.iso** image contains all the packages necessary to upgrade the managed device, and there is no local- or remote-specific type of **.iso** file.
Checksum	**.md5**	You can use the **.md5** file as a checksum to verify the integrity of the file after you download it.
Signature File	**.im**	You can use the **.im** file to update the system-supplied attack signature definitions on BIG-IP Application Security Manager systems. Enterprise Manager can manage the scheduled downloading of updates and installation of new signature files.
Documentation	**.txt** or **.readme**	You can use the text files included with some releases as a source of additional documentation.

Table 9.1 *File types available on* ***downloads.f5.com***

Working with different installation methods

For some packages (**.im** files), we provide both local and remote installation options. We provide alternate methods for installing your software depending on how you want to upgrade the software. If you use Enterprise Manager as your software management system, you must download the local installation version of the software. If you use an **.iso** image, there is no need to select between local and remote versions.

For reference, the differences between the two types of installation are:

- **Local installation**
  Installing software locally requires downloading the entire software image to the hard drive of the managed device and running the installation from the device.
- **Remote installation**
  Installing software remotely requires downloading the installation portion of a software image to the managed device, then manually installing the upgrade using the network as the upgrade source instead of using the managed device's local hard drive. This may be required for devices that use CompactFlash® storage instead of a hard drive.

Usually, you can tell the difference between the types of software images by reading the file name. For example, for the previous Enterprise Manager 1.2 release, there are two different **.im** packages available, **local-install-1.2.2.8.0.im** and **remote-install-1.2.2.8.0.im**. Each of these files installs version 1.2, but they use a different installation method.

Finding software images

The **downloads.f5.com** site hosts all available software upgrades (including hotfixes, patches, vulnerability fixes, and signature file updates) for managed devices. You can download these images to a local client system, then you can later import them to the Enterprise Manager image repository.

To download an image

1. Using a web browser connected to the internet, visit **http://downloads.f5.com**.
   The F5 Sign-on screen opens.
2. In the **User Email** box, type the email address associated with your F5 Technical Support account.
3. In the **Password** box, type the password.
4. Click the **Login** button.
   The Overview screen opens and provides notes about using the Downloads site.
5. Click the **Find a Download** button.
   The Product Lines screen opens listing all F5 product families.
6. Locate the appropriate product family and click the adjacent product version link.
   The Product Version screen opens, listing the available download containers for the current product version.
7. Select a product container by clicking the name of the container that corresponds to the software that you want to download.
   The End User License Agreement (EULA) screen opens.
8. Read the EULA and click **I Accept** to accept the licence agreement.
   The Select a Download screen opens.
9. To download a file, click the name of the file.
   The Select a Download screen opens, prompting you to select a file transfer protocol.
10. Click the download icon next to the protocol that you want to use.
    A dialog box opens, prompting you to save the file to your local system.

Checking the integrity of software images

After you download software images to a local system, you may want to check the integrity of the files that you downloaded. When we create software images, we also create an **md5** checksum. You can use the **md5** checksum to confirm that you have an exact copy of the file that is available on **downloads.f5.com**.

Depending on your client system, you can use a tool to check the validity of a file using the **md5** checksum. For Linux® systems, you can use the included **md5sum** tool from the command line. For other client systems, including Microsoft® Windows® systems, you may need to use an external application to check **md5** validity.

Working with the image repository

The Enterprise Manager image repository provides a central location where you can store all images for software upgrade, hotfix installation, and Application Security Manager attack signature definitions. Once you download software or hotfix images from the F5 Networks Downloads site, 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 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. There are three different image repositories (software, hotfix, and attack signature), but you can work with each image list in a similar fashion.

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.

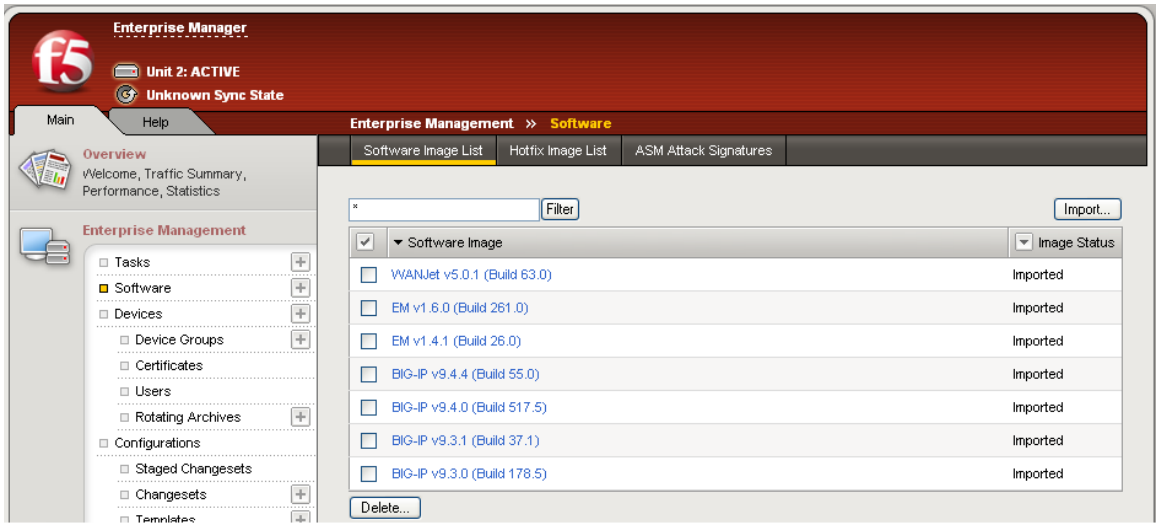

Figure 9.1 *The software image list displays the software images stored in the Enterprise Manager software repository. The menu bar selects different image list screens.*

To add an image to an image list

Once you download a software image from the F5 Networks Downloads site, you can add it to the appropriate 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 images.
2. To import a specific type of image, on the menu bar, click the image type:
   - **Software Image List**: for full version software images for upgrade or roll back.
   - **Hotfix Image List**: for a hotfix to an existing software installation.
   - **ASM Attack Signatures**: for system-supplied attack signatures for Application Security Manager systems.

   After you click an image type, the appropriate image list screen opens.
3. Above the image list, click **Import**.
   The Import 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 image list screen opens and the image name appears in the list with the status of **Importing**. When the importation completes, you can deploy the image to managed devices.

Important

When you import a software, hotfix, or attack signature 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, hotfix, or attack signature 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, hotfix images, or attack signatures

From the appropriate list screen, 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, hotfix, or attack signature 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 (that are compatible with the upgrade) 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***). BIG-IP hardware platforms support this functionality, and 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 **Tasks**.
   The New Task screen opens.
2. In the Software Installation section, click **Install Software Image**, then click **Next**.
   The Software Upgrade wizard opens, prompting you to select a software image upgrade, then devices on which to install the upgrade.
3. 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 Install Hotfix Images and click **Next**. See **Installing hotfixes to one or more devices** on page 9-13 for information on installing hotfixes.*

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 **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.
2. 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.
3. For **Device Filter**, select an option to display which devices are compatible, or which devices are not compatible, with the software image you selected for **Software Image**.
   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 Configuration Options list, select what device configuration to use on the newly upgraded boot location:
   - **Install full configuration** - copies the current full device configuration from another boot location to the newly upgraded boot location.
   - **Install minimum configuration** - leaves the newly upgraded boot location in a new, basic configuration state.

3. In the **Post Installation** list, select which boot location to use for rebooting the device upon completion of the upgrade process.
4. For **Configuration Archive**, select whether you want to include private SSL keys in the configuration archive created during the task.
5. 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.

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 installation 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 remove a device from the upgrade task:
   a) Click the **View** 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 Step 4 screen opens after you confirm the removal of the device from the software upgrade task.
3. If 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 **Tasks**.
   The task list screen appears.
2. Click the **New Task** button.
   The New Task screen opens.
3. In the Software Installation section, click **Install Hotfix Images**, then click **Next**.
   The Hotfix Installation wizard opens, prompting you to choose a product version and hotfixes to install.
4. Follow the steps on the following pages to work through the wizard screens to install hotfix upgrades.

Important

If the hotfix image that you want to install is not available in the hotfix list, you may need to download the hotfix image, or import it to the software repository. See ***Downloading software, hotfix, and attack signature images****, on page 9-1 or see* ***Adding images to the repository*** *on page 9-5.*

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 members of 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. For Device Filter, select an option to limit the devices that appear in the Compatible Devices table by selecting a display option:
   - **Compatible Devices in Standby Mode** - displays only compatible devices currently in Standby mode
   - **Compatible with Hotfix** - displays all devices compatible with the hotfix you selected on the previous screen

   ***Note**: The Compatible Devices table displays only devices that are compatible with the hotfix image(s) you selected on the previous screen.*
3. 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 previous screen.
4. To move to the next 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 select installation and task options for the upgrade task

You can specify the post-installation event or configure the task error behavior on the Step 3 wizard screen.

1. In the **Post Installation** list, select whether you want to reboot each device after installing a hotfix.
2. For **Device Error Behavior**, select the action that you want the system to take if it encounters an error during the task:
   - **Continue task on remaining devices** - finishes the task and installs the hotfix to as many selected devices as possible.
   - **Cancel task on remaining devices** - stops the task when an error occurs, and does not install the hotfix to any devices still pending.
3. To move to the Step 4 screen, where you can review the details of the hotfix installation task you configured, click **Next**.

To review hotfix installation options

You can review and elect to remove a device from the hotfix installation task in Step 4 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 **View** 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 installation tasks*, on page 9-22, 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.

Working with attack signatures

In addition to managing the installation of software and hotfix upgrades, Enterprise Manager can assist you in managing attack signatures for the BIG-IP Application Security Manager.

Attack signatures are the foundation of the Application Security Manager's negative security logic. ***Attack signatures*** are rules or patterns that identify attacks or classes of attacks on a web application and its components. For more information on how to use attack signatures with an Application Security Manager system, see the ***Configuration Guide for BIG-IP® Application Security Management***.

With Enterprise Manager, you can import system-supplied attack signatures into the image repository and deploy them to as many managed devices as you require. Additionally, you can use Enterprise Manager to check for updated system-supplied attack signatures and import them into the image list automatically.

Managing Application Security Manager attack signatures involves two main areas of management: managing signature updates, and installing new signatures. When you manage signature updates, you ensure that Enterprise Manager uses the latest Application Security Manager attack signature definitions available in the repository. When you install new signatures, you deploy these signatures to managed BIG-IP Application Security Manager systems.

Managing signature updates

As new threats are discovered, F5 regularly updates Application Security Manager attack signatures. Using Enterprise Manager, you can automatically check for, and download, new updated attack signature definitions for images stored in the image repository. If you use this feature, you can avoid possible frequent manual checks for updated attack signature files.

Additionally, at any time, you can check for updates to all definitions stored in the image repository from the ASM attack signature list screen.

Important

Enterprise Manager checks for updated Application Security Manager attack signature files from ***downloads.f5.com****. In order for the system to communicate with the F5 servers, you must configure the Enterprise Manager system settings to use your network DNS server. See* ***To configure DNS****, on page 3-16, for instructions.*

Updating signature images automatically

To keep the BIG-IP Application Security Manager systems updated on a regular basis, you can configure Enterprise Manager to regularly check for updated signatures. If updates are available for any attack signature in the image repository, you can automatically download the updates. Then, after you download the updates, you can start an Application Security Manager attack signature installation task to upgrade managed BIG-IP Application Security manager systems. See *Installing attack signatures to one or more devices*, on page 9-19 for more information.

If you do not want to automatically update signature images, you can configure an alert to notify you that updates are available, so that you can check for, and download these updates manually. See *Updating signature images manually*, on page 9-18 for instructions on manually updating attack signature images.

To schedule automatic attack signature file downloads

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Tasks**.
   The task list screen opens.
2. On the menu bar, click **Options**.
   The Tasks Options screen opens.
3. In the Attack Signature Update Schedule table, for **Check for Updates**, choose an option to determine how often the system checks for updates to existing attack signature images:
   - **Never**: Enterprise Manager does not automatically check for updated attack signature images.
   - **Daily**: The system checks for updated signatures once each day.
   - **Weekly**: The system checks for updated signatures once a week.
   - **Monthly**: The system checks for updated signatures once a month.

   Based on your selection, the table changes to display additional boxes for **Day of the Week**, **Day of the Month**, and **Start Time**.
4. 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 updates for attack signature images in the repository.
5. For **Automatically Download New Updates**, select whether you want to automatically add updated images to the repository.

6. Click **Save Changes** to save your changes.

Note

If you choose to not automatically download updated attack signature images, the system still triggers an alert when it checks for updated images if an alert is configured for new Application Security Manager signature updates. This alert is enabled by default, but you must specify an alert action on the Enterprise Manager Alerts screen to receive an email notification. See ***Configuring system alerts****, on page 11-5 for instructions.*

Updating signature images manually

If you receive an alert to check for updates, or if you want to periodically check for updates, you can update all attack signatures stored in the image repository from the ASM Attack Signatures list screen.

After you check for updates, you can download the updates from the Check for New Signatures screen.

To manually check for updated attack signatures

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Software**.
   The software images list screen opens.
2. On the menu bar, click **ASM Attack Signatures**.
   The ASM Attack Signatures screen opens.
3. Above the list click, **Check for New Signatures**.
   The Check for New Signatures screen opens and displays the status of the checking task.

The screen refreshes at regular intervals until the systems checks for any available updates for the signature files listed in the Available ASM Attack Signatures table. After the task completes, the system indicates if any update is available for each of the signature files in the repository.

To download updates for attack signature images

Manually downloading attack signature images requires that you previously checked for updated attack signatures and have opened the Check for New Signatures screen. See *To manually check for updated attack signatures*, preceding.

1. On the Check for New Signatures screen, in the Available ASM Attack Signatures table, check the Select box next to each signature file that you want to update.
2. Click **Start Task**.
   The ASM Attack Signature Update screen opens and displays the status of the update task.

The screen refreshes at regular intervals until the system updates all of the Application Security Manager attack signature files you selected on the previous screen. At any time, you can click **Exit to Task List** to open the Task List screen.

Note

You can also use the import image procedure to update attack signature images. See ***Adding images to the repository****, on page 9-5 for information about adding attack signature images to the image repository.*

Installing attack signatures to one or more devices

Because you want to regularly update attack signatures on Application Security Manager systems in the network, it is important to have a simple method of deploying signatures to many devices at once. You can use the Attack Signature Installation wizard to create an Application Security Manager attack signature installation task. An ***attack signature installation task*** is a series of jobs that you configure to install, to one or more managed devices, an Application Security Manager attack signature stored in the Enterprise Manager image repository. Each job consists of one individual signature update per device.

To start an attack signature installation task

1. On the Main tab of the navigation pane, expand **Enterprise Management**, and click **Tasks**.
   The task list screen opens, displaying all running and completed tasks.
2. In the Software Installation section, click **Install ASM Attack Signature**.
3. Click **Next** to start the Install ASM Attack Signature wizard and follow the steps on the following pages to work through the wizard screens to install attack signatures.

Important

If the attack signature that you want to install is not available in the signature list, you may need to download the attack signature image, or import it to the image repository. See ***Downloading software, hotfix, and attack signature images****, on page 9-1, or see* ***Adding images to the repository*** *on page 9-5.*

To select an attack signature to install

You can select an attack signature image in Step 1 of the Attack Signature Installation wizard.

1. From the **Product Version** list, select the product version to which the signature you are planning to install applies.
   The attack signatures table changes to display signatures compatible with the software version you selected.
2. In the attack signature table, select the option button to the left of any attack signature that you want to install.
3. To move to the next screen where you select devices on which to install the attack signature, click **Next**.

To select target devices

You can select the target devices for the attack signature installation on the Step 2 screen of the Attack Signature Installation wizard.

1. In the **Device Group** list:
   - If you want to install to devices belonging to a particular device group, select the device group name
   - Otherwise select **All Devices** to see a list of all devices compatible with the attack signature you selected.
2. For **Device Filter**, select an option to limit the results in the Compatible Devices table:
   - **Compatible Devices In Standby Mode**: displays all managed devices on which you can install the selected attack signatures that are in Standby mode.
   - **Compatible with Attack Signature**: displays all managed devices on which you can install the selected attack signature.
3. In the Compatible Devices table, check the Select box to the left of the devices for which you want to install the attack signature you selected on the previous screen.
4. To move to the next wizard screen, where you can set task options for the attack signature installation task, click **Next**.

To set task options

You can set error handling options for the attack signature installation task on the Step 3 screen of the Attack Signature Installation wizard.

1. For **Device Error Behavior**, select an option to determine what action Enterprise Manager takes when it encounters an error during the task:
   - **Continue Task on Remaining Devices**: the system finishes the task and installs the definition on as many selected devices as possible.
   - **Cancel Task on Remaining Devices**: the system stops the task when an error occurs, and does not install the attack signature on any devices still pending.
2. To move to the next wizard screen, where you can review and start the task, click **Next**.

To review task details

You can review task settings and change the task name for the attack signature installation task in Step 4 of the Attack Signature Installation wizard.

1. Review the information on the screen.
2. If any of the device information is incorrect, click the **Back** button to return to a previous wizard screen to correct it.
3. If you want to change the task name, in the **Task Name** box, type a new name.
   This name appears in the task list while the task is running, and after the task finishes.
4. To start the task to install the attack signature indicated in the **ASM Attack Signature** box on the devices indicated in the Task Summary table, click **Start Task**.
   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 as targets for attack signature installation, and the progress of each installation. The section *Monitoring installation tasks*, following, 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 installation tasks

When you start a software upgrade, hotfix installation, or attack signature update task, 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 individual jobs (such as installations or upgrades on a single device in a series) in a task finish, the system marks the task **Finished**, and 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, hotfix installation, or attack signature update, 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.

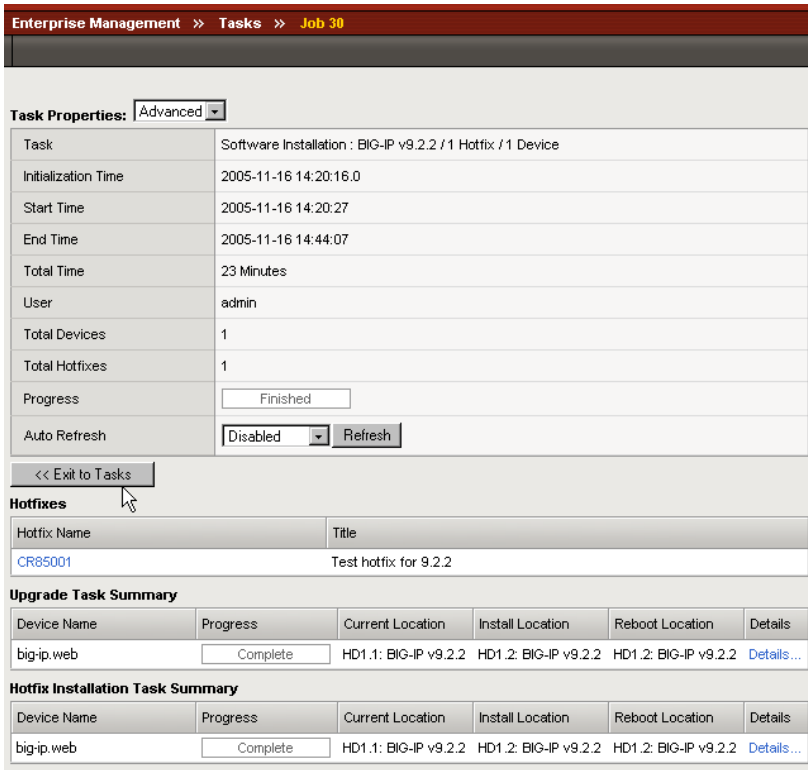

Figure 9.2 *The task properties screen displaying details of a software upgrade with hotfix installations*

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.

10

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 his 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 other wizards in Enterprise Manager. 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 user access 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 **Edit** 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 User Access 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 **Edit** 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.

11

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 cannot 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 on to the device to further investigate the device's status.

State	Status Icon	Condition Name
Enterprise Manager can contact the device, and the device is in Active Mode.		Active Mode
Enterprise Manager can contact the device and the device is in Standby Mode.		Standby Mode
Enterprise Manager cannot currently contact the device.		Unreachable
Enterprise Manager can contact the device, but cannot retrieve all of the information on the device.		Impaired
The connection between the device and Enterprise Manager is disabled because the device was set to Maintenance Mode.		Maintenance Mode
The device is in a modified state of Maintenance Mode for the purpose of replacing the physical device.		Device Replacement Mode

Table 11.1 *The six 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**.

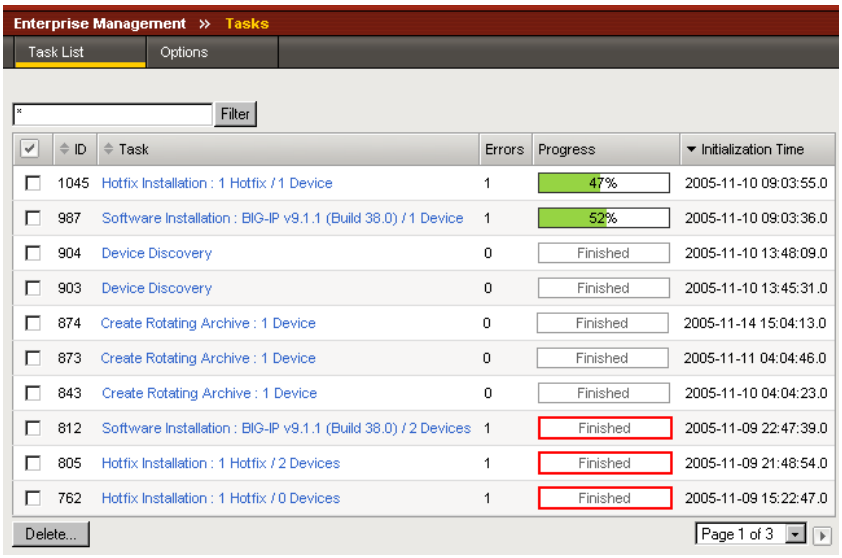

Figure 11.1 *The task list provides an overview of running and completed tasks*

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 most tasks complete, 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, including any dependent jobs required to complete the overall task. 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 3-14.*

To set alert default options

1. On the Main tab of 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 **Maximum History Entries** 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. On the Main tab of 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. For **Conditions**, check the appropriate Select boxes, depending on which metrics that you want to track with alerts.
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 you can use in managing your F5 Networks devices. The alerts that you can set include:

- Configuration change intervals for redundant systems
- Device status change
- Device unreachable by Enterprise Manager
- Certificate expired or near-expiration
- Completed software, hotfix, or attack signature image installations
- Failed software, hotfix, or attack signature image installations
- Clock skew between the Enterprise Manager and managed devices
- Failed rotating archive creation

Alerting for device status changes

When the state of a managed device changes, Enterprise Manager can send an alert message so that you can monitor the status of devices in the network. You can configure alerts for devices changing between Active and Standby mode, devices changing to an Impaired state, or when Enterprise Manager loses the connection to a managed device.

Warning for Active or Standby mode

When you manage redundant systems, Enterprise Manager monitors the Active or Standby state of each peer device. The status icon in the device list corresponds to the active/standby state of a device. When the status changes, the corresponding icon changes. However, if you want to immediately notify a user as soon as the active/standby stage of a managed device changes, you can configure a custom alert.

Warning for Impaired status

When Enterprise Manager cannot properly collect all configuration data from a device, but can still communicate with the device, the system changes the status to Impaired. The status icon for the device changes to indicate the impaired status.

This state occurs when Enterprise Manager cannot fully import all data from a managed device. For example, if you have an extremely long pool name, Enterprise Manager may truncate this name in its database. This does not affect the pool on the managed device, but it does affect how the pool is presented in Enterprise Manager. Although you can still perform management tasks on the device, because the configuration is not completely represented, the device status is marked Impaired.

You can configure a custom alert that immediately notifies a user if the status of a managed device changes to Impaired. If a device changes to Impaired, a user could take steps on the managed device to correct the situation.

Warning for an unreachable device

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 receive a warning 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 that the system triggers an alert on selected days, as the certificate expiration date nears.

When you create an alert for certificate expiration, we recommend that you select all possible thresholds for the alert (14 days, 7 days, 3 days, and 1 day from expiration) to ensure that you receive as many reminders as possible prior to certificate expiration.

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 who 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 (more than a 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.

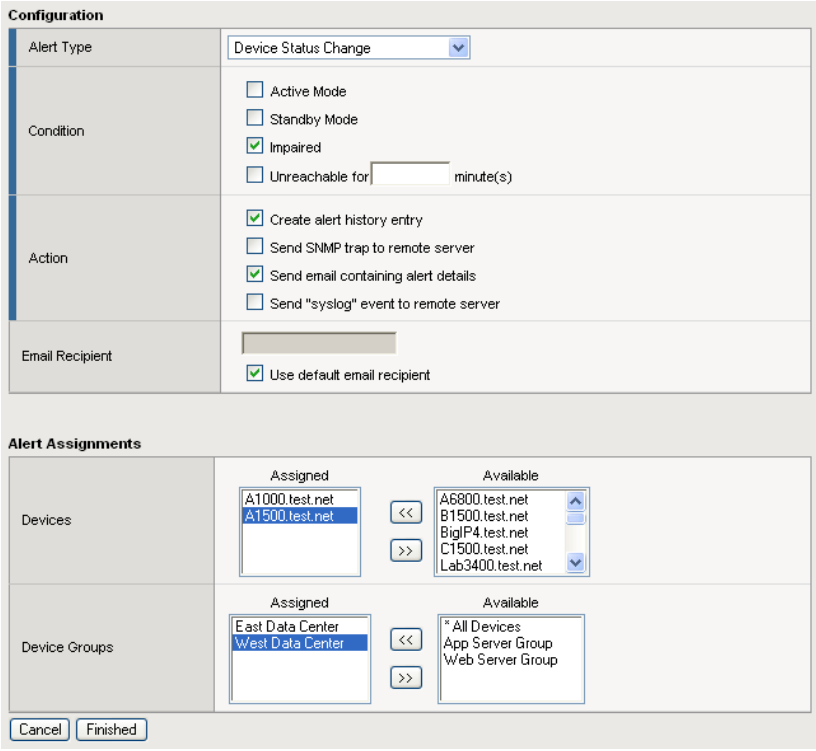

Figure 11.2 *Defining the alert type and actions, then assigning devices to the alert on the New Alert screen*

To create an alert for a device or device group

1. On the Main tab of 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, for each setting, 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 the option 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:
   - To send an email to the default email recipient listed on the Alert Options screen, check the Select box.
   - To send an email to an alternate recipient, clear the Select box and type a new email address.
8. If you selected the option 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:
   - To log an event on the default syslog server listed on the Alert Options screen, check the Select box.
   - 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.

12

Managing Device Certificates

- Working with device certificates
- Exporting device certificate information

Working with device certificates

Because the BIG-IP® Local Traffic Manager™ can control your SSL traffic, you may have a large number of SSL and web certificates on many different Local Traffic Manager 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 Local Traffic Manager 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 on to 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** list, click the name of a device or device group.
4. Click the Move (**<<**) button.
   The selected device or device group moves to the **Enabled** list.
5. Click **Save Changes**.
   Enterprise Manager now monitors certificates defined on the devices and device groups that you moved to the **Enabled** list.

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. For the **Devices** or **Device Groups** setting, in the **Enabled** list, click the name of a device or device group.
4. Click the Move (**>>**) button.
   The selected device or device group moves to the **Disabled** list.
5. Click **Save Changes**.
   Enterprise Manager no longer monitors certificates defined on the devices and device groups that you moved to the **Disabled** list.

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 12.1 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 12.1 *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.

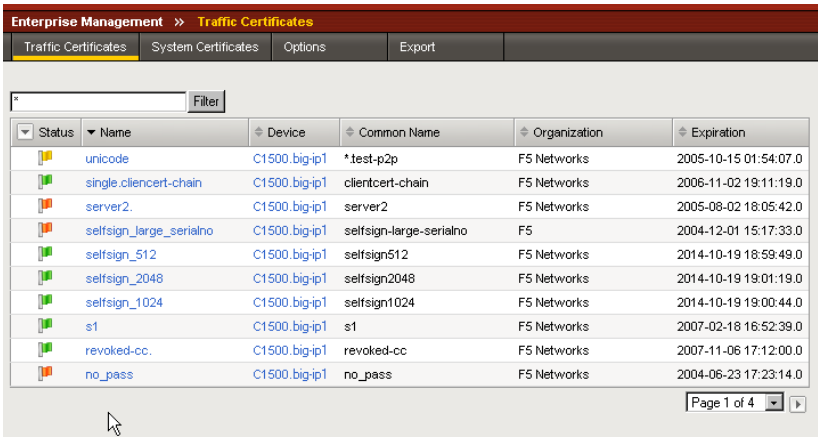

Figure 12.1 *The Traffic Certificates screen outlines important certificate information*

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 11-4.

◆ Note

You cannot configure certificate-based alerts on devices or device groups until you enable certificate monitoring on those devices or device groups.

Exporting device certificate information

When managing device certificates, you may want a simple, single-file copy of all the certificate information about all certificates that are stored on all managed devices in the network. You can use Enterprise Manager to export a list of all certificates (including all pertinent values for each certificate) to a file in a comma-separated values format.

For each certificate, the exported file contains the following information:

- Certificate Name
- Device Name
- Certificate Type
- Key Type
- Version
- Serial Number
- Expiration Date
- File Name
- Bit Length
- Management Mode
- Common Name
- Subject Organization
- Subject Division
- Subject Country
- Subject State
- Subject Locality
- Issuer Organization
- Issuer Division
- Issuer Country
- Issuer State
- Issuer Locality

To export certificate information

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 **Export**.
   The Certificates Export screen opens.
3. In the **File Name** box, click the **certificate_export.csv** link.
   A browser-based dialog box opens so that you can rename or save the file on your local system.

After you save the file, you can open it using a text editor or spreadsheet application.

13

Auditing Enterprise Manager System Events

- Working with Enterprise Manager system logging
- Searching the audit log

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 features seven processes that enable the system to manage other F5 devices in the network. The processes are briefly described here:

- **discoveryd**
  This process enables the device discovery features so that Enterprise Manager can identify and manage F5 devices in the network.
- **emadmind**
  This process enables the scheduled Enterprise Manager ConfigSnyc feature.

- **emalertd**
  This process enables the custom alerting features for managed devices, including creating alert instances, assigning alert actions, and logging alert events.
- **emdeviced**
  This process enables device management features such as managing device groups, performing high availability functions, and refreshing device status information.
- **emfiled**
  This process enables the features required to manage device configuration archives, including scheduling a rotating archive schedule, and maintaining pinned archives.
- **emreportd**
  This process enables the reporting features so that you can export certificate or configuration 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

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 enabled. 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.
- **Enable**
  This causes the system to log messages for user-initiated configuration changes only. This is the default value.
- **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 change the audit logging state

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 logs

You can find the Enterprise Manager system log in the same location as you can find it on the BIG-IP system. The Enterprise Manager audit log is available from the same screen.

To view log files

1. On the Main tab of the navigation pane, expand **System**, and click **Logs**.
   The System Logs screen opens.
2. Depending on the type of log you want to view, do one of the following:

- To view local traffic logs, on the menu bar, click **Local Traffic**. The screen changes to display a log of local traffic events.
- To view Enterprise Manager logs, from the Audit menu, choose List.
  The screen changes to display a log of management activity on this Enterprise Manager system.

Searching the audit log

When you need to find specific events in the audit log, you can use the Enterprise Manager audit search feature to find specific events by user, event text, or by date.

To search the audit log

1. On the Main tab of the navigation pane, expand **System**, and click **Logs**.
   The System Logs screen opens.
2. From the Audit menu, choose Search.
   The Search Logs screen opens.
3. For **User Name**, type all or part of a user name to search the audit log for user names that match.
   ***Note**: You can use the default asterisk (*) to search for all user names.*
4. For **Start Time**, select a month, day, year, and time to set the earliest point for the audit log search.
5. For **Stop Time**, select a month, day, year, and time to set the latest point for the audit log search.
6. For **Event Text**, type all or part of a character string included in the **Event** description in the audit log.
   ***Note**: You can use the default asterisk (*) to search for all event text.*
7. Click **Search** to perform the search using the criteria you specified. A table appears below the Search Properties table that lists all audit log entries that meet your search criteria.

To refine your search, you can change any values in the Search Properties table, then click **Search** again. If you want to perform a different search, click **Reset** to clear the values, then enter new search criteria.

Glossary

administrative partitions

Administrative partitions are logical containers containing a defined set of BIG-IP® system objects and are used for user management purposes.

attack signature

Attack signatures are the foundation of the BIG-IP Application Security Manager's negative security logic. Attack signatures are rules or patterns that identify attacks or classes of attacks on a web application and its components.

attack signature installation task

An attack signature installation task is a series of jobs that you configure to upgrade one or more attack signature definitions on managed BIG-IP Application Security Manager™ systems with definitions that are stored in the Enterprise Manager image repository.

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 template

A configuration template is a configuration management tool that works with existing changesets to create a model device configuration framework for use in creating new changesets.

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 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.

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.

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 BIG-IP Local Traffic Manager 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*.

NAT (Network Address Translation)

A NAT is an alias IP address that identifies a specific node managed by the BIG-IP system to the external network.

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.

staged changeset

A staged changeset is a device configuration changeset that is ready to be deployed. When a user stages a changeset, the system prepares a configuration change but awaits approval from a designated user before deploying the change.

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 on to the BIG-IP system Configuration utility.

template

See *configuration template*.

template variables

Template variables are unique values or settings required by each managed device in order to properly run the configuration change specified by the template.

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.

variables

See *template variables*.

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

A

Active Directory 3-21
address range
  discovering by subnet 4-2
  for SSH access 3-6
admin account 3-5
administrative partitions
  and changesets 6-7
  and templates 7-9
  defined 6-7
  in a staged changeset 8-4
  in a text changeset 6-16
Administrator user role 3-22
advanced network, configuring 3-6
Advanced Operator user role 3-22
alert defaults, configuring 11-4
alert history
  setting maximum entries 11-5
alerts
  assigning device groups 11-10
  assigning devices 11-10
  configuring system alerts 11-5
  defining alert types 11-6
  deleting 11-11
  for certificate expiration 11-7
  for clock skew 11-8
  for completed installation tasks 11-7
  for device unreachable 11-7
  for failed installation tasks 11-8
  for failed rotating archive schedule creation 11-8
  modifying 11-11
  setting an action 11-10
  setting default email recipient 3-14
  setting default syslog server address 3-14
  setting defaults 3-14
  setting maximum history entries 3-14
  specifying alert condition 11-10
  specifying alert type 11-9
allowed values
  for a variable 7-15
archive. See UCS archives.
ASM attack signatures. See attack signatures
attack signature installation
  reviewing task options 9-21
  selecting devices 9-20
  selecting image 9-20
Attack Signature wizard 9-19
attack signatures
  automatically updating 9-17
  definition 9-16
  installing on managed devices 9-19
  updating definitions 9-16
  updating manually 9-18
audit logging
  enabling 13-3
  searching log files 13-5
  viewing log files 13-3
authentication
  specifying the source 3-21
auto-discover and devices 4-2

B

base registration key 3-1
basic network
  configuring 3-6
BIG-IP system
  managing 4-1
boot location
  and availability on BIG-IP platforms 9-8

C

certificate monitoring
  disabling 12-2
  enabling 12-1
certificates
  creating alerts for expiration dates 12-3
  viewing details 12-3
  viewing status 12-2
Change User Password wizard 10-6
changeset
  adding new class path in text 6-11
  and adding new devices 6-2
  and administrative partitions 6-7, 7-10
  and applications 6-3
  and available object classes 6-8
  and available system classes 6-8
  and differences from templates 7-2
  and differences from UCS archives 6-2
  and managing dependencies 6-4
  and new standards 6-3
  and object classes 6-7
  and object instances 6-9
  and syntax for text configuration 6-13
  and system classes in text changeset 6-15
  and UCS 6-1
  and variables 6-12, 6-13
  creating 6-5
  creating by text entry 6-13
  creating with wizard 6-5
  defined 6-1
  deploying 6-18
  editing configuration text 6-13
  for object classes in text changeset 6-15
  for text elements 6-15
  in a staged changeset 8-3
  introducing 6-1
  modifying 6-17
  modifying configuration text 6-11

reviewing the summary 6-10
See also staged changeset.
selecting a source in wizard 6-6
staging 8-1
staging for deployment 6-11
syntax for object settings in text configuration 6-16
using a device source 6-6
using a template source 6-6, 6-12
verifying 6-17
Changeset wizard
introduction 6-5
overview of tasks 6-5
reviewing the summary 6-10
selecting a device source 6-7
selecting a source 6-6
selecting a template source 6-12
selecting object classes 6-7
selecting object instances 6-9
selecting system classes 6-8
command syntax conventions 1-15
compatibility. See feature compatibility.
ConfigSync
and Enterprise Manager systems 3-9
enabling auto-detect 4-9
scheduling for Enterprise Manager peers 3-11
setting defaults for Enterprise Manager pair 3-11
synchronizing redundant system 4-10
configuration search feature 5-14
configuration template. See template.
Configuration utility
accessing 3-1
and Enterprise Manager 1-9
configuration viewer 6-20
Copy User Access Configuration wizard 10-3

D

dependencies
and templates 7-6, 7-12
managing in a changeset 6-4, 6-10
managing in a template 7-6
Deploy Staged Changeset wizard 8-10
DevCentral
and templates 7-20
device
creating changeset for 6-5
device configuration
changing 8-1
in changesets 6-1
managing with changesets 6-1
searching 5-14
viewing 6-20
device configuration archives
default settings 3-13
device configuration data
comparing 5-11
deploying 6-18
deploying a current configuration 6-19
managing with changesets 6-2
managing with templates 7-3
device group
using with alerts 4-14
device groups
creating 4-12
managing members 4-13
using with software upgrades 4-14
device licenses
managing 4-15
device list
adding devices 4-2
deleting devices 4-6
device replacement mode
enabling 4-24
using the checklist 4-24
devices
adding to device group 4-12, 4-13
adding to device list 4-2
deleting from device list 4-6
discovering 4-2
managing device group memberships 4-14
managing redundant systems 4-8
rebooting remotely 4-10
removing from device group 4-13
selecting as changeset source 6-7
setting communication properties 4-7

E

email
configuring postfix options 3-17
starting postfix service 3-15
email recipient
setting default 3-14, 11-5
Enterprise Manager processes 13-1
Enterprise Manager system
installing software 9-9
managing as managed device 4-2
EULA
and managed devices 4-15

F

failover
changing device state 4-9
definition 4-8
managing device state 4-8
feature compatibility
with basic user management features 1-2
with changesets 1-3
with high availability features 1-5
with tasks 1-4
fully qualified domain name 3-4

G

General Properties screens, viewing 1-11

H

help 1-12
high availability 1-5
and guidelines for Enterprise Manager systems 3-10
configuring Enterprise Manager pair 3-10
configuring initial settings 3-4
installing software 9-8
managing redundant systems 4-8
reviewing variance in Enterprise Manager pair 3-8
setting up an Enterprise Manager 3-10
history entries
setting alert history maximum 3-14
hotfix installation
monitoring on task list 9-22
reviewing task options 9-15
selecting devices 9-14
selecting image 9-13
starting 9-13
Hotfix Installation wizard 9-13

I

installation 2-1
interfaces
choosing for management 2-1
configuring for NAT 2-4
configuring for SNAT 2-6
configuring for tiered network 2-5
for Enterprise Manager pair 3-10
using management 2-2
using TMM switch 2-2
IP address
discovering devices with 4-2
iRules
and changesets 6-10
and templates 7-12

L

Launch Pad
using 10-5
LCD
setting management IP address 3-4
LDAP 3-21
license
activating 3-1
and F5 products 3-1
License Device wizard 4-15
licenses. See device licenses.

M

maintenance mode
defined 4-22
enabling 4-23
turning off 4-23
managed device
definition 4-1
managing a BIG-IP system 4-1
managing a WANJet appliance 4-1
managing an Enterprise Manager system 4-2
managing group memberships 4-14
rebooting 4-10
See also devices.
management interface 3-4
menu 1-9
menu bar 1-11
MGMT port. See interfaces.

N

NAT
configuring devices to work with Enterprise Manager 2-4
using with Enterprise Manager 2-4
navigation pane 1-9
network configuration
configuring SNAT 2-6
configuring tiered network 2-5
using NAT 2-4
using with SNAT 2-6
working with NAT 2-4
working with tiered configuration 2-5

O

object classes
and templates 7-11
available for changesets 6-8
including in a text changeset 6-15
including in changesets 6-7
syntax for text configuration 6-15
using unclassified objects in a changeset 6-15

object instances
adding to a changeset 6-9
and templates 7-11
object list screens 1-10
object settings
and syntax for text changeset 6-16
online help 1-12, 1-17
Operator user role 3-22

P

partition
See administrative partitions.
permissions
for user roles 3-22
pinned archives
creating 5-8
pinning a rotating archive 5-9
restoring to a device 5-10
setting maximum number 3-13
platform guide 1-16
platform management configuration
creating 3-3
platform management settings 3-3
postfix service
configuring options 3-17
starting 3-15
preferences
Enterprise Manager 3-8

Q

Quick Start Instructions 1-16

R

RADIUS 3-21
redundant pair 3-4
redundant systems
managing failover state 4-8
managing high availability 4-8
synchronizing 4-9
refresh interval 3-12
release notes 1-16
resource objects. See dependencies.
restricted user roles
and templates 7-3
root account 3-5
rotating archives
creating a schedule 5-5
deleting archives 5-7
managing 5-4
modifying 5-5
modifying archives 5-7
restoring to a device 5-10
setting maximum number 3-13

S

Setup utility
running 3-6
SNAT
configuring to work with Enterprise Manager 2-6
using with Enterprise Manager 2-6
SNMP
determining version compatibility 3-15
setting defaults 3-15
software images
checking integrity 9-5
downloading 9-1
file types 9-2
software installation
adding a hotfix 9-11
and tiered configurations 9-9
displaying compatible devices 9-10
monitoring on task list 9-22
on Enterprise Manager systems 9-9
performing rollbacks 9-9
reviewing task options 9-12
selecting devices 9-10
selecting images 9-10
setting the install location 9-11
starting a task 9-10
software repository
adding ASM attack signatures 9-6
adding hotfixes 9-6
adding images 9-5
adding software images 9-6
removing images 9-7
Software Upgrade wizard 9-8
adding a hotfix to a software installation 9-11
SSH access 3-6
SSL certificates 12-1
staged 8-8
staged changeset
and templates 7-1
and UCS archives 8-4
and user roles 8-1
creating 8-2
defined 8-1
deploying 8-8
deploying from a list 8-9
deploying from properties screen 8-9
deploying through a wizard 8-8
deploying with wizard 8-10
for wizard 6-18
managing variables 8-5
previewing variable settings 7-15
saving 8-5
selecting administrative partitions 8-4

selecting source 8-3
selecting target devices 8-3
setting task properties 8-4
staging a changeset 8-1
verifying 8-6
Staged Changeset wizard 8-2
standard template
defined 7-7
included templates 7-7
using for common tasks 7-8
status icons 11-1
stylistic conventions 1-15
subnet
and device discovery 4-2
searching by class B or C network 4-3
support account 3-5
Support Information wizard 4-19
syslog server address
setting default 3-14, 11-5
system
using unit ID 3-5
system alerts 11-5
system certificates
definition 12-1
See also certificates.
system classes
and related object instances 6-8
and syntax for text configuration 6-15
as available for changesets 6-8
including in a text changeset 6-15
system event logging
and events 13-1
differences from a BIG-IP system 13-2
enabling 13-2

T

tables
filtering 1-11
sorting 1-10
task list
deleting items 9-22
deleting tasks 11-3
monitoring installation tasks 9-22
opening 9-15, 9-21
using as overview 11-2
task properties screen 11-4
tasks
cancelling pending 9-22
viewing details 9-23
technical support 1-17
template
and included standard templates 7-7
creating 7-9
template list 7-16
template properties
changing 7-17
managing 7-16
See also templates.
template variables. See variables.
Template wizard
assigning variables 7-13
introducing 7-9
managing variable values 7-14
previewing staged changeset variables 7-15
reviewing dependencies 7-12
selecting a partition 7-9
selecting a source 7-9
selecting object classes 7-11
templates
and administrative partitions 7-9
and allowed variable values 7-15
and dependencies 7-6, 7-12
and DevCentral 7-20
and device configuration management 7-1
and differences from changesets 7-2
and iRules 7-12
and list screen 7-16
and object classes 7-11
and object instances 7-11
and staged changeset 7-1
as a changeset source 6-6, 6-12
creating 7-9
defined 7-1
editing properties 7-13
editing text 7-5
editing variables 7-13
exporting 7-20
importing 7-20
in a staged changeset 8-3
managing properties 7-16
managing variable values 7-14
modifying 7-18
publishing 7-2
See also staged changeset.
selecting a source 7-9
using standard templates 7-7, 7-8
using to add new devices 7-3
variables 7-13
wizard 7-9
text changeset
constructing elements 6-15
creating 6-13
tiered configuration
configuring to work with Enterprise Manager 2-5
installing software 9-9
using with Enterprise Manager 2-5
time zone 3-5
TMM switch interface. See interfaces.

traffic certificates
definition 12-1
See also certificates.

U

UCS
and changesets 6-1
UCS archives
and differences from changesets 6-2
and staged changesets 8-4
backing up Enterprise Manager configurations 5-2
comparing 5-11
creating a default rotating schedule 5-5
deleting archives 5-7
managing 5-1
managing devices in a rotating schedule 5-5
managing in a rotating schedule 5-4
modifying archives 5-7
restoring Enterprise Manager archives 5-3
restoring to a managed device 5-10
saving a UCS archive 5-8
working with Enterprise Manager archives 5-1
upgrade. See software installation or hotfix installation.
user account
adding users 3-19
choosing an authentication source 3-19
modifying Enterprise Manager users 3-20
setting the authentication source 3-21
user account data
copying 10-3
managing for managed devices 10-1
managing with the Launch Pad 10-5
user accounts
managing Enterprise Manager users 3-19
user configuration set. See UCS archives.
user list screen 10-1
user role
and permission chart 3-23
and restricted types 3-22
and staged changesets 8-1
for types 3-22
managing 3-22
specifying 3-23
using permissions 3-22
users
managing with the Configuration utility 10-2
viewing in a list 10-1
viewing roles on managed devices 10-2

V

variable
name 7-4
variables
and allowed values 7-4
and changesets 6-13
and default value 7-4
and elements of a variable 7-4
defined 7-13
description 7-4
editing in a template 7-13
in a changeset 6-12
in a template
managing allowed values 7-15
managing in a staged changeset 8-5
managing values 7-14
previewing 7-15
using syntax for configuration text 7-5
Verify Staged Changeset wizard 8-7

W

WANJet appliance
managing 4-1
warm backup
and Enterprise Manager high availability 3-8
definition 3-8
web certificates 12-1
web certificates. See also certificates.
wizard
using Attack Signature 9-19
using Change User Password 10-6
using Changeset 6-5
using Compare Device Configurations 5-11
using Copy User Access Configuration 10-3
using Deploy Staged changeset 8-10
using Hotfix Installation 9-13
using License Device 4-15
using New Staged Changeset 6-18
using Software Upgrade 9-8
using Staged Changeset 8-2
using Support Information 4-19
using Template 7-9
using Verify Staged Changeset 8-7