Enterprise Manager™ Administrator Guide

version 2.3

MAN-0314-03

Product Version

This manual applies to product version 2.3 of the Enterprise Manager.

Publication Date

This manual was published on November 21, 2011.

Legal Notices

Copyright

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

Trademarks

3DNS, Access Policy Manager, Acopia, Acopia Networks, Advanced Client Authentication, Advanced Routing, APM, Application Security Manager, ARX, AskF5, ASM, BIG-IP, Cloud Extender, CloudFucious, CMP, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, EM, Enterprise Manager, F5, F5 [DESIGN], F5 Management Pack, F5 Networks, F5 World, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iApps, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, IT agility. Your way., L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, Message Security Module, MSM, Netcelera, OneConnect, Packet Velocity, Protocol Security Module, PSM, Real Traffic Policy Builder, Scale^N, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, TrafficShield, Transparent Data Reduction, VIPRION, vCMP, WA, WAN Optimization Manager, WANJet, WebAccelerator, WOM, 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.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by U.S. Patent 6,505,230. Other patents pending. This list is believed to be current as of November 21, 2011.

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/).

Table of Contents

1

Performing Basic Device Management

2

User Roles and Authentication

3

Managing UCS Archives

4

Using Templates and Changesets to Manage Device Configurations

5

Managing Software Images

6

Managing User Account Data

7

Monitoring Object and Device Performance

8
Using Alerts

9
Managing Device Certificates

10
Auditing Enterprise Manager System Events

11
Working with Application Security Manager Policies and Attack Signatures

Glossary

Index

1

Performing Basic Device Management

- Overview of device management
- Performing basic tasks on managed devices
- Viewing device status
- Managing licenses
- Using high availability systems
- Collecting information for F5 support
- Maintaining and replacing devices

Overview of device management

F5 Networks® Enterprise Manager™ is an appliance that simplifies the administrative tasks associated with managing multiple F5 Networks devices. Enterprise Manager also collects and stores information about managed devices in a database, which you can access through a web-based interface. The product is scalable, so as you add F5 devices to your network, you can manage them using Enterprise Manager.

You can use Enterprise Manager to manage:

- Devices running BIG-IP® software version 9.3 or later
- BIG-IP® Local Traffic Manager™ Virtual Edition version 10.2 or later
- BIG-IP® Secure Access Manager™ version 8.0 or later
- WANJet® version 5.0 or later
- All Enterprise Manager devices

Although Enterprise Manager works with multiple versions of BIG-IP software, we recommend that you upgrade your managed devices to the latest version to ensure the most optimal performance.

Performing basic tasks on managed devices

Once you add devices to the Device List screen, you can remotely perform basic management tasks, such as:

- Verifying and testing device communication
- Rebooting devices
- Specifying device refresh interval
- Deleting devices

◆ **Note**

For specific information about discovering and importing devices, see the ***Enterprise Manager™ Getting Started Guide****.*

Verifying and testing device communication

When Enterprise Manager discovers a device, it adds it to the device list with the default IP address that you specified. While Enterprise Manager can see the device at this address, you must ensure that the managed device can communicate back to Enterprise Manager. You do this by verifying that the IP address for Enterprise Manager is properly configured. If it is not, then the device cannot communicate back to Enterprise Manager, and the software update functionality does not work properly.

To verify the Enterprise Manager IP address on a device

1. On the Main tab, 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. From the **Device Properties** list, select **Advanced** to display additional device properties.

4. In the **EM Address** field, verify 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.

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 device's connection to Enterprise Manager

1. Log on to the managed device command line as the **root** user.
2. 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**.

   A **connected to <EM_address>** message means that the device can properly communicate with Enterprise Manager.

◆ **Important**

*If you receive a **connection refused** message, you may need to change the IP address in the **EM Address** field on the Device Properties screen, or addresses specified in your NAT or SNAT.*

Rebooting managed devices to a new software image

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 the 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 Main tab, expand **Enterprise Management**, and click **Devices**.
   The Device list screen opens.
2. Click the name of a device.
   The Device Properties screen opens.
3. On the menu bar, click **Properties,** and **Boot Location**.
   The Boot Image Locations screen opens, displaying the active and available boot locations and the software installed on each.

4. Click the select button for the image that you want to use to reboot the device.
5. Click **Reboot**.
   After you confirm the reboot, the device reboots and the screen refreshes to indicate the new active boot location.

Specifying a device refresh interval

By default, Enterprise Manager collects information once every 60 minutes, and displays that information on the Device List screen and device's General Properties screen. You can reduce the amount of management traffic by increasing this interval, or you can more closely monitor the state of devices by decreasing the interval.

◆ **Tip**

*You can refresh device information immediately at any time, by selecting devices and clicking the **Update Status** button on the Device List screen, or on the General Properties screen of a specific device.*

To specify a device refresh interval

1. On the Main tab, expand **Enterprise Management**, and click **Options** and **Devices**.
   The Device Options screen opens.
2. In the **Refresh Interval** field, type a new interval value to adjust the number of minutes that the Enterprise Manager waits before requesting new information from each managed device.
3. Click **Save Changes**.

Deleting devices from the device list

To remove a device from the Devices list, select the check box next to the device you want to remove, and click **Delete**.

◆ **WARNING**

If you delete a device from the Device List screen, Enterprise Manager removes from its database all associated configuration information for that device, such as alerts, certificate information, and device archives. If you add this same device to Enterprise Manager in the future, you must re-configure these settings.

Viewing device status

With Enterprise Manager™, you can get an immediate overview of the status of the devices in your network by viewing the status icons on the Device List screen. (You access the Device List screen by expanding the **Enterprise Management** on the Main tab and clicking **Device**.)

Status icons, as defined in Table 1.1, provide quick insight into the state of your network because they indicate whether Enterprise Manager is successfully connecting to all of your managed devices.

Icon	Connection Condition
🟢	Active Mode Indicates that the device is enabled and that the Enterprise Manager can connect to the device.
⚪	Standby Mode Indicates that Enterprise Manager can connect to the device.
♦	Offline Mode Indicates that the device is enabled, but offline, and that the Enterprise Manager cannot connect to the device.
◆	Forced Offline Mode Indicates that only active connections to the device are allowed.
⚠	Impaired Indicates that there is a communication error, but the device can still receive updates.
🔵	Maintenance Mode Indicates that communication between Enterprise Manager and the managed device is disabled.
🟠	Device Replacement Mode Indicates that communication between Enterprise Manager and the managed device is disabled for the purpose of replacing the managed device.
✖	Unreachable 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 network issues.

Table 1.1 *Status icons for managed devices*

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

◆ **Tip**

In addition to viewing the status of your devices, you can also create system alerts to notify individuals in your organization about certain conditions for the devices in your network. This can help you to respond quickly to issues with the managed devices, such as an expired certificate or an unreachable device. You can also configure these alerts to work with any existing network management servers in the network. See ***Overview of alerts****, on page 8-1, for more information.*

Managing 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. Enterprise Manager provides 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 to license or renew a license on as many devices as you need.

Licensing a device

Using the License Device 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.

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.

◆ **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 on the AskF5 Knowledge Base (**http://support.f5.com**) for information about these licensing issues.*

To start a device licensing task

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List Screen opens.
2. Click **New Task**.
   The New Task screen opens
3. For the **Devices** setting, select the **License Device** option.
4. Click **Next**.
   The Device Selection screen opens where you can select devices to include in the licensing task.

To select devices to license

1. From the **Device List**, select an option to specify the types of devices displayed.
2. For **Device Filter**, select an option to further narrow the managed devices displayed.
3. In the Device list area, select the check box next to each device that you want to license.
4. Click **Next**.
   The system retrieves device license information, including the End User License Agreement (EULA) from the F5 licensing server. After the system retrieves license information, the system indicates which devices are ready for licensing by displaying **Success**. Alternately, the message may indicate **EULA required**. If any of the messages in the Details field indicate **EULA required**, then a Review EULAs screen opens.
5. Click **Next**.
   If EULAs are not required, skip to the *To specify task options and start the license task*, on page 1-9.
   Otherwise, accept the EULAs for the devices as described in the following procedure.

◆ **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.

To accept EULAs for devices

The Review EULAs screen presents all available license agreements, and you can switch between these agreements if there is 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, select the check 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.

To specify task options and start the license task

1. On the Task Options page, select an item from each list to specify the task options.
   For information about each option, click the Help tab.

   ***Note**: We recommend that you accept the default option to reboot each device after licensing.*

2. Click **Next**.
   The Task Review screen opens.

3. In the **Task Name** field, type an optional name for the task.

4. Review the task information.

5. To start the task, click **Start Task**.
   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.

   ***Note**: If you want to stop the screen from refreshing, in the **Auto Refresh** box, move your cursor over the countdown timer and click it.*

   When the licensing task is finished, the Task Summary area displays **Complete**.

Using high availability systems

A ***redundant system configuration*** is a pair of F5 Networks systems configured for failover. In a redundant system configuration, 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.

During the device discovery process, Enterprise Manager detects managed devices that are part of a redundant system. The device and its associated peer are displayed on the device properties screen.

Enterprise Manager provides the following basic management for high availability redundant systems.

- Manage a high availability device's failover state
- Synchronize peer configurations

◆ **Note**

*For more information about configuring redundant systems and different configurations of redundant systems such as an active-active configuration, see the **TMOS® Management Guide for BIG-IP® Systems**, or the **WANJet® Appliance Administrator Guide**.*

Managing a high availability 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 view a device's failover state

1. On the Main tab, expand **Enterprise Management**, and click **Devices**.
   The Devices screen opens.
2. Move your cursor over the status icon to the left of a device name.
   A tool tip displays, indicating the details about the device's status.

To change a device's failover state from active to standby

1. On the Main tab, expand **Enterprise Management**, and click **Devices**.
   The Devices screen opens.
2. Click the device name of the device for which want to change the failover state.
   The Device Properties screen opens, displaying the device and the peer state.

3. Click **Switch to Standby Mode** and confirm the change.
   The Device List screen opens, indicating the new state of the device and its peer.

Synchronizing peer configurations

You can remotely synchronize the configurations between managed peer devices in a BIG-IP high availability system. Before doing so, you must first enable the **ConfigSync Auto-Detect** setting on the managed device pair.

To enable ConfigSync auto-detect

1. On the Main tab, expand **Enterprise Management**, and click **Devices**.
   The Devices screen opens.
2. Click on the name of the device for which you want to enable ConfigSync auto-detect.
   The Device Properties screen opens.
3. Below the ConfigSync area, click **Enable Auto-Detect**.
   The Device Properties screen refreshes, and ConfigSync status information appears in the ConfigSync area.

   Note*: The ConfigSync area displays only if the device you selected is configured for high availability.*

To synchronize configurations between peers

1. On the Devices screen, click the name of the device with which you want to synchronize its peer.
   The Device Properties screen opens, displaying the current configuration information in the ConfigSync area.
2. Below the ConfigSync areas, select one of the following options:
   - To copy the current device's configuration to the peer device, click **PUT Configuration**.
   - To copy the peer device's configuration to the current device, click **GET Configuration**.

Collecting information for F5 support

To properly diagnose and address issues with F5 Technical Support, you are typically required to provide basic system and configuration information. Using Enterprise Manager's Support Information wizard, you can easily gather the required information to provide to F5 Technical Support. The Support Information wizard saves you significant time, since you can collect this information centrally, rather than logging on to each individual device to copy configuration files and device information.

Using the Support Information wizard

The Support Information wizard assists 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).

◆ **Important**

To gather support information, you are required to enter a case number. You must initiate a support case with F5 Technical Support and receive a case number before using the following procedure.

To start a support information gathering task

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List Screen opens.
2. Click **New Task**.
   The New Task screen opens
3. For the **Support** setting, enable the **Gather Support Information** option.
4. Click **Next**.
   Continue working through the wizard screens, as described in the following pages, to collect support data.

To specify a case number and notes

In the Step 1 screen, you provide a case number and additional information about the task.

1. In the **Case Number** field, type the case number assigned to the support case.
2. In the **Additional Information** field, type any notes or information that may assist support engineers in diagnosing and solving your support case.
3. Click **Next** to move to the Step 2 of 4 screen.

To add device data

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

1. Click **Add**.
   The Support Information screen opens.

   ***Note**: If required, your Technical Support representative will provide **qkview** parameters values for the support case. To add these parameters, select **Advanced** from the **Add Devices** list to display the **qkview Parameters** field where you can type the information.*

2. Select from the **Device List**, the types of devices you want to view.

3. For **Device Filter**, select an option to further narrow the managed devices displayed.

4. Select the check 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.

To include attachments with the device data

On the Step 2 wizard screen, you can add attachments such as screen shots, error messages, or log files with the support data to send to F5 Technical Support.

1. Above the File Attachments area, click **Attach**.
   The Import Attachment screen opens.

2. In the **File Name** field, type the path and file name of the file, or click **Browse** 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. Click **Next** to move to the Step 3 of 4 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 select an upload destination for the support information. Depending on your selections, the screen may change to prompt you for additional information.

1. From the **Destination** list, select a destination.
    - **F5 Support Site**
      Uses the standard F5 support server and FTP to upload the information to a directory that matches the case number.
    - **F5 Support Site**
      Uses the standard F5 support server and FTP to upload the information to a directory that matches the case number.
    - **Custom Location**
      Allows you to specify a custom FTP server destination, and prompts you for more information.
    - **Local Download**
      Saves the gathered support information in a compressed file on your local client system.

    ***Note**: If you select **Local Download**, you do not need to specify any additional settings.*
2. If you selected **F5 Support Site**, ensure that the email address in the **Email Address** field matches the email associated with the case number assigned to this support case.
3. If you selected **Custom Location**, type the required information in the following fields.
    - **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. Click **Next** to move to the Step 4 of 5 screen.

To send support information

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

1. 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.
2. 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 verify the FTP information and **Email Address**.*

Maintaining and replacing devices

In certain cases, you may need to perform maintenance on a managed device in the network or even replace a device. Before performing these tasks, you can use the Enterprise Manager to switch the device into maintenance mode. ***Maintenance mode*** is a device state in which communications between Enterprise Manager and the managed device are suspended so that you do not receive unnecessary alerts or configure tasks for a managed device that you know is offline.

Enabling or disabling maintenance mode for a 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 communications on the managed device itself. Maintenance mode only disables communication between Enterprise Manager and a managed device.

To enable or disable maintenance mode for a device

1. On the Main tab, 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 Properties screen opens.
3. Below the Device Properties area, click the **Maintenance Mode** button.
   The Maintenance Management screen opens.
4. From the **Mode** list, select one of the following options:
   - **Maintenance Mode**
   - **Maintenance/Replacement Mode Off**
5. In the **Reason** field, type a note to indicate the reason for enabling or disabling maintenance mode.
   This text appears on the Device list and is noted in the Enterprise Manager audit log.
6. Click **Save Changes**.
   The Properties screen opens and the device state changes and the status icon on the screen and on the Device List screen changes to indicate the new state.

Using the device replacement checklist

In certain cases, you may need to replace a managed device. You can use Enterprise Manager's Maintenance/Replacement mode to assist you in tracking the steps required to replace the device.

When you change the state of a device to Replacement mode, the Device Replacement Checklist displays a list of common tasks for replacing a managed device. As you complete the necessary task to successfully replace the device, select the check box next to the task. This list provides you information about the state of all of the replacement tasks and access to each screen required to finish the tasks.

The tasks include the following tasks.

- **Put device into Device Replacement Mode**
  When you replace a device, you must place it into device replacement mode so that Enterprise Manager does not attempt to perform management tasks.

- **Create a 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**
  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**
  When you later restore the UCS archive to the new device, setting the host name restores the additional general properties (such as IP address, time zone, and HA settings).

- **Licensing**
  Your licensing options depend on the type of replacement that you are performing and consist of the following.

  - **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)
Restore the UCS archive that you archived earlier to ensure that the device configuration matches the device that you replaced.

◆ **Exit device replacement mode**
Click the **Exit device replacement mode** link to set the device to active mode and open the device properties screen.

2

User Roles and Authentication

- Managing user roles and authentication

Managing user roles and authentication

The User list displays all users who have and their privileges to manage devices in your network. Each managed device authenticates the stored user names. You can add new users and assign roles from the same User List screen.

◆ **WARNING**

When you add users, you must use the same administrator-level user name that you currently use for managing BIG-IP systems 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 screen.

Adding new users

To add a new user

1. On the Main tab, expand **System** and click **Users**.
   The Users list screen opens.
2. Click **Create**.
   The New User screen opens.
3. In the **User Name** field, type the administrative-level user name that you are currently using to manage BIG-IP systems in your network.
4. For **Password**, in the **New** and **Confirm** fields, type the password for the user and confirm the password.
5. From the **Role** list, select **Administrator**, **Operator**, or **Application Editor**.

   Note: *If you select another user role, managed devices cannot authorize the user to perform management tasks, and the user cannot initiate tasks using the Enterprise Manager system.*
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. To allow the user to access the Enterprise Manager from the command line, from the **Terminal Access** list, select **Enabled**.
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** fields.
9. Click the **Finished** button to return to the user list, or click **Repeat** to add another use.

Modifying user accounts

To modify a user account

You update user passwords and permissions from the User Account Properties screen.

1. On the Main tab, 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. Perform one or more of the following tasks:
   a) To change the user password:
      For **Password**, in the **New** and **Confirm** fields, type the new password for the user.

   b) To change the user role:
      From the **Role** list, select **Administrator** or **Operator**.

   c) 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** setting indicates this user's current partition access.

   d) To allow the user access to the command console:
      From the **Terminal Access** list, select **Enabled** to permit the user to access the Enterprise Manager device from the command line.
4. Click **Update** to save the changes to the user account properties.

Modifying user authentication source

By default, Enterprise Manager uses a local database to authenticate users. Enterprise Manager maintains a local authentication list of users, but you can choose to use a remote LDAP, Active Directory, RADIUS, or TACACS+ authentication source.

If you use a remote authentication source, you should configure Enterprise Manager to use your remote database.

To specify an authentication source for a user

1. On the Main tab, expand **System** and click **Users**.
   The Users list screen opens.
2. On the menu bar, click **Authentication**.
   The Authentication Source screen opens.
3. Below the Authentication area, click **Change**.
   The **User Directory** field changes to a list.

4. From the **User Directory** list, select the type of remote source to use to authenticate users:

   - **Active Directory**
   - **LDAP**
   - **RADIUS**
   - **TACACS+**

   The screen displays additional settings, specific to the remote authentication source you selected.

5. In the Authentication area, specify the configuration settings for the remote authentication server.
   See the online help for detailed information about the Authentication area.

6. Click **Finished** to save your changes.

Modifying configuration comparison settings

When you perform an archive comparison task, Enterprise Manager compares certain configuration files by default.

◆ **Note**

For information about the archive comparison task, see ***Comparing multiple versions of archives****, on page 3-9.*

To modify configuration file comparison settings

1. On the Main tab, expand **Enterprise Management**, click **Options**, and select **Archives**.
   The Archives option screen opens.

2. Modify the **Files to Compare** list, as required:

   - To add a configuration file to compare, in the **File Name** field, type the path and file name of the configuration file, and click **Add**.
   - To remove a configuration file from the comparison list, click the file name then click **Remove**.
   - To reset the list to the default, click **Restore Default Values**.

3. Click **Save Changes**.

3

Managing UCS Archives

- Maintaining rotating archives for managed devices
- Retaining specific configuration archives
- Restoring UCS archives for managed devices
- Modifying or deleting configuration archives
- Comparing multiple versions of archives
- Searching for specific configuration elements
- Managing Enterprise Manager archives

Maintaining rotating archives for managed devices

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. This means that you always have a secure location to store device configuration archives for all your managed devices.

The advantage of scheduling rotating archives is that if 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's configuration changes. Thus, you do not unnecessarily save any duplicate configuration archives, and you always have one or more archives of recent configurations from which you can restore the configuration. In a rotating archive schedule, Enterprise Manager saves multiple archives and cycles out old archives as it creates new ones.

By default, Enterprise Manager stores up to 10 rotating device archives and 10 saved, or ***pinned***, archives per device in its database. Enterprise Manager automatically rotates archives in a first in, first out manner. That is, once the database reaches the maximum number or archives, Enterprise Manager deletes the oldest archive in the rotating archive list. Conversely, you must manually delete pinned archives.

If you attempt to create a pinned archive that exceeds the limit, the system warns you that it cannot create a new pinned archive until you delete at least one from the current list, or increase the maximum limit.

Changing default archive options

If you want to maintain more device configuration for backup and restore flexibility, you can increase this maximum limit as needed, but the number of stored archives can affect the disk space on the Enterprise Manager device.

◆ **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.

To change the default archive storage options

1. On the Main tab, expand **Enterprise Management**, and click **Options**, and **Archives**.
   The Archive Schedule screen opens.
2. Change the maximum number of archives that Enterprise Manager saves in its database, in the **Maximum Rotating Archives** field or the **Maximum Pinned Archives** field.
3. Click **Save Changes**.

Creating rotating archive schedules

After you add devices to the Device List screen, you can set up a rotating archive schedule. You can create a customized archive schedule for a specific device, or create several archive schedules and assign any number of devices to each schedule.

To create a rotating archive schedule

1. On the Main tab, expand **Enterprise Management,** and click **Tasks**, **Schedules**, and **Archive Collection**.
2. Click the **Create** button.
   The New Scheduled Task screen opens.
3. In the **Archive File Name** field, type a name for the rotating archive schedule.
   This name appears in the Archive Collection list.
4. From the **Check for Changes** list, select the frequency that you want Enterprise Manager to check managed device configurations.
   The screen refreshes to display additional options.
5. Specify a day of the week, month, and time of day that you want Enterprise Manager to check for device configuration changes.
6. From the **Private Keys** list, select whether you want to include or exclude private SSL keys in the rotating archive.
7. From the **Status** list, select whether you want to enable or disable the rotating archive schedule after you create it.
8. For the **Devices** or **Device Lists** setting, in the **Available** list, select a device or device list.
9. Click the Move button (<<) to move the selected devices or from the **Available** list to the **Assigned** list.
10. When you finish adding devices or device lists to the **Assigned** list, click **Finished**.
    The Archive Collection list screen opens and the new rotating archive schedule appears in the list.

Now, whenever a device configuration in the **Assigned** list changes during the interval you specified, Enterprise Manager creates an archive of the device's configuration and adds it to the rotating archives on the Archives Collection screen.

Modifying rotating archive schedules

After you create a rotating archive schedule and add devices, you can modify elements of the schedule, including the interval and its enabled state. You can then make these changes affect all the devices subscribed to that schedule. Additionally, you can manage individual device to a particular schedule.

To modify a rotating archive schedule

1. On the Main tab, expand **Enterprise Management,** and click **Tasks**, and then **Schedules**.
   The Rotating Archives list screen opens.

2. In the list, click the name of the schedule you want to modify.
   The Scheduled Task Properties screen opens.

3. To change the archive interval, in the **Configuration Check** field, select how often you want Enterprise Manager to check managed device configurations.
   The screen refreshes to provide options for the frequency you selected.

4. Specify a day of the week, month, and time of day that you want Enterprise Manager to check for changes to device configurations.

5. In the **Private Keys** list, select an option to include or exclude the private SSL keys in the rotating archive.

6. In the **Status** list, select an option to specify the state of the rotating archive schedule:

   - **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. To add devices to this rotating archive schedule:

   a) In the Device Assignments area, for the **Devices** setting, in the **Available** list, select a device.

   b) Click the Move button (**<<**) to move the selected devices from the **Available** to the **Assigned** list.

8. To remove devices from this rotating archive schedule:

   a) In the Device Assignments area, for the **Devices** setting, in the **Assigned** list, select a device.

   b) Click the Move button (**>>**) to move the selected devices from the **Assigned** to the **Available** list.

9. Click **Save Changes**.

Retaining specific 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.

Creating pinned 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.

To create a new pinned archive

1. On the Main tab, 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 Archives screen opens.
4. Click the **Create Pinned Archive** button.
   The New Archive screen opens.
5. In the **File Name** field, type the file name of the new archive that you want to create.
6. In the **Description** field, type a note that you want to appear in the Pinned Archives area next to the archive file name.
7. From the **Private Keys** list, select an option to include or exclude the private SSL keys in the rotating archive.
8. Click **Create**.
   Enterprise Manager creates a UCS archive of the current device and the archive displays when the Device Archive screen opens.

To pin an existing configuration archive

1. On the Main tab, 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 area, select the check box next to the archive name(s) for which you want to create a pinned archive.
5. Click **Pin Archive**.
   The archive status changes to **Pinned** and displays until you delete it.

Restoring UCS archives for managed devices

You can use Enterprise Manager to restore a UCS archive on any managed device. This saves you time because you can restore the configuration for all of your devices from Enterprise Manager, without having to log on to each individual device.

◆ **WARNING**

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

To perform a basic UCS restoration for a device

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

2. Click the name of the device for which you want to restore an archive.
   The Device Properties screen opens.

3. On the menu bar, click **Archives**.
   The Device Archives screen opens.

4. 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**.

◆ **Important**

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

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 configuration archives

1. On the Main tab, 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 area, select the check box for the archive(s) that you want to delete.
5. Click **Delete**.

To modify an archive description

1. On the Main tab, 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 area, click the name of the archive for which you want to modify the description.
   The Archive Properties screen opens.
5. In the **Description** field, type the new description.
6. Click **Save Changes**.

Comparing multiple versions of archives

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

You can use the Compare Device Configurations wizard to assist you in configuring an archive comparison task to compare either the current configuration to an archive, or compare two stored UCS archives.

◆ **Note**

Configuration files may vary by managed device, or licensed features.

Comparing device configurations using the wizard involves two main procedures.

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

Starting an archive comparison task

The Compare Archive wizard works in a fashion similar to other wizards in Enterprise Manager.

To start an archive comparison task

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List Screen opens.
2. Click **New Task**.
   The New Task screen opens.
3. For **Configuration Archives** setting, select **Compare Archive**.
4. Click **Next**.

To select a device and comparison option

1. From the **Device** list, select the managed device for which you want to compare device configurations.
2. From the **Comparison** list, select one of the following options:
   - **Current configuration to an archive**
     Compare the current configuration of the device you selected in the **Device** box to one of the archived configurations listed in the Configuration archives area.

- **Two configuration archives**
  Compare two archived configurations.

3. Based on the **Comparison** option you selected in the previous step, select the configurations you want to compare.
   - If you are comparing the current configuration to an archive, in the Configuration Archives area, select the button next to the archived configuration that you want to compare.
   - If you are comparing two archived configurations, in the Configuration Archives area, select the check boxes next to the two archives that you want to compare.
4. Click **Next** to move to the Step 3 of 3 screen.

To review and initiate the comparison task

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

1. To change the task name, in the **Task Name** field, type a new name. This name appears in the task list while the task is running, and after the task finishes.
2. Review the information in the Task Summary area.
3. To make changes, click **Back** and navigate to the screen that contains the options you want to change
4. To start the task, click **Start Task**.
   The Task Properties screen opens, displaying details relevant to the task that you configured, as well as task progress.

Comparing archive files

The Task Properties screen provides a summary of the task, where you can view differences between configuration files. 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, 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 area, 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**

If ***File Not Found*** *displays in the Comparison column, it indicates that the system did not detect the file at the specified location, or the file does not exist. Check the path and file name if you did not expect this message.*

Searching for specific configuration elements

You can use the Configuration Search feature to search all available configuration files on a managed device for specific elements. This can help you find and view particular objects or settings for any managed device in your network.

◆ **Tip**

*When you use the following procedure to search every managed device's configuration for a specific element, remember that you filter your options only after all matching objects are found. Thus, the search time may be lengthy if you are managing a large number of devices. To decrease the search time, you can limit it to only a specific device or set of configuration files. You do this by typing a character string in the **Matching Objects** filter field above the Matching Objects list before typing a word in the **Keyword** field. Then, when you click the **Search** button, the system looks at only the configuration files listed in the Matching Objects list.*

To search device configurations

1. On the Main tab, expand **Enterprise Management**, and click **Configurations**.
   The Search Configuration screen opens.
2. In the **Keyword** field, 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 area changes to display configuration files that contain instances that match the string you typed in the **Keyword** field.
4. In the **Matching Objects** filter field, 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 area.
6. To clear the configuration file list, click **Reset**.

Managing Enterprise Manager archives

An Enterprise Manager UCS archive contains the managed BIG-IP system UCS archive, as well as additional information about managed devices in an Enterprise Manager system, including:

- Device properties information
- Device certificates
- Custom alerts
- Certificate lists
- History information such as the task list and alert history list
- Rotating archive schedules

These UCS archive files are mandatory to restore a configuration, therefore, it is important that you create and securely store UCS archives. To easily manage these files, you can configure Enterprise Manager to create UCS archives at scheduled intervals, with the option of storing any archive indefinitely.

Creating configuration archives

You have two main options for creating a UCS archive.

- ◆ **Basic**
  A basic UCS archive contains configuration data specific to a device. To create a basic UCS archive, you 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 *Maintaining rotating archives for managed devices*, on page 3-1, for more information about rotating archive schedules.

- ◆ **Advanced**
  An advanced UCS archive includes the device configuration information as well as all imported data, including UCS information, and managed device UCS archives.

  See *To create an advanced UCS Enterprise Manager archive*, following.

◆ **Important**

Because creating an advanced UCS archive may involve a large amount of data, verify first that you have adequate disk space available on the Enterprise Manager system and that there are no tasks currently running.

To create an advanced UCS Enterprise Manager archive

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

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

   The **em-backup** script begins 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 for safe storage.

◆ **Note**

The ***em-backup*** *script may take several minutes to complete, depending on the number of UCS archives that are stored on the Enterprise Manager system.*

Restoring configuration archives

You have two main options for restoring an Enterprise Manager UCS archive.

- **Basic**
  A basic UCS restoration re-establishes all Enterprise Manager configuration information for managed devices, including certificate information, and custom alerts.
- **Advanced**
  An advanced UCS restoration includes all of the basic Enterprise Manager configuration data in addition to imported data, such as managed device UCS archives.

To perform a basic UCS restoration for Enterprise Manager

1. On the Main tab, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. Click the name of the device for which you want to restore an archive.
   The Device Properties screen opens.
3. On the menu bar, click **Archives**.
   The Device Archives screen opens.
4. 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**.

To perform an advanced UCS restoration for Enterprise Manager

To perform the following procedure, you must have **root** access to the command line. You can only perform the following procedure on an advanced device configuration file created using the **em-backup** script.

1. Log in as **root** at the command line of the Enterprise Manager system that you want to restore.
2. Copy the advanced Enterprise Manager UCS archive that you created with the **em-backup** script to the Enterprise Manager system that you want to restore.
3. At the command prompt, type the following command, where **<archive_name>** is the path and file name for the archive file, and press Enter.

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

   The **em-restore** script begins the process of restoring all configuration and imported data stored on the Enterprise Manager system.
4. When the process completes, delete the **<archive_name>.ucs** file from the target system, and reboot the device.

4

Using Templates and Changesets to Manage Device Configurations

- Overview of templates and changesets
- Overview of network objects and dependencies
- Managing template variables
- Using a standard template
- Creating a custom template
- Importing and exporting templates
- Creating a changeset
- Modifying a changeset
- Verifying and deploying staged changesets
- Viewing device configurations

Overview of templates and changesets

Enterprise Manager™ offers two versatile options that you can use to simultaneously manage multiple device configurations: templates and changesets.

A ***template*** is a tool that you use to create and deploy new configurations based on an existing device configuration. You use a template as a model, changing template variables to modify elements that are specific to the new (targeted) device. 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 template variable. Then, edit the allowed values for the variable to include all the necessary times zones.

A ***changeset*** is a collection of user-defined configuration data that you create and save for any managed device in your network and distribute to other managed devices. For example, when you configure a BIG-IP® system, you typically specify certain profiles, monitors, and iRules®. To set up these systems individually, you must keep track of each setting, and manually enter those values for every new device that you add to the network. However, if you use changesets, you can deploy the same profiles, monitors, and iRules® configurations from one device to as many devices as needed.

Templates offer you the ability to set variables for different devices in the network, so you can use templates in conjunction with changesets to help manage common network configuration tasks. Since these options are somewhat inter-related, it helps to have a basic understanding of the elements associated with each.

Although changesets and templates each represent a collection of configuration files that you can use to manage device configurations, they differ in three primary ways, as outlined in the following table.

Changesets	Templates
Used to manage a single set of configuration data.	Used to manage elements of configuration data that vary from device to device.
Used to deploy configuration data to devices, without changing any values of the configuration.	Used to stage a configuration that is customized for multiple devices, using device-specific variables.
Used for a wide variety of tasks, including setting up a device, maintaining consistent configurations on multiple devices, and creating new applications.	Used primarily to stage individualized configuration changes for multiple devices.

Table 4.1 *Primary differences between changesets and templates*

Performing device configuration management tasks

The flexibility of templates and changesets helps you to efficiently manage the following tasks.

- **Deploy common configurations to new devices**
  When you add a new device to your network, you can deploy common configuration elements from a prototypical device to the new device. You can change certain settings or variables specific to the new, targeted device.
- **Manage configuration standards across multiple devices**
  If there is a change in a standard configuration element for your network, you can modify it on one managed device, then deploy that modification to other managed devices.
- **Roll out new applications**
  You can deploy new application settings to as many devices as needed, reducing the time it takes to perform application installation when managing multiple BIG-IP systems.
- **Audit configuration changes**
  Enterprise Manager tracks in its database, any configuration changes you make to a device using templates or changesets. This can assist you in auditing changes later.
- **Manage network object dependencies**
  Using templates and changesets, you can automatically manage dependencies for network objects.

Overview of network objects and dependencies

When creating a template or changeset, you can include any type of available object class. An ***object class*** is the general type of network object that you want to include in the template. For example, a BIG-IP virtual server named **www_server_one** belongs to the Local Traffic / Virtual Servers object class, and the **named.conf** file belongs to the System / BIND object class. The available object classes vary depending on the managed device and its licensed features. Enterprise Manager displays any associated network dependencies for objects.

In general for object classes, the last part of the class name is indicative of the object type. 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. In contrast, for system classes, the class name does not clearly indicate which object is affected. Table 4.2 outlines the system class names and their related objects or settings.

System Class Name	Related Object
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 4.2 *System classes and related objects*

Starting with version 9.4.3, BIG-IP systems use a different method of managing configuration files, and only the **named.conf**, **main.cf**, and **master.cf** objects noted in Table 4.2 appear in changesets. To view configuration settings and confirm compatibility with **bigpipe** commands, see *Viewing device configurations*, on page 4-29.

For more information about object classes, see the ***Configuration Guide for BIG-IP® Local Traffic Manager***™, and for information about **bigpipe** commands, see the ***Bigpipe Utility Reference Guide***. Documentation is available from the AskF5® support site (**http://support.f5.com**).

Honoring network object dependencies

To successfully copy a network object from one BIG-IP® system to another using changesets and templates, you must honor the network object's dependencies 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, you usually need to also define dependent objects or resources, such as pools, nodes, or profiles.

The presence of dependencies adds a level of complexity to the process of storing and copying device configurations. 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. However, when you use templates and changesets, Enterprise Manager automatically manages these dependencies.

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 focus of the configuration change. When you deploy a template 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.

Reviewing network object elements

You typically use the Template and Changeset wizards to create a template or changeset. These wizards prompt you for the information required and automatically generate the proper syntax.

The configuration syntax for changesets and templates consists of the following elements.

- Object classes
- System classes
- Unclassified objects
- Administrative partitions
- Object settings

Once you create a template or changeset, you can review the text version. The network object elements and text syntax are defined as follows.

About object classes

Every network object in a template or changeset must have a class directive. For example, if you include pools, Enterprise Manager includes the class path as follows:

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

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

About system classes

Any system settings contained in a configuration must specify a system class directive. For example, if you include DNS settings in a template or changeset, Enterprise Manager includes the system class path as follows:

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

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

About unnamed objects

Certain objects included in a changeset or template require additional information. For example, classes containing SSL certificate data require that you specify the object within the class directive, and if you include SSL certificates and SSL keys, you must specify the name of the target files. Enterprise Manager copies the object data with these directives to the sample.crt and sample.key files on the target device, respectively, as in the following example.

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

Working with administrative partitions

If a managed device supports administrative partitions, Enterprise Manager also includes object partition information in the template or changeset text. If you include an object targeted to a specific partition, the system precedes the object class directive with the following text, where **target_partition** is the name of the partition on the target device. For example:

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

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

Including object settings

All class paths in a template or changeset must include the object configuration setting. For example, for a changeset that includes the virtual server **MyVIP**, which references its pool, **MyPool**, Enterprise Manager would include the following syntax:

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

Once you deploy the template or changeset, the target devices you selected contain the local traffic objects **MyVIP** and **MyPool**.

Managing template variables

While changesets require that you manage network object dependencies, templates use variables to manage device configurations. ***Template variables*** are unique values or settings specific to each managed device. Variables can be virtual server names, node addresses, port information, and so forth.

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.

Because a template is essentially a guideline for a configuration change that you can apply to multiple devices, variables are specific to each device.

Reviewing template variables

When you create a template with variables, you can modify template variable elements before you save the template. Additionally, you can view and modify these settings by clicking **Manage Variables** on a Template Properties screen.

There are six main variable elements.

- **Variable Name**
  Usually, the system chooses a variable name but, in some cases, you can specify the name for a variable. The variable name appears in the template configuration text and staged changeset if you do not specify a variable description.
- **Default Value**
  The system uses the default value for a variable when you deploy a changeset based on this template you created.
- **Description**
  Because only the variable name is visible in the template text, and is usually system-assigned, we recommend that you provide a variable description. This description allows you and others to properly apply the variable when you stage or deploy a changeset based on this template.
- **Editable**
  As an Administrator-level user, you can specify whether a user can change a variable when they use this template to stage a changeset.
- **Visible**
  If you restrict a user’s ability to edit the value of a variable, you can also hide the variable setting from restricted users when they use the template to stage a changeset.
- **Edit Allowed Values**
  As an Administrator-level user, you can also specify the allowed values for the template. Then any user staging a changeset with this template selects from a list of values, which can prevent errors.

Reviewing template variable syntax

When you create a custom template, you typically use the Template wizard to construct the template from network objects on a managed device. The wizard prompts you for the necessary information, and automatically generates the proper text syntax. Once the template is created, you can add additional variables to the template text as required, using the following format, where **<variable_name>** is the name of the variable in the network object.

```
@define <variable_name>
```

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

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

In this example:

- The first line specifies the variable **@node_ip** after the variable flag **@define**. The **@define** text flags the line as a variable, and prompts the system to replace the variable with a value when you deploy the template.
- 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**.

Although the leading *at* symbol (@) is not required for variables names, the Enterprise Manager uses it to distinguish a variable from static configuration information. The *at* symbol can also help you easily identify variables when you read the configuration text.

◆ **Note**

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

Using a standard template

Enterprise Manager ships with the following templates that you can use for standard configuration 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)
tm_node_enable	Enables a local traffic server address (all pools)
ltm_node_disable	Disables local traffic server address (for all pools, only allowing established connections)
ltm_node_down	Sets a local traffic server address to **down** (for all pools, allowing no new connections)

Table 4.3 *Standard templates and descriptions*

◆ **Tip**

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 template, changeset, or staged changeset.

To view standard template properties

1. On the Main tab, expand **Enterprise Management**, click **Configurations** and select **Template List**.
2. Click the name of the template you want to view.
3. The Template Properties screen opens.

Creating a custom template

Creating a custom template using the Template wizard involves the following tasks:

- Selecting a source
- Selecting an object class
- Selecting an object instance
- Reviewing and managing dependencies for objects
- Reviewing template properties

By default, only Administrator-level users can create templates, which can be based on a device or any existing template, except standard templates. Alternatively, they can select text as a source and manually type the configuration, or copy the text of a configuration and paste it, into the Text field. Administrators can also delegate, to the Operator or Application Editor roles, the ability to use published templates. (For more information about managing user role permissions, see *Managing user permissions*, on page 3-18.)

To select a source for a template

1. On the Main tab, expand **Enterprise Management**, and click **Task List**.
2. Click the **New Task** button.
3. For the **Configuration** setting, select **Create Template**.
4. Click the **Next** button.
   The New Template screen opens.
5. In the **Name** field, type a name for the template. This name later appears on the template list.
6. In the **Description** field, type a description for the template.
7. From the **Source** list, select a source on which you want to base the template. The subsequent Template wizard screens vary, depending on the source you use.
   - If you selected **Device**, then from 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.
8. Click **Next**.
   The Class Selection screen opens.

To select object types for a template

When you select a template or device as a source for the custom template, you must select an object class. An object class is the general type of network object that you want to include in the template. You select object classes from the Step 2 screen of the New Template wizard.

1. In the **Object List** setting, select a class from the **Available** list, then click the Move button (<<) to move it to the **Selected** box.
2. Repeat step 1 as necessary to add additional classes, and then click **Next**.
   The Object Selection screen opens.

To select object instance for a template

For each class you select, you must also select an associated object instance. An ***object instance*** is the specific network object you want to include in the template. You select object instances from Step 3 screen of the New Template wizard.

1. In the **Object Type** setting, select an object from the **Available** list, then click the Move button (<<) to move it to the **Selected** box.
2. Repeat step 1 as necessary to add additional objects, and then click **Next**.
   The Template Summary screen opens.

To review and manage network dependency options for a template

You can configure Enterprise Manager to automatically include dependent objects for selected object classes, or you can choose not to include them, and type them in manually on the target device when you deploy the changeset based on this template. You manage network dependency options from Step 4 screen of the New Template wizard.

1. From the **Dependency Handling** list, select one of the following options:
   - **Include resource objects**
   - **Skip resource objects**
2. To view details for an object, click the name of an object in the **User Selected Objects** setting.
   Details about that object appear below the list in several fields, some of which you can edit.
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 for an associated resource object, click the name of an object in the **Resource Objects** list.
   Details about that object appear below the list.

5. Click **Next**.
   The Template Properties screen opens, where you can view the template properties you configured.

To review and modify template properties for a template

You can view and modify the new template you created on the Step 5 screen of the New Template wizard.

1. To modify the contents of the template, select **Advanced** from the **Template Text** list. The screen displays the **Add Path** and **Search and Replace** buttons.
2. To add a new class:
   a) From the **Object Type** list, select an object type.
   b) Click **Add Type**.
      The system generates the proper syntax for the class path, and adds it to the Text field.
3. To find and replace a value:
   a) In the **Search For** field, type an existing value.
      You can type a user-specified value such as an IP address or object name. This value is case-sensitive.
   b) In the **Replace With** field, type a new value.
   c) Click **Search and Replace**.
      The system searches through the data in the **Text** field and prompts you to confirm any changes, if found.
4. After you review or change information, click **Next**.
   The Template Variables Properties screen opens.

To review and modify template variable properties for a template

From the Step 6 screen of the New Template wizard, review and edit the template variable values as required, and click **Finish**. The Template List screen opens, displaying the template you created.

For information about template variables, see *Managing template variables*, on page 4-9.

To publish a template so that it is available for others to use, see *Publishing templates*, on page 4-15.

Publishing templates

When you create a custom template, it is available only for you to deploy and use. To make the template available for others, you must publish it. 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.

To publish a template

1. On the Main tab, expand **Enterprise Management**, click **Configurations**, and select **Templates**.
   The Templates list screen opens.

2. Click the name of the template you want to publish.
   The General Properties screen opens.

3. Select the **Published** check box.

4. Click the **Save Changes** button.
   The template is now available for others to use as a source.

Importing and exporting templates

Templates are a flexible method 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**) by importing and exporting them.

◆ **Note**

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.

You can import a template from DevCentral by copying and pasting text from the site to the **Text** field 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.

To import template text from DevCentral

1. Log on to the DevCentral site, **http://devcentral.f5.com** using your account information.
2. Click the **Samples** link at the top of the screen.
   The Samples screen opens, displaying the latest contributions to the CodeShare pages.
3. Click the **Advanced Design & Config** link.
   The Advanced Design & Config CodeShare screen opens, listing all sample code available in this category.
4. 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.
5. In the Template Text section, highlight the template text.
6. Copy the text. (From the browser's Edit menu choose Copy, or press Ctrl + C).
7. Log on to Enterprise Manager.
8. On the Main tab, expand **Enterprise Management**, and click **Templates**.
   The Templates list opens.
9. Above the template list, click **Create**.
   The New Template screen opens.
10. In the **Name** and **Description** fields, type an appropriate name and description for the new template.

11. For the **Source** setting, select **Text**.
12. Click **Next** to move to the Template Properties screen.
13. In the **Text** field, 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 area above the **Text** field.*
14. Click **Next** to move to the Template Variable Properties screen.
15. After you configure variables for the template, click **Finish**.

For detailed information see *Creating a custom template*, on page 4-12.

To export 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, expand **Enterprise Management**, **Configurations**, and select **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** field, 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** field to create a new template, or you can submit it for inclusion on the DevCentral CodeShare site.

Creating a changeset

To create a changeset, we recommend that you use the Changeset wizard, which automatically locates dependencies for each network object included in the changeset. Additionally, the Changeset wizard writes all of the syntax required to correctly classify network objects and system settings in the changeset configuration file. This process ensures that you can successfully deploy the changeset to other managed devices.

Creating a changeset using the Changeset wizard involves the following tasks:

- Selecting a source
- Reviewing dependencies for objects

Enterprise Manager stores changeset information in text form, ensuring compatibility with configuration files on a managed device. You can verify the compatibility of the changeset with managed devices in the network, then deploy it to those devices. This gives you better control over device configurations in your network.

By default, only Administrator-level users can create changesets. Administrators can delegate, to the Operator or Application Editor roles, the ability to stage a changeset using published templates.

Selecting a changeset source

The first step in creating a changeset is selecting a source.

To select a source for a changeset

1. On the Main tab, expand **Enterprise Management**, **Tasks**, and click **New Task**.
2. In the Configurations section, select **Create Changeset**.
   The New Changeset Step 1 screen opens.
3. In the **Name** field, type a name for the changeset.
   This name later appears on the changeset list.
4. In the **Description** field, type a description for the changeset.
5. From the **Source** list, select a source on which you want to base the changeset.
   The subsequent screens vary, depending on the source you use.
   - If you selected **Device**, skip to *Using a device as a changeset source*, on page 4-19.
   - If you selected **Template**, click **Next**, and then skip to, *Using a template as a changeset source*, on page 4-20.
   - If you selected **Text**, click **Next**, and then skip to, *Using text as a changeset source*, on page 4-19.

Using a device as a changeset source

When you select a managed device as the source for a changeset, you specify the device and the partition from which you want to copy some or all of its device configuration. Administrative partitions are logical containers with a defined set of BIG-IP system objects, and are used for access control purposes.

◆ **Important**

Administrative partitions are supported on BIG-IP software version 9.4.x and later. If you are working with changesets on a device that does not support administrative partitions, select ***Common*** *for the partition.* ***Common*** *includes all partitionable BIG-IP system objects.*

To use a device as a changeset source

If you selected device for the changeset source, perform the following tasks from the Step 1 screen of the New Changeset wizard, for each class you want to add.

1. From the **Device** list, select the device from which you want to copy objects.
2. From the **Partition** list, select the partition from which you want to copy objects and click **Next**.
   The Step 2 screen of the New Changeset wizard opens.
3. For the **Object Type List** setting, select a class from the **Available** list, then click the Move button (<<) to move it to the **Selected** box.
4. Click **Next** when you have finished adding classes.
   The Step 3 screen of the New Changeset wizard opens.
5. For the **Object List** setting, select an object from the **Available** list, then click the Move button (<<) to move it to the **Selected** box.
6. Click **Next** when you have finished adding objects.
   The Step 4 screen of the New Changeset wizard opens.
7. Review the selected objects and click **Next**.
   The Step 5 screen of the New Changeset wizard opens. Skip to *Reviewing object dependencies for a changeset*, on page 4-21.

Using text as a changeset source

Creating a text-based changeset requires fewer steps in the wizard, however, the text must be accurate. Unlike when you use a device or template as a source, Enterprise Manager does not automatically manage dependencies and variable information when you use this option.

The text version of a changeset appears 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.

For further information about the requirements for using text as a changeset source, see *Reviewing network object elements*, on page 4-6.

To use text as a changeset source

You specify the text for a changeset on the Step 1 screen of the New Changeset wizard.

1. From the **Select Object Type** list, select a network object class, and click **Add Type** for each object class you want to add.
   The object type appears in the **Text** field.

   ***Note**: Alternatively, you can type the object classes and associated information directly into the **Text** field.*

2. In the **Text** field, type the configuration information associated with the object types you added.
3. Click **Finished** to save the new changeset.

Using a template as a changeset source

When you select a template as a changeset source, you can view the template and add new variables as required. For specific information about template variables, see *Managing template variables*, on page 4-9.

To use a template as a changeset source

If you selected template as the changeset source, perform the following tasks from the Step 1 screen of the New Changeset wizard.

1. Click the button next to a template name and click **Next**.
   The Step 2 screen of the New Changeset wizard opens.
2. Review the variable values.
3. To modify the value of an editable template variable, in the Value column adjacent to a variable name, type a new value or select a value from the value list.
4. Click **Next**.
   The Text of Changeset screen opens. Skip forward to *Reviewing object dependencies for a changeset*, on page 4-21.

Reviewing object dependencies for a changeset

If you used a device as a changeset source, you must define how to handle network object dependencies.

To review and manage dependency options for a changeset

You review and manage network object dependencies on the Step 5 screen of the New Changeset wizard.

1. From the **Dependency Handling** list, select one of the following options:
   - **Include resource objects**
   - **Skip resource objects**
2. To view details about an object, click the name of an object in the **User Selected Object** box.
   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 about an object, click the name of an object in the **Resource Objects** list.
   Details about that object appear below the list.
5. Click **Next**.
   The Text of Changeset screen opens, where you can view the changeset you configured.

Reviewing and modifying changeset properties

After you have configured a changeset, you can review the text for the changeset, make any necessary alterations, and then save it.

To review and modify a changeset

1. To modify the contents of the changeset, select **Advanced** from the **Text of Changeset** list.
   The screen displays the **Add Type** and **Search and Replace** buttons.
2. To add a new class:

   a) From the **Select Object Type** list, select a new class path.

   b) Click **Add Type**.
   The system generates the proper syntax for the class path, and adds it to the **Text** field.

3. To find and replace a value:

   a) In the **Search For** field, type an existing value. You can type a user-specified value such as an IP address or object name. This value is case-sensitive.

   b) In the **Replace With** field, type a new value.

   c) Click **Search and Replace**.
   The system searches through the data in the **Text** field and prompts you to confirm any changes, if found.

4. After you review or change information, click **Finish**.
   The Changeset List screen opens, displaying the changeset you created.

Modifying a changeset

When you create a changeset, Enterprise Manager stores the changeset as text that represents the objects and dependencies you selected. You can change any details of the changeset for an object, such as dependencies, IP address, and so forth, at any time.

To modify a changeset, you manually edit the text of the changeset from the Changeset Properties screen.

To modify a changeset

1. On the Main tab, expand **Enterprise Management**, click **Configuration**, and select **Changeset List**.
   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** field, type a new description.
   - To add objects to the changeset, in the **Object Class** 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** field.
4. Click **Save Changes** to save the modified changeset.

Verifying and deploying staged changesets

Depending on your user role privileges, you can immediately verify or deploy an existing staged changeset. We recommend that you verify a staged changeset prior to deploying it to ensure that it works properly on the target device.

Selecting a method to verify a staged changeset

Using Enterprise Manager, you can store configuration information in changesets or templates, and deploy it to one or more BIG-IP systems in your network through staged changesets. A ***staged changeset*** is a configuration change in a staged state where a user can verify and approve it prior to deployment.

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

You can verify a staged changeset using either of the following methods:

- **Using the Staged Changeset wizard**
  You can verify the changeset from screen 3 of the Staged Changeset wizard. See *Verifying a staged changeset using the Staged Changeset wizard*, following.
- **Using the Deploy Changeset wizard**
  To verify one or more staged changesets, you can use the Deploy Changeset wizard. See *Verifying staged changesets using the Deploy Staged Changeset wizard*, on page 4-25.

◆ **Tip**

If you specify that a template you create requires verification, then you must verify all staged changesets based on that template. Therefore, the ***Deploy*** *button appears only after you verify the staged changeset.*

Verifying a staged changeset using 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 using the Staged Changeset wizard

1. On the Staged Changeset Properties screen (Step 3 of 3 in the 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, and indicates whether the staged changeset verification is successful on all target devices.

2. Once the process quits running, click **Finished** to return to the Staged Changeset Properties screen.

Verifying staged changesets using the Deploy Staged Changeset wizard

To verify one or more staged changesets, you can use the Verify Staged Changeset wizard. When you complete the task, you can immediately deploy the staged changeset.

To select one or more staged changesets to verify

1. On the Main tab, expand **Enterprise Management**, click Configurations, and select **Staged Changeset List**.
   The Staged Changeset screen opens.
2. Select the check box next to each staged changeset that you want to verify.
3. Click **Verify** or **Deploy**.
   The Deploy Staged Changeset wizard screen opens.
4. From the **Error Behavior** list, select an option:
   - **Continue task on remaining devices:** The system continues to verify staged changesets for devices on which an error was not encountered, until the task finishes.
   - **Cancel task on remaining devices:** The system immediately stops the verification task if it encounters an error or an invalid staged changeset, and does not verify staged changesets for pending devices.
5. Click **Next**.
   The Task Summary screen opens (screen 2 of Deploy Staged Changeset wizard).
6. Click **Verify**.
   The system verifies the deployment and displays the results in the Verification Results area.
7. Click **Finished**.
   The Task Summary screen opens.

Once you verify the changeset, you can deploy it. See *Deploying a staged changeset using the Deploy Staged Changeset wizard*, on page 4-27.

To verify a staged changeset

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. From the **Error Behavior** list, select an option:
    - **Continue task on remaining devices:** The system continues to verify staged changesets for devices on which an error is not encounters, until the task finishes.
    - **Cancel task on remaining devices:** The system immediately stops the verification task if it encounters an invalid staged changeset, and does not verify pending devices.
2. Click **Next** to move to the Task Summary screen.
3. 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.
4. In the **Name** field, change the task description if necessary.
5. Click **Verify**.
   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.
6. Once the process quits running, click **Finished**.

Selecting a method to deploy staged changesets

After you create a changeset, you can deliver the device configuration data and settings in the changeset to any managed device in the network. When you deploy configuration data to a managed device, Enterprise Manager creates a back up of any existing configuration settings on the device, then overwrites the configured settings with the deployed changeset options. This provides you with the option to restore the original configuration for the device if required.

◆ **Important**

*Verify a staged changeset prior to deploying it to ensure that it works properly on the target device. See **Verifying and deploying staged changesets**, on page 4-24.*

You can deploy a staged changeset one of two ways:

- ◆ **From the Deploy Staged Changeset wizard**
  You can deploy a staged changeset from Task Summary screen of the Deploy Staged Changeset wizard. See Deploying a staged changeset using the Deploy Staged Changeset wizard in the following section.

- **From the Staged Changesets screen**
  You can deploy one or more existing staged changeset from the Staged Changesets screen. See *Deploying staged changesets from the Staged Changeset screen*, following.

Deploying a staged changeset using the Deploy Staged Changeset wizard

After you verify a staged changeset from the Deploy Staged Changeset wizard and click **Finished**, you can deploy the staged changeset.

To deploy a staged changeset from the Deploy Staged Changeset wizard

1. From Task Summary screen (screen 2 of Deploy Staged Changeset wizard), click **Deploy**.
   The Deploy Staged Changeset screen opens, and the progress bar on the task list indicates the progress of the task. When the task is complete, the task results display in the Task Summary area.
2. Click the **Details** link to view the task details, or click **Exit to Task List**.

Deploying staged changesets from the Staged Changeset screen

From the Staged Changeset screen, you can deploy one or more staged changesets.

To deploy one or more staged changesets from the Staged Changeset screen

1. On the Main tab, expand **Enterprise Management**, click **Configurations**, and select **Staged Changeset**s.
   The Staged Changeset screen opens.
2. Select the check box next to each staged changeset that you want to deploy.
3. Click **Verify** or **Deploy**.
   The Deploy Staged Changeset wizard screen opens
4. From the **Error Behavior** list, select an option:
   - **Continue task on remaining devices:** The system continues the deployment task on devices for which an error is not encountered, until the task finishes.
   - **Cancel task on remaining devices:** The system immediately stops the deployment task if it encounters an error, and does not deploy the staged changeset to pending devices.
5. Click **Next**.
   The Task Summary screen opens (screen 2 of Deploy Staged Changeset wizard).

6. Click **Deploy**.
   The Deploy Staged Changeset screen opens and the progress bar on the task list indicates the progress of the task. When the task is complete, the task results display in the Task Summary area.
7. Click the **Details** link to view the task details, or click **Exit to Task List**.

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, expand **Enterprise Management**, then click **Devices**.
   The Device List 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** and select **Configuration Viewer**.
   The Configuration Viewer opens.
4. In the **Partitions/Paths** box, click name of the partition that you want to view.
   The module listed in the **Modules** box change to display all modules available for the selected partition or path.
5. In the **Modules** box, click the type of system configuration that you want to view.
   The **Object Types** box changes to display all object types classes available for the selected module type.
6. In the **Object Types** box, click one or more network object types.
   The **Objects** box changes to display the objects available for the selected object type.
7. In the **Objects** list, click one or more objects.
   The screen changes to display a text view of the object configuration you selected.

See *Creating a custom template*, on page 4-12, for more information about the elements of the configuration source text.

5

Managing Software Images

- Overview of software image management
- Downloading and managing software images
- Copying and installing software to managed devices
- Viewing installation task progress

Overview of software image management

Installing software and hotfixes on BIG-IP® systems involves several steps that can be very time-consuming when you have to perform them on numerous individual systems.

When using Enterprise Manager™ as your centralized software management system, you can catalog and store several versions of software images, and deploy them to as many managed devices as necessary. Once the task is initiated, you can easily monitor its progress from the task list.

Depending on the software version you are installing, you may also have the option of distributing an image to a device and installing it at a later time. Separating the image distribution task from the installation process can potentially decrease your maintenance window.

Reviewing available software downloads

Software images are available for download from the F5 Networks Downloads site at **http://downloads.f5.com**.

◆ **Note**

*For specific information about how to download software images, see **Downloading software images**, on page 5-5.*

The F5 Downloads site hosts four main classes of files.

- **Releases**
  Full software products are called ***releases***, and usually include an image you can use to upgrade your software to a newer version.
- **Hotfixes**
  Minor updates that fix known issues to the current software version are included in ***hotfixes***.
- **Attack signatures**
  BIG-IP® Application Security Manager™ uses ***attack signatures*** to ensure that your applications are protected against new attacks and threats. For information about installing attack signatures, see *Managing ASM attack signatures for Application Security Manager*, on page 11-4.
- **Patches**
  Known vulnerabilities can typically be fixed with ***patches***.

These classes consist of different file types, defined in Table 5.1.

File Type	File Extension	Purpose
Software Image	**.iso**	Use a software image to perform a full upgrade. A software image contains all the packages necessary and is not specific to a local or remote installation.
Hotfix Package	**.im** or **.iso**	Use hotfix packages to install fixes developed since the last release. Legacy hotfix packages are IM files, which update a portion of the existing software without requiring a full installation. All other hotfix packages are ISO files, which require that you install the base software image with the hotfix. ***Note***: *Legacy software includes version 9.x of BIG-IP® Local Traffic Manager™, Application Security Manager™, WebAccelerator™ system, and Global Traffic Manager®, as well as WANJet® version 5.0, Secure Access Manager™ version 8.0, and Enterprise Manager™ version 1.x.*
Signature File	**.im**	Use signature files to update the system-supplied attack signature definitions on BIG-IP Application Security Manager systems.
Checksum	**.md5**	You can use the checksum file to verify the integrity of a file after you download it.
Documentation	**.txt** or **.readme**	Some releases include text or readme files as additional documentation.

Table 5.1 *File types available on **downloads.f5.com***

Reviewing installation options

F5 provides two different methods for installing your software.

- **Local installation**
  Requires downloading the entire software image to the hard drive of the managed device and running the installation from the device. This method is required when you use Enterprise Manager as your software management system.
- **Remote installation**
  Requires downloading the installation portion of a software image to a 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 method may be required for devices that use CompactFlash® storage instead of a hard drive.

You can typically tell the difference between the types of software installation method by reading the file name. For example, for the Enterprise Manager version 1.2 release, the local installation **.im** package is named **local-install-1.2.2.8.0.im**, and the remote **.im** package is named **remote-install-1.2.2.8.0.im**.

Using multiple boot locations

BIG-IP systems allow for a multiple boot capability, which means that you can choose to 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 may also be 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

We recommend that when you are performing an installation to a system in a high availability configuration, 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 Install 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 on Enterprise Manager systems, including the system you are working on. This means that Enterprise Manager can perform a self-install, as long as you added Enterprise Manager software to the software repository.

◆ **Note**

For legacy systems, you can install only software, not hotfixes, for the Enterprise Manager system on which you are working.

If you elect to discover Enterprise Manager devices in the network during a software upgrade or hotfix installation task, you can upgrade any Enterprise Manager systems that appear in the list of devices.

Essentially, you configure an upgrade task for Enterprise Manager much the way you configure any managed device, however, certain options may not be available. 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.

Checking the integrity of software images

Every software image includes the **md5sum** program, which verifies the integrity of the software image file that you downloaded. The verification process is dependent on the software version and client.

- For non-legacy software (managed devices running versions later than 10.x and Enterprise Manager version 2.x and later), the **md5sum** program runs automatically.
- For legacy software, the verification process varies according to your client system:
    - For Linux® systems, you can use the **md5sum** tool from the command line.
    - For other systems, including Microsoft® Windows® systems, you may need to use an external application to verify the **md5** checksum.

Performing software version rollbacks

You can use the Software Install wizard to install a previous software version (also known as rollbacks or downgrades) on managed devices.

It is important to note that Enterprise Manager applies the current device configuration to any newly installed software, whether it is an upgrade or a downgrade. Therefore, when you roll back to a previous software version, the device configuration may no longer be valid because of compatibility issues between the software versions. For this reason, we recommend that you manually configure the device after completing the downgrade task.

◆ **Note**

You cannot downgrade a Logical Volume Management (LVM) system (or a system using Volume Management) to version 9.x, nor can you go from a boot location running version 10.x software to version 9.x software using the Software Install wizard. You must perform this downgrade manually.

Downloading and managing software images

You obtain software images, and other files to assist you in managing devices in your network, from the F5 Networks Downloads site at **downloads.f5.com**. To access the F5 Downloads site, use your F5 Networks single sign-on account for technical support and downloads. If you do not have an account, you must first create one on the F5 Downloads site.

Once you download a software image, you can then add it to the Enterprise Manager software repository for installation on a managed device.

Downloading software images

When downloading software images, we recommend that you download and import the ISO (**.iso**) image file, because it contains all of the packages necessary to install the software and does not require that you specify a local or remote installation.

To download a software image

1. Using a web browser connected to the internet, browse to **http://downloads.f5.com**.
   The F5 Sign-on screen opens.

2. In the **User Email** field, type the email address for your F5 Technical Support account and in the **Password** field, type your password.

3. Click **Login**.
   The Overview screen opens and provides notes about using the Downloads site.

4. Click **Find a Download**.
   The Product Lines screen opens listing all F5 product families.

5. 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.

6. 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.

7. Read the EULA and click **I Accept** to accept the licence agreement.
   The Select a Download screen opens.

8. Click the name of the file you want to download.
   The Select a Download screen opens.

9. Click the download icon next to the protocol that you want to use.
   A dialogue box opens, prompting you to save the file to your local system.

Adding and removing software images in the software repository

After you download a software image from the F5 Networks Downloads site, you can add it to the appropriate Enterprise Manager software repository.

To add an image to the software repository

◆ **Important**

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

1. On the Main tab, expand **Enterprise Management**, click **Repository**, and select one of the following:
   - **ASM Attack Signature List**: for system-supplied attack signatures for Application Security Manager systems. For information about managing ASM attack signatures, see *Managing ASM attack signatures for Application Security Manager***, on page 11-4**.
   - **Hotfix Image List**: for hotfixes to existing software.
   - **Software Image List**: for full version software images for upgrade or roll back.

   After you click an image type, the associated image list screen opens.
2. Above the image list, click **Import**.
   The Import screen opens.
3. For the **File Name** setting, click **Browse** to search for the image using a directory or folder view.
4. After you specify the path and file name, click **Import**.
   The Software 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, as described in *Copying and installing software to managed devices*, on page 5-8.

To remove an image from the software repository

◆ **Important**

If you remove an image from the list, Enterprise Manager deletes the image from its database. To deploy this image in the future, you must add the image back to the software repository.

1. On the Main tab, expand **Enterprise Management**, click **Repository**, and select one of the following:

- **ASM Attack Signature List**: for a list system-supplied attack signatures for Application Security Manager systems. For information about managing ASM attack signatures, see *Managing ASM attack signatures for Application Security Manager*, **on page 11-4**.
- **Hotfix Image List**: for a list of hotfixes to an existing software installation.
- **Software Image List**: for a list of full version software images for upgrade or roll back.

After you click an image type, the associated image list screen opens.

2. Select the check box next to the image name that you want to remove, and click **Delete**.
After you confirm the deletion, Enterprise Manager removes the image from its database, and then from the image list.

Copying and installing software to managed devices

Once you have downloaded an image into the software repository, you can install it on your managed device. Enterprise Manager provides you efficient methods for copying and installing software and hotfix images to devices in your network. The wizard you use for this task is dependent on the software version you are installing, and is defined as follows.

- **Software Image Copy and Installation wizard**
  Generally applies to managed devices running versions later than 10.x and Enterprise Manager version 2.x. See *Using the Software Image Copy and Installation wizard*, following.
- **Legacy Software Image Installation wizard**
  Applies to version 9.x of BIG-IP Local Traffic Manager, Global Traffic Manager, WebAccelerator system, and Access Security Manager, as well as WANJet version 5.0, Secure Access Manager version 8.0, and Enterprise Manager version 1.x. See *Using the Legacy Software Image Installation wizard*, on page 5-11.

Working with volumes

Before starting the software installation task, it is important to understand the options for storing the new software image. Beginning in BIG-IP version 10.0 and Enterprise Manager version 2.0, F5 implemented a new disk-formatting scheme based on Logical Volume Management (LVM). ***LVM*** is a tool that dynamically adds virtual storage space to the BIG-IP system through the use of volumes. A ***volume*** is a specific section of the hard drive that can hold a complete version of software.

While the BIG-IP system's previous legacy and standard disk management schemes facilitated a more rigid method of allocating disk space, LVM allows you to install software images in a separate volume of a currently running system, without impacting the system or application traffic to the device. With this new scheme, you can also install software to another boot location while continuing to use the active boot location. During a normal maintenance window, you can boot the system to the new boot location, at which time you can test application traffic and verify that the new image is working as expected.

When you prepare to install BIG-IP version 10.x or Enterprise Manager version 2.x software, you have the option to format the system's hard drive as volumes, or leave the drive formatted as partitions. A ***partition*** is a logical container that you create, containing a defined set of BIG-IP system objects. You use partitions to control user access to the BIG-IP system.

On each device properties screen, in the advanced view, you can see which type of disk management scheme a managed device uses, allowing you to determine why an image may, or may not, be installed on a device.

Using the Software Image Copy and Installation wizard

You use the Software Image Copy and Installation wizard to guide you through the steps to copy and install software and hotfix images. Because the process of copying and installing a software image at the same time may become lengthy if you have a wide-area network, you have the option to copy the software to a device and install it at a later time. Separating the software image copy and installation processes gives you the flexibility to minimize your maintenance window.

◆ **Note**

You cannot install software to a Compact Flash boot location using the Software Image Copy and Installation wizard.

The following procedures apply only to managed devices running versions later than 10.x and Enterprise Manager version 2.x.

To start a software image copy and install task

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens.
2. Click **New Task**.
   The New Task screen opens.
3. For the Software Installation option, click **Copy and Install Software and Hotfix Images**.
4. Click **Next**.
   The Software Image Copy and Installation wizard opens.

   Continue working through the wizard screens, as described in the following pages, to copy a software image to selected devices.

To select a device and software image

On the Step 1 screen of the Software Image Copy and Installation wizard, you can select software images and devices on which to copy the software image.

1. From the **Software Image** list, select the software version that you want to copy to one or more devices.
2. From the **Hotfix Image** list, select a hotfix you want to include with the installation. This step is optional.
3. From the **Task Type** list, select one of the following options:
   - **Copy Install Image(s)** copies and installs the software image to the selected devices, in one task.
   - **Copy Image(s) Only** copies the software image to the selected device, but does not install the image.

- **Install Image(s) Only** installs a software image that was previously copied to selected devices.

4. From the **Device** list, select the types of devices you want displayed.
5. For the **Device Filter** setting, select an option to further narrow the managed devices displayed.

   The devices compatible to the options you selected display in the Compatible Devices in Standby or Offline Mode list.
6. In the Compatible Devices list, select the check box next to the device to which you want to copy the software image.
7. Click **Next** to move to the Step 2 of 3 screen.

To set the task options

1. From the **Configuration** list, select an option to select an option to install the full device configuration on the new boot location or only the essential, basic configuration.
2. From the **Post-Install Run Location** list, select an option to reboot using the upgraded software on the upgraded boot location or to continue to run on the current location.
3. From the **Configuration Archive** list, select an option to include or exclude private keys in the configuration archive.
4. From the **Device Error Behavior** list, select the action you want the system to take if an error occurs during installation.
   - **Continue task on remaining devices:** The system continues installing the software for selected devices on which an error was not encountered, until the task is finished.
   - **Cancel task on remaining devices: The** system stops the task immediately if an error occurs, and does not complete the installation on any devices still pending.
5. Click the **Start Task** button

See *Viewing installation task progress*, on page 5-16, for additional information about the task list.

Using the Legacy Software Image Installation wizard

You use the Legacy Software Image Installation wizard to:

- Install a legacy software image
- Install a legacy hotfix image

Installing a legacy software image

You use the Legacy Software Installation wizard to install legacy software images. To start a legacy software image installation task

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List Screen opens
2. Click **New Task**.
   The New Task screen opens.
3. For the Software Installation setting, select **Install Legacy Software Image**.
4. Click **Next**.
   The Legacy Software Image Installation wizard opens.

   Continue working through the wizard screens, as described in the following pages, to install a legacy software image.

To select a legacy software image

You select a legacy software image to install, and the devices on which to install the image, in Step 1 of the Legacy Software Image Installation wizard.

1. From the **Software Image** list, select the legacy software image that you want to install.
   The Compatible Devices table refreshes to display only devices that are compatible with the software image you select. If a device does not appear in the Compatible Devices area, check the software version on the device to verify that the hotfix is compatible.
2. Verify that the device’s **Disk Management Scheme** option (displayed on the advanced properties screen of the device) and the software’s **Supported Disk Management Schemes** option (displayed in the software images properties screen) are compatible.

   a) Review the release notes, available on **http://support.f5.com**, to verify that the software version you selected is compatible with the device to which you want to install the image.

   b) Verify that the image was downloaded and is in the software repository by seeing if it is listed on the Software Images screen.

3. From the **Device List**, select one of the following options to specify the types of devices displayed.
    - To view devices belonging to a particular device list, select the device list name.
    - To view all compatible devices, select **All Devices**.
4. From the **Device Filter** list, select an option to further limit the devices displayed.
   The Compatible Devices table displays only devices that are compatible with the hotfix image you select. If a device does not appear in the Compatible Devices area, check the software version on the device to verify that the hotfix is compatible.
5. In the Compatible Devices area, select the check box next to the devices on which you want to install the software image.
6. Click **Next** to move to the Step 2 of 4 screen.

To select associated hotfixes to include

Step 2 of 4 of the Legacy Software Image Installation wizard displays available legacy hotfixes that are compatible with the software image that you selected.

1. In the hotfix table, select the hotfix that you want to install.
   If no hotfixes appear in the table, verify that you imported a compatible software image to the software repository.
2. Click **Next** to move to the Step 3 of 4 screen.

To set options for the legacy software installation task

You can specify the install location and select a reboot option in Step 3 of 4 of the Legacy Software Image Installation wizard.

1. From the **Install Location** list, select the boot location that you want to install the software image.
   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 on the specified devices.
2. From the **Configuration Options** list, select the device configuration that you want 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 essential configuration**: leaves the newly upgraded boot location in a new, basic configuration state.
3. From the **Device Error Behavior** list, select the action you want the system to take if an error occurs during installation.

- **Continue task on remaining devices: The** system continues installing the upgrade for selected devices on which an error was not encountered, until the task is finished.
- **Cancel task on remaining devices: The** system immediately stops the task if an error occurs, and does not install the upgrade to any devices still pending.

4. From the **Post Installation** list, select the boot location to use for rebooting the device upon completion of the upgrade process.
5. For the **Configuration Archive** option, select an option to include or exclude the private SSL keys in the configuration archive created during the task.
6. Click **Next** to move to the Step 4 of 4 screen.

To review task options and initiate the task

You can review the details of the upgrade task you just configured in Step 4 of 4 of the Legacy Software Image Installation wizard.

1. In the **Task Name** field, type a new name to change the task name as it appears in the task list.
2. Review the information in the Task Summary area. You can change any of the following settings for an installation task on the device:
    - **Install Location**, you can select a different installation location for a target device.
    - For **Run Location** you can select a new run location for the target device.
    - For **Configuration**, you can change the type of configuration to install by selecting either **Full** or **Essential**.
3. Click **Start Task**.
   The Task Properties screen opens, displaying details relevant to the task that you configured, as well as task progress. See *Viewing installation task progress*, on page 5-16, for additional information about the task list.

Installing a legacy hotfix image

When you install legacy hotfixes, you must specify only one hotfix per device, and only on the managed device's active boot location.

To start a legacy hotfix image installation task

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens.
2. Click **New Task**.
   The New Task screen opens.

3. Next to Software Installation, click **Install Legacy Hotfix Image**.
4. Click **Next**.
   The Legacy Software Hotfix Installation wizard opens.

   Continue working through the wizard screens, as described in the following pages, to install a legacy hotfix.

To select a legacy hotfix image and the device on which to install the image

You select a legacy hotfix image in Step 1 of the Legacy Hotfix Image Installation wizard.

1. From the **Product Version** list, select the product version to which you want install the legacy hotfix.
   The Available Hotfixes table changes to display hotfixes compatible with the software version you selected.
2. In the Available Hotfix area, select the check box next to the hotfix that you want to install.

   Note*: If the hotfix image that you want to install does not display, verify that it exists in the software repository. If it is not available, you must download the image. See* ***Downloading and managing software images****, on page 5-5.*
3. Click **Next** to move to the Step 2 of 4 screen.

To select devices on which to install the legacy hotfix

You select the devices on which to install the legacy hotfix image in Step 2 of the Legacy Software Hotfix Installation wizard.

1. From the **Device List**, select one of the following options to specify the types of devices displayed.
   - To view devices belonging to a particular device list, select the device list name.
   - To view all compatible devices, select **All Devices**.

   The Compatible Devices table changes according to the option you select.
2. For the **Device Filter** setting, select an option to further limit the devices that appear in the Compatible Devices area.
   If a device does not appear in the Compatible Devices area, check the software version on the device to verify that the hotfix is compatible.
3. In the Compatible Devices area, select the check box next to the devices on which you want install the hotfix.
4. Click **Next** to move to the Step 3 of 4 screen.

To set task error options

You configure the task error behavior in Step 3 of the Legacy Hotfix Image Installation wizard.

1. From the **Device Error Behavior** list, select the action you want the system to take if an error occurs during installation.
    - **Continue task on remaining devices: The** system continues installing the hotfix for selected devices on which an error was not encountered, until the task is finished.
    - **Cancel task on remaining devices: The** system stops the task immediately if an error occurs, and does not install the hotfix to any devices still pending.
2. Click **Next** to move to the Step 4 of 4 screen.

To review and initiate the legacy hotfix installation task

You review and initiate the legacy hotfix installation task in Step 4 of the Legacy Software Hotfix Installation wizard.

1. Review the information in the Task Summary area.
2. Click **Remove**, below the Task Details table, if you want to remove a device from the install table.
   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 **Start Task**.
   The Task Properties screen opens, displaying the task details and its progress. See *Viewing installation task progress*, on page 5-16, for additional information about the task list.

Viewing installation task progress

From the Task List screen, you can view a summary of the tasks running and the details for a particular task. The task list displays an overview of all tasks on Enterprise Manager, including running and completed tasks.

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

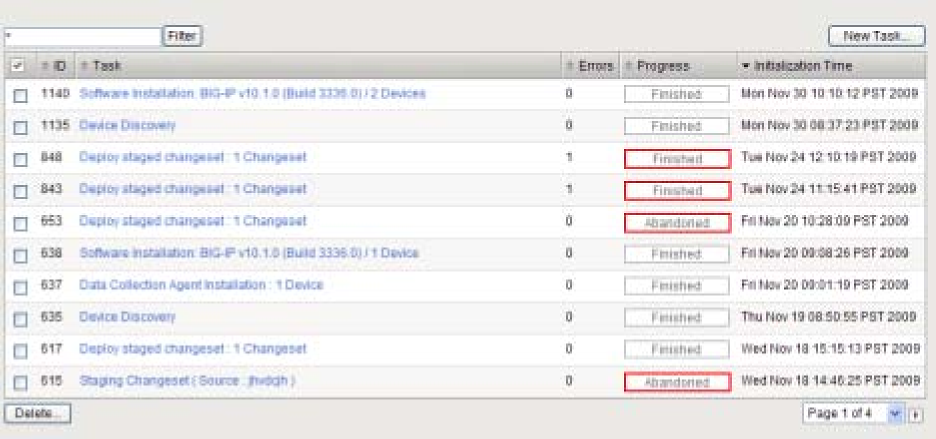
When all the individual jobs (such as installations or upgrades on a single device in a series) in a task finish, the system marks the task **Finished**, and the task name and description remains in the task list until you delete it.

Managing tasks

When 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. From the task list, you can click the name of a task to view additional details on the task properties screen.

To access the task list

On the Main tab, expand **Enterprise Management**, and click **Tasks**.
The Task List Screen opens, displaying all running tasks in Enterprise Manager.



☑	ID	Task	Errors	Progress	Initialization Time
□	1140	Software installation: BIG-IP v10.1.0 (Build 3336.0) / 2 Devices	0	Finished	Mon Nov 30 10:10:12 PST 2009
□	1135	Device Discovery	0	Finished	Mon Nov 30 08:37:23 PST 2009
□	848	Deploy staged changeset : 1 Changeset	1	Finished	Tue Nov 24 12:10:19 PST 2009
□	843	Deploy staged changeset : 1 Changeset	1	Finished	Tue Nov 24 11:15:41 PST 2009
□	653	Deploy staged changeset : 1 Changeset	0	Abandoned	Fri Nov 20 10:28:09 PST 2009
□	638	Software installation: BIG-IP v10.1.0 (Build 3336.0) / 1 Device	0	Finished	Fri Nov 20 09:08:26 PST 2009
□	637	Data Collection Agent Installation : 1 Device	0	Finished	Fri Nov 20 09:01:19 PST 2009
□	635	Device Discovery	0	Finished	Thu Nov 19 08:50:55 PST 2009
□	617	Deploy staged changeset : 1 Changeset	0	Finished	Wed Nov 18 15:15:13 PST 2009
□	615	Staging Changeset (Source : jhvdqh)	0	Abandoned	Wed Nov 18 14:46:25 PST 2009

Figure 5.1 *Task list example*

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, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens, displaying all tasks running on Enterprise Manager.
2. Select the check box next to 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.

To access the Task Properties screen

From the Tasks List, click the name of a task to access the Task Properties screen, where you can:

- View task properties.
- View task details, including an installation log, task results, and suggestions for failed jobs.

To cancel pending tasks

On the task properties screen, below the task summary table(s), click **Cancel Pending Items**. 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.

6

Managing User Account Data

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

Managing user accounts

When you manage BIG-IP® systems, you usually create and manage user accounts individually on each of these devices. If you have a large number of systems, it can be labor intensive to keep track every user's specific privileges on each device.

Using Enterprise Manager™ to manage user accounts saves you valuable time by providing you lists of all users in your network, and each device on which they have access privileges. You can also view user accounts in the context of device list to see which users have access to which devices in a custom device list.

◆ **Note**

*See the **Managing User Accounts** chapter in the **TMOS® Management Guide for BIG-IP® Systems** for further information about user accounts, including understanding user account types and user roles, and managing an authentication source.*

Viewing user roles

You can view all users for the managed devices in your network from the Enterprise Manager ***user list***. The user list provides you centralized access to details about each user account, without requiring that you to log on to the individual devices.

To view users

On the Main tab, expand **Enterprise Manager**, click **Access Control**, and select **Users**.

To view user-specific roles on devices or device lists

On the User list screen, select from the following options:

- To view a list of devices that a user has access to, click either the user name or the number in the Devices column.
- To view a list of device list that a user has access to, click the number in the Device List column.

For either 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 list. From these screens, you can drill down further for more detail about the users' roles on devices and in device lists.

◆ **Note**

*On the user-specific device lists 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 the selected device list.*

To view a list of user accounts on a device

1. On the Main tab, 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 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 List User Access screen, click the **Launch** link to open the managed device's configuration utility to manage the adjacent user account.

Copying user access configuration information

When you configure user account information on a BIG-IP system, you set parameters such as user names and passwords, shell access information, web interface and root access privileges, and an authentication source. When you configure BIG-IP systems individually, you must log on to each device and specify these parameters.

To configure this information more quickly and easily, you can use the Manager Copy User Access Configuration wizard. With this feature, you can create a common user account configuration on one device, and replicate that user account information on as many devices as required. This means that you can efficiently add new users and user account information to devices in your network from one central location.

Using the Copy User Access Configuration wizard

The Copy User Access Configuration wizard functions in a manner similar to other wizards in Enterprise Manager and involves starting a task, 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, expand **Enterprise Management**, and click **Tasks**.
   The Task List Screen opens.
2. Click **New Task**.
   The New Task screen opens.
3. For the **User Access**, option, click **Copy User Access Configuration**.
4. Click **Next** to move to the Step 1 of 3 screen.

To select devices and configuration data

On the Step 1 of 3 screen of the wizard, you can select source and destination devices, and choose what type of configuration data to copy.

1. From the **Source Device** list, select the device that you want to use as the data source for user configuration data.
2. For **Configuration Data**, select the check the box next to each type of data that you want to copy from the source device.
3. From the **Device List**, select one of the following options to specify the types of devices displayed.
4. From the **Devices** list, select an option to further narrow the managed devices displayed.
5. In the Compatible Devices area, select the check box next to each device to which you want to copy configuration data.

6. Click **Next** to move to Step 2 of 3.

To set task options

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

1. From the **Device Users** list, select the action that you want the system to take when copying user accounts to a destination device.
   - **Add users not already present on the device: The** system 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: The** system deletes the user account list on the destination device and replaces it with the user account list from the source device.
2. From the **Device Error Behavior** list, select the action you want the system to take if an error occurs during installation.
   - **Continue task on remaining devices**: The system continues installing the software for selected devices on which an error was not encountered, until the task is finished.
   - **Cancel task on remaining devices: The** system stops the task immediately if an error occurs, and does not complete the installation on any devices still pending.
3. Click **Next** to move to the Step 3 of 3 screen.

To review task options and initiate the task

You can review task options and start the task from the Task Review screen. This screen summarizes the task, including the source device, the configuration data to be copied, and the destination devices.

1. 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 opens, where you can specify users to include in the task.
2. When the settings are 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.

To start a copy task from the Launch Pad

1. On the Main tab, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. Click the name of the device that contains the 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 area, select the check 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 Copy User Access Configuration wizard opens with the **Source Device** and **Configuration Data** settings selected.
6. Complete the tasks described on page 6-3, *To select devices and configuration data*.

◆ **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

When you use Enterprise Manager as your user management system, you can create a task to automate a password change process for any user on any managed device in your network. This saves time as well as ensures that when you change a user account password, the new password is identical for the user on each device that you select.

Using the Change User Password wizard

You can use the Change User Password to assist you with changing user passwords. This wizard works in a way similar to other wizards in Enterprise Manager, and involves four main procedures:

- 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 change user password task

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List Screen opens.
2. Click **New Task**.
   The New Task screen opens.
3. For the **User Access** setting, select the **Change User Password** option, and click **Next**.
   The Step 1 of 4 screen opens.

To select a user and devices

On the Step 1 of 4 screen you select a user account, and the devices on which to change the user's password.

1. From the **User Name** list, select the user whose password you want to change.
2. From the **Device List**, select the types of devices displayed.
3. From the **Devices** list, select an option to further narrow the managed devices displayed.
4. In the Compatible Devices area, select the check box next to each device for which you want to change the user's password.
5. Click **Next** to move to Step 2 of 4.

To specify a new password

1. For the **Authentication** setting, in the **Password** field type the new user password.
2. In the **Confirm** field, re-type the password.
3. Click **Next** to move to Step 3 of 4.

To set task options

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

1. From the **Device Error Behavior** list, select the action you want the system to take if an error occurs during installation.
    - **Continue task on remaining devices**: The system continues installing the software for selected devices on which an error was not encountered, until the task is finished.
    - **Cancel task on remaining devices: The** system stops the task immediately if an error occurs, and does not complete the installation on any devices still pending.
2. Click **Next** to move to the Step 4 of 4 screen.

To review task options and initiate task

The Step 4 of 4 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. 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. When the settings are correct, click **Start Task**.
   The Task Properties screen opens and displays information about the configuration copy task.

7

Monitoring Object and Device Performance

- Collecting performance data and health statistics
- Using custom statistic profiles
- Viewing device statistics
- Managing storage for statistics
- Backing up and restoring the statistics database

Collecting performance data and health statistics

You can use the Enterprise Manager™ system to monitor the health, performance, and status of the F5 Networks® devices in your network at the device and object level. This can assist you in determining when you need to add new devices and help you identify any systems that are not performing at full capacity.

The Enterprise Manager system uses its Data Collection Agent, **big3d**, to gather this information. When you enable statistics collection, Enterprise Manager checks each managed device to verify the installed version of the Data Collection Agent. Once the version is verified, Enterprise Manager starts building a statistics database for all devices, according to the default statistics profile.

If the version is not compatible, the Data Collection Agent wizard manually initiates a task to push a new version of the Data Collection Agent to your managed devices.

◆ **Important**

Due to the processing power required to collect and store statistical information, data collection is available only for Enterprise Manager 3000 and 4000 platforms. If you upgraded to the current version of Enterprise Manager from a version prior to 1.7, you must re-license the system before using the data collection features.

Enabling statistics data collection

The statistics collection feature is disabled by default. To mitigate any potential traffic interruption, we recommend that you enable statistics collection during a network maintenance window when the effect on production traffic is minimized.

◆ **Important**

Enterprise Manager collects statistics only from devices that have BIG-IP® Local Traffic Manager™ (LTM®) licensed and provisioned. Starting with Enterprise Manager version 2.3, Enterprise Manager can also collect statistics from devices licensed and provisioned for BIG-IP® Global Traffic Manager™.

To enable statistic data collection

1. On the Main tab, expand **Enterprise Management** and click **Options**.
2. On the menu bar, click **Statistics** and select **Data Collection**. The Data Collection options screen opens.
3. From the **Collect Statistics Data** list, select **Enabled**.
4. Click **Save Changes**.

When you enable statistics collection, Enterprise Manager checks each managed device to verify that it has a compatible version of the Data Collection Agent. If a device requires a more recent version, Enterprise Manager marks that device as **Impaired** on the Device List screen, and displays a message indicating that an upgrade is required.

◆ **Note**

Once statistics collection is enabled, you can also assign a default statistics profile for newly discovered devices. For more information, see ***Assigning a default statistics profile for newly discovered devices****, on page 7-7.*

Installing the Data Collection Agent

To upgrade and install the Data Collection agent on one or more devices, use the Data Collection Agent Installation wizard. The Data Collection Agent Installation process involves three main tasks:

- Selecting the devices on which to install the Data Collection Agent
- Setting the install options
- Reviewing settings and starting the task

◆ **WARNING**

BIG-IP® Global Traffic Manager™ systems also use the Data Collection Agent to report performance information. When a new version of the Data Collection Agent is pushed to the managed Global Traffic Manager devices in your network, they may experience a single network traffic interruption of up to 60 seconds between synchronization group members. During this time, Global Traffic Manager clients may not respond to DNS requests with optimal routing information.

To select devices on which to install the Data Collection Agent

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List Screen opens.
2. Click **New Task**.
   The New Task screen opens.
3. For the **Software Installation** setting, click **Install Data Collection Agent**, then click **Next**.
   The Data Collection Agent Installation screen (Step 1) opens.
4. From the **Device List**, select an option to filter the list of devices.
   The Compatible Devices table changes according to the group you select.
5. In the **Device Filter** area, select an option to narrow the Compatible Devices displayed.
   - **Devices with data collection enabled in Standby Mode or Offline requiring update:** Displays only devices that are in standby or are offline, and have data collection enabled.
   - **Devices with data collection enabled in requiring update:** Displays all devices that require an update.

- **Devices with data collection enabled with correct version:** Displays only devices that have the correct version of **big3d** agent installed.
- **Devices with data collection disabled**: Displays only devices on which data collection is disabled.

6. In the Compatible Devices area, select the check box next to each device that you want to upgrade.
7. Click **Next** to move to the screen where you set task options, Step 2 of 3.

To set install options

On the Step 2 screen of the Data Collection Agent Installation wizard, you select the configuration archive format and the device error behavior.

1. From the **Configuration Archive** list, select whether an option to include or exclude private SSL keys in the configuration archive.
2. To set an error handling option for this task, select an option from the **Device Error Behavior** list:
   - **Continue task on remaining devices:** The system continues installing the upgrade for selected devices on which an error was not encountered, until the task is finished.
   - **Cancel task on remaining devices:** The system immediately stops the task if an error occurs, and does not install the upgrade to any pending devices.
3. Click **Next** to continue to the screen where you review the settings and start the task.

To review task options and start the task

On the Step 3 screen of the Data Collection Agent Installation wizard, you can review the task options and start the Data Collection Agent installation.

1. In the **Task Name** field, you can type a new name to change the task name as it appears in the task list.
2. Click **Start Task**.
   The Task Properties screen opens.

Choosing a statistics profile

A ***statistics profile*** specifies the type of information that you want Enterprise Manager to collect. These statistics can include such things as bytes and packets in and out of the device, connections made on the device, CPU utilization, memory, and disk usage. The statistics profile types correspond to the type of object you want to monitor: device, virtual server, pool, pool member, or node.

When configuring monitoring for your devices you can use the following statistics profiles, or a combination of both, for the objects in your network.

- **Standard statistics profiles**
  These profiles contain default metrics to collect and threshold values optimized for specific objects. You cannot modify standard statistics profiles. The default data collected is: Device Global, Device Chassis, Device CPU, Device Disk Space, Device UDP, Device TCP, Device HTTP, Device Client SSL, LTM Virtual Server, LTM Pool, LTM Pool Member, and LTM Node.
- **Custom statistics profiles**
  These are profiles that you create and for which you define metrics and optional threshold values. By enabling or disabling data collection on certain metrics, you can prioritize the information you are collecting, ensuring that your system resources are allocated appropriately. For information about custom statistics profiles, see *Using custom statistic profiles*, on page 7-8.

Viewing standard statistic profiles

The standard profile contains default threshold values that represent the known minimum or maximum values for certain device statistics. You cannot modify or delete a standard profile.

To view standard profiles in the Device Profiles list

1. On the Main tab, expand **Enterprise Management** and click **Statistics**.
2. On the menu bar, click the name of the profile you want to view and from the list, select the type of profile.
   The profile screen of the object type you selected opens.
3. Click the profile name containing ***Standard** to view the standard profile for the object type you selected.
   The threshold information for the standard profile you selected appears.

Assigning a statistics profile to a specific device or object

You can assign the same statistics profile to a several of objects in the same object class, or a number of devices. By doing so, you can make a change to the statistics profile that affects devices and objects assigned to that particular profile. This makes managing larger groups of objects or devices more efficient.

◆ **Note**

When you apply a new custom profile to a device or network object, you receive a message alerting you that the profile is being reconfigured. Statistics collection continues when additional metrics data is received.

To assign a statistics profile to a device

1. On the Main tab, expand **Enterprise Management**, and click **Statistics**.
2. Click the link for the device to which you want to assign a statistics profile.
3. On the menu bar, click **Statistics** and choose **Configure**.
   The device selection and monitoring profile information appears.
4. In the Device Selection table, review the settings for **Device**.
5. Specify whether you want to enable or disable statistics collection on the device, by selecting either **Enabled** or **Disabled** from the **Collect Statistics Data** list.
6. From the **Object Type** list, select **Device**.
7. In the Device Name table, from the **Associated Profile** list, select a profile that you want to assign to the corresponding device.
8. Click **Save Changes** to save the configuration.

To assign a statistics profile to a virtual server, pool, or node

1. On the Main tab, expand **Enterprise Management**, and click **Devices**.
   The Device List screen opens.
2. In the Device Name column of the Device List table, click the link for the device to which you want to assign a performance monitoring profile.
   The **Device Properties** screen opens.
3. From the Statistic menu, choose **Configure**.
   The device selection and monitoring profile information appears.
4. In the Device Selection table, ensure that the information for the **Device List** and **Device** are correct.

5. Specify whether you want to enable or disable statistics collection on the object, by selecting either **Enabled** or **Disabled** from the **Collect Statistics Data** list. The statistics are marked **Enabled** by default.
6. From the **Object Type** list, select the type of object to which you want to assign a performance monitoring profile.
   The screen displays the appropriate object type table, listing the names of the objects and their associated profiles.
7. To further filter the objects you want displayed, select an option for the **Associated Filter** list.
8. From the **Associated Profile** list, select the statistics profile to which you want the corresponding object associated.

   Tip: *To assign the same profile to all of the objects in the object list, click the **Copy to List** button. The profile you select for the first object populates to all other objects in the list. If the list of objects spans multiple screens and you want to use the **Copy to List** feature for all the objects on all screens, you must assign the profile on each of the screens separately.*
9. Click **Save Changes**.

Assigning a default statistics profile for newly discovered devices

To monitor new devices from the moment Enterprise Manager discovers them in your network, you can assign a default statistics profile.

◆ **Note**

*Statistics collection must be enabled for a device, before Enterprise Manager can monitor it. See **Enabling statistics data collection**, on page 7-1*

To assign a default statistics profile

1. On the Main tab, expand **Enterprise Management**, and under **Devices**, click **Statistics**.
   The Device Profiles screen opens.
2. Click **Device Profiles**, **Virtual Server Profiles**, **Pool Profiles**, **Pool Member Profiles**, or **Node Profiles**, depending on the type of object for which you want to collect data.
3. From the **Profile Name** list, select the profile that you want to assign to newly discovered devices.
4. Click **Save Changes**.

To override the default profile, you can assign a new statistics profile or a custom profile to a newly discovered device.

Using custom statistic profiles

In most cases, the standard statistics profile is best for monitoring the performance of F5 devices in your network. However, you also have the option to create and use a custom profile. With a custom statistics profile, you can select from a number of hardware, traffic, and connection related areas, designating minimum and maximum thresholds for the data that you want to collect.

Creating, viewing, and deleting custom statistics profiles

When you create a new custom profile, you can base it on an existing profile (including a standard profile), changing the collected metrics and thresholds as required.

To create a custom statistics profile

1. On the Main tab, expand **Enterprise Management**, and click **Statistics**.
   The Device Profiles screen opens.
2. Depending on the type of custom profile you want to create, on the menu bar, click **Device Profiles**, **Virtual Server Profiles**, **Pool Profiles**, **Pool Member Profiles**, or **Node Profiles**.
   The profile screen of the object type you selected opens.
3. Click **Create** at the top of the profiles table.
   The New Profile screen opens.
4. From the **Profile Source** list, select an option based on your intent:
   - To create a profile, accept the default option, **None**.
   - To use an existing profile's metric collection settings as a template for a new profile, select a profile name from the list. The profile metrics appear for the profile source you select.
5. In the **Name** field, type a name for the profile.
6. In the **Description** field, type a description for the statistics profile.
7. From the **Collection Interval** list, select the interval at which you want the data collected for the profile.

   Note: *Frequent data collection requires more storage space, which reduces the total amount of historical data you can store.*
8. In the Profile Metrics table, select the **Collect Data** check box for the metrics that you want to collect.
9. To specify thresholds, type a value in the **Minimum Threshold** and **Maximum Threshold** fields.

   Note*: You can specify thresholds for the metric, or leave the threshold information blank. If you leave the field blank, the system does not apply threshold values for that metric.*

10. Click **Finished**, located at the bottom of the list.
    The Device Profiles screen opens, displaying the new performance monitoring profile.

For information about how to assign a profile to a device, see *Assigning a statistics profile to a specific device or object, on page 7-6*.

To view the properties of the custom profile you created, click the profile name link in the **Profile Name** column of the profiles table.

To delete a statistics profile

1. On the Main tab, expand **Enterprise Management**, click **Statistics**, and then **Device Profiles**.
   The Device Profiles screen opens.
2. In the object profile table, select the check box next to the **Profile Name** of the profile you want to delete, and click **Delete**.
3. Click **Delete**, located under the Delete Confirm table to confirm deletion.

Viewing device statistics

Once you assign statistics profiles to objects, you can access a graphical representation of the information statistics collected. You can view the collected statistics information in a summary or a detailed graph format to determine the health and activity of your network objects and devices at a glance. Data refreshes at 60-second intervals.

To view statistics

1. On the Main tab, expand **Enterprise Management**, click **Statistics** and select **View**.
   The Statistics screen opens.
2. In the **Object Type** list, select the object type for the statistics you want to view.
   The screen refreshes to display the information related to the object type you selected. Statistics appear in a summary graph. If there are no statistics for the object type you selected, the **Data** column in the device name list table shows **No Data**.
3. From the **Time Span** list, select a time range to display as much data as needed. The system limits the display to the most recent data collected.
4. To review details about the utilization of a device, move your cursor over a graph.
   A box displays additional information about the device.
5. To view a detail graph for each summary data graph displayed, click a summary data graph.
   The detailed graph view displays the monitor name, the object instance that the system monitors, and a graphical representation of the statistical data according to the value you selected as a time span for statistics collection.

By default, Enterprise Manager displays up to 8 records per screen. If there are more than 8 graphs, the screen displays a link to the graphs, where you can view up to 11 graphs.

◆ **Tip**

*To change the number of devices displayed, in the navigation pane, click **System**, then click **Preferences** and change the **Records Per Screen** setting. This is a global setting and changes affect all list screens on the Enterprise Manager system. Note that performance could be affected if you select a large number of items to display on a screen.*

Customizing displayed statistics

On the Statistics screen, you can specify what you want displayed in the summary graphs by selecting an option from the **Rule** list. For example, if you select Device Health, the graphs change to display a set of graphs that display statistics related to the physical health of the device such as chassis temperature, CPU fan speed, and processor utilization percentage.

Table 7.1 outlines the viewing options available from the **Rule** list.

Rule	Statistical graphs displayed
All Active	All statistics currently configured in the associated statistic profile
All Errors	All statistics related to error conditions
Commonly Used	A subset of commonly used statistics available in the associated statistic profile
Common Errors	A subset of commonly occurring errors available in the associated statistic profile
Device Health	A subset of device statistics related to the physical health of the device
Device Stats	A subset of device statistics related to the traffic management of the device
HTTP Stats	A subset of statistics related to HTTP traffic
Out of Range	A collection of statistics where the value is currently exceeding a user-set threshold
Red Line	A collection of resource-utilization statistics that have a user-set threshold
SSL Stats	A subset of statistics related to SSL traffic
TCP Stats	A subset of statistics related to TCP traffic
UDP Stats	A subset of statistics related to UDP traffic

Table 7.1 *Rule classes for statistics graphs*

To customize displayed statistics

1. On the Main tab, expand **Enterprise Management**, click **Statistics** and select View.
   The Statistics screen opens.

2. From the **Rule** list, select an option.

3. From the **Time Span** list, select a time range for viewing collected data.
   The data displayed is limited to the most recent data collected.

Managing storage for statistics

Enterprise Manager stores statistical data until the system reaches the storage capacity that you define. When that capacity is met, the oldest data in the system is replaced with new data, up to the storage limit you set. If you decrease the allocated statistics storage capacity, the system removes the oldest data to reduce the amount of stored statistics to meet the new limit.

When you enable statistics collection, it affects the overall performance of Enterprise Manager. Therefore, it is important to plan for your system's database storage needs by understanding your system's capacity and estimating your storage requirements in order to maximize the value of the statistics features.

The Enterprise Manager system's default value of 1 GB for statistics data storage is intentionally low, allowing you to establish a reasonable value based on your environment. Once you have estimated the availability of storage on your system, you can change the default database maintenance storage capacity setting of 1 GB, using the procedure *To configure statistics data storage*, on page 7-14. Increasing the default setting is essential to monitoring statistics data over time.

There are a number of ways to manage your storage needs, including estimating your storage capacity, creating remote backups of the information you no longer need, setting statistics storage limits, and creating alerts to warn you when you reach a storage capacity threshold on your system.

To help you plan for statistics storage:

- View the system hard drive allocation by file type
- Calculate statistics data storage

Viewing system hard drive allocation by file type

The statistics database shares drive space on the Enterprise Manager system with software images, attack signature files, system logs and backups, and so on. Depending on how many devices and objects for which you want to collect statistics, the size of the statistics database may be limited by how many other parts of the Enterprise Manager system are using the shared file system. The size of the database affects how long you can store statistical data, and how you use graphs over time to identify trends.

To determine how the system is allocating disk space, you can use the System Information screen. Additionally, you can create a system alert to notify you when you meet a threshold for statistics data storage. For information about creating an Enterprise Manager system alert, see *Creating alerts for Enterprise Manager*, on page 8-6.

To open the System Information screen

On the Main tab, expand **Enterprise Management**, and click **System Information**.

The System Information screen presents both visual and textual representations of how Enterprise Manager allocates disk space.

Calculating statistics data storage

Enterprise Manager provides information about the amount of space available for the storage of statistics, the amount of space currently in use for statistics data, and the estimated number of days of storage with the current data allocation.

To determine the allocation of resources on the drive, as well as estimate the storage capacity, you can recalculate the estimated days of storage without committing the change. When you have determined that you are satisfied with the storage space value, you can opt to save the changes.

◆ **Important**

*If you change the **Allocated Statistic Storage Space** setting to a value less than the current value, Enterprise Manager removes statistics data from the database, starting with the oldest, until it reaches the new lowered storage limit. If you want to retain your older statistics, perform a database backup before you reduce the allocated statistics storage space. See **Backing up and restoring the statistics database, on page 7-15**, for information about backing up your statistics database.*

To configure statistics data storage

1. On the Main tab, expand **Enterprise Management**, and click **Statistics**.
   The Device Profiles screen opens.
2. From the **Options** menu, choose **Data Storage**.
   The Data Storage screen opens.
3. Review the available statistics storage space, statistic storage currently in use, and the estimated statistic storage space with the current settings.
4. To determine the allocation of resources that best suits your performance needs, select a value from the **Allocated Statistic Storage Space** list.
5. Click **Recalculate**.
   The system recalculates statistic storage based on the change, without saving the configuration.
6. When you are satisfied with the allocation of statistic storage, click **Save Changes** to commit the configuration changes.

Backing up and restoring the statistics database

The Enterprise Manager system offers the following options to back up the statistic database.

- Backing up and restoring the statistics database from the command line
- Scheduling remote backups of the statistics database

If the Enterprise Manager system is configured as a high availability system, you can back up your system's monitoring information by regularly running the ConfigSync task. See *Managing user roles and authentication*, on page 2-1, for more information.

In the high availability configuration, you can schedule and configure the inclusion or exclusion of statistics data on the Enterprise Manager system.

After you have created a backup, you can successfully restore the database when required.

Backing up the statistics database from the command line

You can back up and restore the statistics database from the command line using the following procedures.

To create a backup of the statistics database

1. Log on to the command line of the Enterprise Manager as the **root** user.
2. Type the following command, on one line:

   ```
   em-backup-extern
   <user@host.com>:/<full_file_path_for_backup_file>
   ```

   The default file name is **f5em_extern-<date stamp>**.

To restore the statistics database

1. Log on to the command line of the Enterprise Manager as the **root** user.
2. Type the following command, on one line:

   ```
   em-restore-extern
   <user@host.com>:/<full_file_path_for_backup_file>
   ```

   For example, if you did not rename the backup file, you would type:

   ```
   em-restore-extern <user@host.com>:/f5em_extern-<date
   stamp>
   ```

Scheduling backups of the statistics database

You also have the option configure the Enterprise Manager system to allow remote access to the statistics database (MySQL database) from a third-party database browsing or editing tool, and then schedule a regular backup interval.

The MySQL database listens on port **3306** of your Enterprise Manager system when data collection is enabled (see *Enabling statistics data collection*, on page 7-1). You can query database information, review overall system statistics, create your own graphs and reports, and save the data outside of Enterprise Manager before database maintenance occurs.

To successfully query the MySQL database, you use the following credentials:

- Username: **f5em_client**
- Password: **default**
- Database name: **f5em_extern**

◆ **Important**

Remote database access is available for data stored on the local database only. If you have configured an external database to store statistical data, Enterprise Manager cannot run scheduled backups.

To allow for remote access to the database information

1. On the Main tab, expand **Enterprise Management**, and click **Statistics**.
   The Device Profiles screen opens.
2. From the **Options** menu, select **Remote Access**.
   The Remote Access Options screen appears.
3. In the Statistics Database Remote Access table, select the **Allow Remote Access** check box.
   Additional options display.
4. In the **Password** field, type a new password to replace the password, **default**.
5. In the **Confirm Password** field, type the new password again.
6. Click **Save Changes** to save the remote access configuration.
   The system uses the user name **f5em_client** and the password you provided to access the remote database.

Once you have remote access to the statistics database, you can schedule regular remote statistics database backups to maximize your storage availability. You can schedule a regular backup of the statistics database to a remote server on a daily, weekly, or monthly schedule at a specific time of day that you specify.

Enterprise Manager uses an **rsync** process to send the statistics database to a remote server. Before you configure a backup schedule, you must first perform a manual key exchange between Enterprise Manager and the remote system to which you want to back up the data.

To configure a password key exchange for database backup

1. Log on to the command line of the Enterprise Manager as the **root** user.
2. At the command line, type the following commands, and press Enter after each:

   ```
   mkdir -p /root/.ssh
   chmod 0700 /root/.ssh
   ssh-keygen -t dsa -f /root/.ssh/id_dsa
   ```

   This creates two files, **/root/.ssh/id_dsa** and **/root/.ssh/id_dsa.pub**, on the Enterprise Manager system, which are the private key and public key, respectively.
3. Copy **/root/.ssh/id_dsa.pub** to the destination server by typing the following command, where **<destination IP>** is the IP address of the remote server:

   ```
   scp /root/.ssh/id_dsa.pub em_backup@<destination IP>:
   ```

4. Log onto the command line of the remote server as user **em_backup**.
5. To create the **/home/em_backup/.ssh** directory on the remote server, type the following commands, and press Enter after each:

   ```
   mkdir -p /home/em_backup/.ssh
   chmod 0700 /home/em_backup/.ssh
   ```

6. On the remote server, type the following commands, and press Enter after each:

   ```
   cat /home/em_backup/id_dsa.pub >>
   /home/em_backup/.ssh/authorized_keys2
   chmod 0600 /home/embackup/.ssh/authorized_keys2
   ```

7. Depending on the version of OpenSSH included, you may need to type the following commands, and press Enter after each:

   ```
   cat /home/em_backup/id_dsa.pub >>
   /home/em_backup/.ssh/authorized_keys
   chmod 0600 /home/em_backup/.ssh/authorized_keys
   ```

8. On the Enterprise Manager system, at the command line, test the connection using SSH with the following command, where **<destination IP>** is the IP address of the remote server:

   ```
   ssh em_backup@<destination IP>
   ```

To schedule a regular statistics backup

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task screen opens.
2. On the menu bar, click **Schedules** and select **Statistics Database Backup**.
   The Task Schedules screen opens.
3. From the **Backup Data** list, select an interval to back up the statistics database.
   Additional options for **Day of the Month** or **Day of the Week**, and **Start Time** display depending on the option you choose for backup.
4. From **Day of the Month** or **Day of the Week** list, select a day on which you want Enterprise Manager to back up the database.
5. For **Start Time**, set a time for the system to back up the database.
6. In the **Username** field, type the user ID that you use to log on to the remote system.
7. In the **Hostname** field, type the FQDN of the remote system where you plan to back up the statistics database.
8. In the **Path** field, type the file path for the remote system.
9. Click **Save Changes**.

8

Using Alerts

- Overview of alerts
- Setting alert default options
- Creating alerts for Enterprise Manager
- Creating, modifying, and deleting alerts for devices

Overview of alerts

With Enterprise Manager as your network management appliance, you can create alerts to help you better maintain the health of your network. For example, you can create custom system alerts to notify you or others if a device becomes unreachable by Enterprise Manager, upon completion or failure of a software or hotfix installation, or if a device system clock differs from the Enterprise Manager clock.

You can apply alerts to individual devices, or to a device list. You can also create alerts for the Enterprise Management device itself, so that you can maintain the health of your management system.

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:

- Statistical data thresholds exceeded
- Device status change
- 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 statistical data thresholds

For systems that support statistics collection, you can create statistics data threshold alert instances for which you can specify how long a statistic is out of range before the system triggers an alert.

Creating an alert based on statistic thresholds provides you with notification beyond red-line warnings on the Statistics screens.

◆ **Important**

Statistical data threshold alerts are available only for statistics stored locally on the Enterprise Manager system.

Alerting for device status changes

You can create a device status change alert to inform you when:

- Status changes between Active, Standby, Offline, or Forced Offline Mode.
- A device is in an Impaired state.
- Enterprise Manager cannot communicate with 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 status of a managed device changes, you can configure an alert.

Warning for Offline or Forced Offline mode

If you take a device offline, or force it offline, the status icon in the Device list reflects those changes. However, if you want to immediately notify a user as soon as the offline or forced offline status of a managed device changes, you can figure an 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 device status to Impaired.

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. You can still perform management tasks on the device, however, because the configuration is not completely represented, the device status is marked Impaired.

You can create an alert that immediately notifies a user if the status of a managed device changes to Impaired so that the user can 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.

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 for a device to be unreachable. For example, 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.

In addition to monitoring the Device list, you can create an alert to send a notification when a device is unreachable, so the alert recipients can get the managed device back online. When configured, the system checks the connection every 10 minutes and triggers an alert if the device is unreachable.

◆ **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.

Alerting for expired or near-expired certificates

Enterprise Manager can help you easily monitor certificates defined on managed devices in your network. In addition to providing a broad overview of device certificates in the certificate list, you can also create a certificate expiration alert to trigger when a certificate expires or is within a specific number of days of expiration.

When you define an alert for certification expiration, you can specify how many days in advance that you are notified, before the certificate expiration date occurs. 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.

◆ **Note**

You cannot configure certificate-based alerts on devices or device lists until you enable certificate monitoring on those devices or device lists. See, ***Disabling and enabling certificate monitoring****, on page 9-1.*

Notifications for completed installations and upgrades

When you start a software upgrade, hotfix installation, or attack signature installation task, you may not be able to monitor the status of the task. For example, if you start an upgrade on multiple devices, it may not be feasible to manually check to see if a particular device is upgraded.

In addition to viewing all tasks from the Task List and detailed information in the Task Properties screen to monitor progress, you can also create an software install completion or attack signature install completion alert to notify you or others when a specific device completes an upgrade or installation task.

Alerting for failed installations and upgrades

When performing an upgrade, hotfix installation, or attack signature installation task on several devices, you may not be able to closely monitor each job. For example, if you start an upgrade on multiple devices, you may not be able to manually check to see if a particular installation or upgrade failed.

In addition to viewing all tasks from the Task List Screen and detailed information in the Task Properties screen to monitor progress, you can also create a software install failure or attack signature install failure 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.

Warning for system clock discrepancies between the Enterprise Manager and managed devices

When Enterprise Manager adds a device to its managed Device list, it creates a certificate that it uses to authenticate itself to the managed device. If the system clock of Enterprise Manager and the managed device are not synchronized within 15 minutes of each other, the management certificate becomes invalid. An invalid certificate on a device can result in Enterprise Manager losing management privileges for that device.

To prevent this scenario, you can set a clock skew alert that checks the system clocks every 10 minutes and sends a notification if the Enterprise Manager and managed device system clocks are out of synch by a specific number of minutes. Then, the user who receives the alert can log on to the managed device and correct the system clock.

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 rotating archive failure 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.

Setting alert default options

When you create alerts, you can specify delivery options for that alert. You can also set a certain recipient's email address, or a remote syslog server, to receive notifications for all alerts by default. Once these are set, Enterprise Manager sends alert notifications to the default email address you specified, or to the remote syslog server, unless the alert is configured to notify another recipient. For information about for enabling alerting features, such as setting alert default options, and sending email messages or SNMP traps, see the ***Enterprise Manager*™ *Getting Started Guide***.

Creating alerts for Enterprise Manager

To help maintain the health of the Enterprise Manager device, you can create system alerts to notify you when CPU, disk, or memory usage meets or exceeds a particular threshold.

◆ **Important**

*To successfully send alerts, Enterprise Manager must be configured to deliver locally generated email messages. For more information, see the **Enterprise Manager™ Getting Started Guide**.*

To create a system alert for Enterprise Manager

1. On the Main tab, 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 the **Conditions** setting, select the check boxes for the metrics that you want to track with alerts.
   The screen refreshes to display threshold fields for the conditions you selected.
4. In the threshold fields, type a maximum value for the associated condition.
5. In the EM Alert Action area, for **Action**, select the type of action that you want Enterprise Manager to take when the values you specified for the thresholds are met or exceeded.
6. Click **Save Changes**.

◆ **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.

Creating, modifying, and deleting alerts for devices

Creating an alert for a device or device list 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 the New Alert screen.

To create an alert for a device

1. On the Main tab, expand **Enterprise Management**, click **Alerts**, and select **Device Alerts**.
   The Device Alerts list screen opens.

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

3. In the **Name** field, type a name for the alert, as you want it to appear in the Device Alerts screen.

   Note: *Once you create the alert, you cannot change the name.*

4. From the **Alert Type** list, select the alert condition.
   Depending on the type you select, the screen may change to provide additional options.

5. If the alert type requires a threshold, for the **Condition** setting, specify a threshold value.

6. For the **Action** setting, select the check box next to each action 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 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, select the check the box next to the email.

   - To send an email to an alternate recipient, clear the check 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 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, select the check box next to the default syslog server.

   - To log an event on an alternate server, clear the check box and type a new syslog server address in the field.

9. In the Alert Assignments area, assign this alert to devices or device lists:

   a) For either the **Devices** or **Device List** setting, click a device or device list in the **Available** box to select it.

   b) Click the Move button (**<<**) to move the selected devices or device lists to the **Assigned** box.

The alert now applies to devices and device lists displayed in the **Assigned** box.

10. Click **Finished**.
    The Device Alerts screen opens, and the new alert appears in the list.

The flexibility of alerts allows you to easily apply or remove existing alerts for specified devices or device lists. You can also change the alert actions or email recipients for an alert. From the Device Alerts screen, click the name of an alert to open the Alert Properties screen.

To modify an alert

1. On the Main tab, expand **Enterprise Management**, click **Alerts**, and select **Device Alerts**.
   The Device Alerts list screen opens.
2. In the alert list, click the name of the alert that you want to modify.
   The Alert Properties screen opens.
3. Change any of the values in the Configuration, or add or remove devices and groups from the alert in the Alert Assignments area.
4. Click **Save 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, select the check box next an alert, and click **Delete**, located below the list.

9

Managing Device Certificates

- Monitoring device certificates
- Creating a device certificate alert

Monitoring device certificates

When you use BIG-IP® Local Traffic Manager™ to manage your SSL traffic, you can have a large number of SSL and web certificates on many different devices in your network. ***Traffic certificates*** are server certificates that a managed device uses in its traffic management tasks. ***System certificates*** are the web certificates that allow client systems to log into the BIG-IP system Configuration utility.

To assist you in managing these certificates, Enterprise Manager™ provides you a summary of vital certificate information for each managed device in your network that has certificate monitoring enabled.

When you monitor a device list, you automatically monitor all of the certificates on all of the devices that are members of that device list.

Disabling and enabling certificate monitoring

Certificate monitoring is enabled by default for all managed devices. If you no longer want to monitor certain certificates, you can disable a device or device list's certificate monitoring. When you disable certificate monitoring for a device, that certificate no longer displays on the certificate list, and certificate expiration alerts are cancelled.

To enable or disable certificate monitoring

1. On the Main tab, expand **Enterprise Management**, click **Options**, and select **Certificates**.
   The Certificates list screen opens.
2. For the **Devices** or **Device List** setting, in the **Enabled** list, click the name of a device.
3. Click the Move (>>) (<<) buttons to move the select devices to the enabled or disabled list.
4. Click **Save Changes**.

Viewing certificate information

The information that displays on the respective certificate list screen provides a summary of:

- Certificate expiration status
- Certificate and organization name
- Device on which the certificate is configured

Using this overview can save you time over monitoring certificate expiration dates on individual Local Traffic Manager devices.

◆ **Tip**

If you require additional notification for expired or expiring certificates, you can create a certificate expiration alert. For detailed instructions, see ***To create a certificate expiration alert****, on page 9-3.*

To view device certificate screens

1. On the Main tab, 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 certificate.
3. On the menu bar, click **Monitored Certificates** to view the system certificate list.
4. To view additional details about a particular certificate, click the name of a certificate to open the Certificate Properties screen.

In addition to the general certificate information, the certificate list screen also displays a status flag for each certificate. This provides you with a quick visual of the status for your certificates. Table 9.1, following, defines the status flags provided on the certificates page.

Status Flag	Expiration Status
🟥 Red Status Flag	This certificate has expired. When client systems require this certificate for authentication, the client receives an expired certificate warning.
🟨 Yellow Status Flag	This certificate will expire in 30 days or less. The certificate is still valid, but you should take action to prevent certificate expiration.
🟩 Green Status Flag	This certificate is valid and will remain valid for at least 30 more days.

Table 9.1 *Certificate status flag definitions*

Creating a device certificate alert

In addition to monitoring certificate status from the certificate screens, you can also create an alert to log or send an email notification of an upcoming certificate expiration. You create a certificate expiration alert from the New Alert screen, where you can specify the devices or device list, the notification method, and how many days before the certificate expires you want to be notified.

◆ **Important**

All devices display as available from the New Alert screen, even if certificate monitoring has not been enabled for the device. If you assign an alert to a device for which certificate monitoring is not enabled, the alert will fail. Before you create a device certificate alert, F5 recommends that you first verify that certificate monitoring is enabled for the device.

To create a certificate expiration alert

1. On the Main tab, expand **Enterprise Management**, click **Alerts**, and select **Device Alerts**.
   The Device Alerts list screen opens.

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

3. In the **Name** field, type a name for the alert, as you want it to appear in the Device Alerts screen.

   Note: *Once you create the alert, you cannot change the name.*

4. From the **Alert Type** list, select **Certificate Expiration**.

5. For the **Condition** option, select the check box next to the number of days, before the certificate expires, that you want to be notified. You can also type a customized number of days in the **Condition** field.

6. In the **Action** section, select the check box next to the type of notification you want to receive.

7. If you selected the option to send an email, then for **Email Recipient**, you can 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, select the check box for the email.

   - To send an email to an alternate recipient, clear the check box and type a new email address in the field.

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, select the check box.
    - To log an event on an alternate server, clear the check box and type a new syslog server address in the field.
9. In the Alert Assignments area, assign this alert to devices or device list:

    a) For either the **Devices** or **Device List** setting, click a device or device list in the **Available** box to select it.

    b) Click the Move button (**<<**) to move the selected devices or device lists to the **Assigned** box.
    The alert now applies to devices and device lists displayed in the **Assigned** box.
10. Click **Finished**.
    The Device Alerts screen opens, and the new alert appears in the list.

10

Auditing Enterprise Manager System Events

- Reviewing the different event logging options
- Auditing events for Enterprise Manager
- Searching the audit log

Reviewing the different event logging options

So that you can review valuable information about pertinent events, Enterprise Manager™ provides access to a comprehensive set of logs. The types of logs you can view 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 logged when changes are made to the Enterprise Manager system configuration. You can see which enterprise management tasks were initiated from a particular Enterprise Manager system. The Enterprise Manager system logs the messages for these events in the file **/var/log/em**. Logging audit events is optional.

Enterprise Manager and BIG-IP® systems use the Linux utility, **syslog-ng**, to log events. The **syslog-ng** utility is an enhanced version of the standard UNIX and Linux logging utility **syslog**. You can find information specific to BIG-IP system logging features in the *Logging BIG-IP System Events* chapter of the ***TMOS® Management Guide for BIG-IP® Systems***.

Although event logging for Enterprise Manager works the same as in a BIG-IP system, some of the logging options specific to traffic management may not apply to Enterprise Manager. When you set local traffic logging options, some events may not produce logs, because Enterprise Manager does not deal with the same kind of traffic as a BIG-IP Local Traffic Manager™ system.

Viewing log files

You view the Enterprise Manager audit log from the same screen as the BIG-IP system log.

To view log files

1. On the Main tab, expand **System**, and click **Logs**.
   The System Logs screen opens.
2. Select the type of log you want to view:
   - 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.

Auditing events for Enterprise Manager

The Enterprise Manager system features seven processes that enable the system to manage other F5 Networks® 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 lists, 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 audit and log a variety of events. These message include 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.

Viewing and modifying audit logging options

The auditing feature logs messages that pertain to configuration changes that users or services make to the Enterprise Manager system configuration. Changes such as when you create, modify, or delete a managed device, or install a software image. By default, the auditing feature that logs system events is enabled.

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 view and modify the audit logging options

1. On the Main tab, expand **System**, and click **Logs**.
   The System Logs screen opens.
2. On the menu bar, click **Options**.
   The Options screen opens.
3. From the **Audit** list, select a log level.
4. Click **Update**.

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, expand **System**, and click **Logs**.
   The System Properties 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.

11

Working with Application Security Manager Policies and Attack Signatures

- Staging and deploying Application Security Manager Policies
- Managing ASM attack signatures for Application Security Manager

Staging and deploying Application Security Manager Policies

Starting with BIG-IP® Application Security Manager™ (ASM™) version 10.0.1, Enterprise Manager™ helps you to easily manage security policies and ASM attack signature files among multiple devices. Once web applications are installed and initial configuration is completed on each Application Security Manager device, you can stage changesets to deploy new security policies or make modifications to existing security policies. You can deploy the changeset immediately, or at a designated time in the future.

◆ **Important**

Distributed security policies include ASM attack signature set definitions, and not the ASM attack signatures themselves. For the security policies to work properly, the ASM attack signatures (including custom signatures) must be the same on all systems to which you are deploying the security policies. For information about installing and completing the initial configuration of Application Security Manager web applications, refer to the ***Configuration Guide for BIG-IP® Application Security Manager™***.

◆ **Note**

When staging and deploying changesets, Enterprise Manager interprets the instance data based on metadata embedded in the configuration. Therefore, important binary configuration information is hidden because it is not editable.

Using the Stage Security Policy Changeset wizard

Staging and deploying security policies to your Application Security Policy devices using the Stage Security Policy Changeset wizard involves three main procedures.

- Selecting a security policy to stage and deploy to a device
- Selecting a target device on which to install the security policy
- Verifying, staging, and deploying the security policy

◆ **Note**

By default, only users with Administrator or Application Editor permissions can perform the following procedures.

To start a security policy changeset deployment task

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List Screen opens.

2. Click the **New Task** button.
   The New Task screen opens.

3. In the Application Security section, select **Stage a Security Policy Changeset**.

4. Click the **Next** button.
   The Stage Security Policy Changeset wizard opens.

   Continue working through the wizard screens, as described in the following pages, to copy a stage a security policy image for selected devices.

To select a device and a security policy to deploy

On the Step 1 screen of the Stage Security Policy Changeset wizard, you select a security policy and the devices on which to deploy the security policy.

1. From the **Source Device** list, select the device to which you want to deploy the security policy.
   The **Source Device** list changes to show only the devices in the device list you selected.

2. From the **Source Device** list, select the source device that contains the security policy you want to deploy.
   The **Security Policy** list changes to show only the policies available on the source device you selected.

3. From the **Security Policy** list, select the security policy that you want to deploy.
   The security policy names correspond to the security policy names on the Application Security Manager system you selected.

4. From the **Target Device List** list, select an option.
   The Compatible Devices table changes to display the devices in accordance with the option you selected.

5. In the **Target Device Filter** section, select an option on which to filter and display the compatible devices based on the following criteria:

   - **Compatible Devices in Standby Mode or Offline Mode** displays only compatible devices currently in Standby or Offline mode.

   - **Compatible with Security Policy** displays all devices compatible with the image that you selected in the **Security Policy** list.

   - **Incompatible with Security Policy** displays only Application Security Manager devices that are not compatible with the selected security policy.

6. In the Compatible Devices in Standby or Offline Mode table, select the check box next to the device that you want to update.

7. Click **Next** to move to the screen where you select security policy changesets and verify security policy settings, Step 2 of 2.

To verify and deploy a security policy changeset

On the Step 2 screen of the Stage Security Policy Changeset wizard, you can create a staged changeset and confirm security policy settings.

1. In the **Changeset Description** field, type a new description for the staged changeset.
2. From the **Create Archive(s)** list, select one of the following options for archiving information about the device:
    - **Create archive for each device before deploying** prompts the system to create a configuration archive of the target device before deployment.
    - **Do not create archive** prompts the system not to create a configuration archive of the target device before deployment.
3. From the **Archive Options** list, specify whether to include private keys in the archive, if applicable.
4. In the Policy Settings table, for **Policy Name**, type a name for the security policy on the target system.
5. For **Policy Description**, type a description for the security policy on the target system.
6. For **Apply Policy?**, indicate whether you want to apply the security policy on the target system upon deployment.
7. For **Webapp name**, select an web application from the list to associate with the deployed security policy on the target device.
8. To use the settings you specified for steps 4 through 7, click the **Copy to All** button to copy the settings to all other target devices, where possible.
9. Click **Deploy Staged Changeset Now** to deploy the staged changeset you configured or click **Save Staged Changes** to save the staged changeset to deploy at a later time.
   The Staged Changesets table opens. When you deploy the security policy, the system stores it in the **Common** partition of the target device.

◆ **Note**

*When you upgrade an Application Security Manager device, the device detects any invalid ASM attack signature file. The Enterprise Manager system then displays a message indicating that the signature file is out of date. To clear this message and finalize the upgrade, you can update the ASM attack signature file. For information about how to update ASM attack signatures, see **Viewing installation task progress**, on page 5-16.*

Managing ASM attack signatures for Application Security Manager

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

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

With Enterprise Manager, you can import system-supplied ASM 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 ASM attack signatures and import them into the image list automatically. Once you obtain the signature updates, you can deploy them to your managed BIG-IP Application Security Manager devices.

◆ **Important**

For the security policies to work properly, the ASM attack signatures (including custom signatures) must be the same on all systems to which you are deploying the security policies.

Obtaining signature updates

As new threats are discovered, F5 regularly updates Application Security Manager ASM attack signature files. You can configure Enterprise Manager to automatically check for, and download, newly updated ASM attack signature definitions for images stored in the image repository. This feature helps you avoid performing unnecessary and potentially frequent manual checks for updated ASM attack signature files.

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 ASM attack signature images manually*, on page 11-5, for instructions about manually updating ASM attack signature images.

◆ **Important**

Enterprise Manager checks for updated ASM attack signature files from ***downloads.f5.com****. For the system to communicate with the F5 servers, you must configure the Enterprise Manager system settings to use your network DNS server.*

Updating ASM attack signature images automatically

If updated signatures are available for any ASM attack signature in the software repository, you can schedule automatic update downloads. Then, after you download the updates, you can start an Application Security Manager ASM attack signature installation task to upgrade managed BIG-IP Application Security Manager systems. See *Installing attack signatures to one or more devices*, on page 11-7, for more information.

To schedule automatic ASM attack signature file downloads

1. On the Main tab, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens.
2. On the menu bar, click **Schedules** and select **Attack Signature Updates**.
3. From the **Check for Updates** list, select an update option for the ASM attack signature images.
   - **Never**: Enterprise Manager does not automatically check for updated ASM 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 options 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 ASM attack signature images in the repository.
5. If you want Enterprise Manager to instantly download new images to the repository, select the **Automatically Download New Updates** check box.
6. Click **Save Changes**.

Updating ASM attack signature images manually

If you choose not to automatically download updated ASM attack signature images, you can configure the system to trigger an alert when it finds new Application Security Manager signature updates. This alert is enabled by default, but you must specify the action you want the system to take if the alert is triggered. See *Creating alerts for Enterprise Manager*, on page 8-6, for instructions.

If you receive an alert to check for updates, or if you want to periodically check for updates, you can update all ASM 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, expand **Enterprise Management**, click **Repository** and select **ASM Attack Signature List**.
2. Above the list, click the **Check for New Signatures** button.
   The Check for New Signatures screen opens and displays the status of the check for new signatures task.

The screen refreshes at regular intervals as the system checks for available updates for the signature files listed in the Available ASM Attack Signatures section. After the task completes, the system indicates whether an update is available for the signature files in the repository.

To download updates for attack signature images

Before you manually download ASM attack signature images, you must have previously checked for updated attack signatures.

1. On the Main tab, expand **Enterprise Management**, click **Repository** and select **ASM Attack Signature List**.
2. Above the list, click the **Import** button.
   The Import ASM Attack Signature File screen opens.
3. Click the **Browse** button to browse to the location of the ASM Attack Signature file.
4. Click the **Import** button.
   An import status indicator appears, displaying information about the packages as they are downloaded to the image repository.

The screen refreshes at regular intervals until the system updates all of the ASM 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 ***Managing ASM attack signatures for Application Security Manager****, on page 11-4, 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 ASM Attack Signature Installation wizard to create an Application Security Manager attack signature installation task. An ***ASM 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, expand **Enterprise Management**, and click **Tasks**.
   The Task List screen opens, displaying all running and completed tasks.

2. Click the **New Task** button.
   The New Task screen opens.

3. For the **Application Security** setting, select **Install Attack Signature**.

4. Click the **Next** button.
   The Install ASM Attack Signature wizard opens.

   Continue working through the wizard screens, as described in the following pages, to install attack signatures on selected devices.

◆ **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 and managing software images****, on page 5-5.*

To select an ASM attack signature to install

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

1. From the **Product Version** list, select the product version associated with the signature that you are planning to install.
   The attack signatures table changes to display signatures compatible with the software version you selected.

2. In the Attack Signature table, select the check box next to each attack signature that you want to install.

3. Click the **Next** button.

To select target devices

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

1. From the **Device List**, specify the types of devices displayed.
    - To view devices belonging to a particular device list, select the device list name.
    - To view all compatible devices, select **All Device**s.

    The Compatible Devices table changes according to the option you select.
2. From the **Device Filter** list, further narrow the managed devices displayed.
    - **Compatible Devices In Standby Mode**: displays all managed devices on which you can install the selected ASM 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, select the check box next to the devices on which you want to install the ASM attack signature.
4. Click the **Next** button to move to the Step 3 of 4 screen.

To set task options

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

1. From the **Device Error Behavior** list, select the action you want the system to take if an error occurs during installation.
    - **Continue task on remaining devices:** The system continues installing the ASM attack signature for selected devices on which an error was not encountered, until the task is finished.
    - **Cancel task on remaining devices:** The system immediately stops the task if an error occurs, and does not install the ASM attack signature on any devices still pending.
2. Click the **Next** button to move to the Step 4 of 4 screen.

To review task details and initiate task

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

1. To change the task name, in the **Task Name** field, type a new name. This name appears in the task list while the task is running, and after the task finishes.
2. Review the information in the Task Summary area.

3. To make changes, click the **Back** button, and navigate to the screen that contains the options you want to change.
4. To start installation task, click the **Start Task** button.
   The Task Properties screen opens, displaying details relevant to the task that you configured.

Glossary

administrative partition

An administrative partition is logical containers with a defined set of BIG-IP system objects, and are used for access control purposes.

attack signature

Attack signatures are the foundation of the BIG-IP® Application Security Manager™ system'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. The attack signature definitions are stored in the Enterprise Manager™ software image repository.

base registration key

A base registration key is a 33-character string that lets the license server know which F5 products you are entitled to license.

big3d agent

See *Data Collection Agent*.

boot location

A boot location is a portion of a drive with adequate space required for a software installation. This was previously referred to 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 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 configurations.

configuration template

A configuration template is a configuration management tool that uses existing changesets to create a model device configuration framework for creating new changesets.

Configuration utility

The Configuration utility is the browser-based application that you use to configure the BIG-IP system.

Data Collection Agent

The Enterprise Manager system uses its Data Collection Agent to gather statistic information from managed devices.

dependency

A dependency indicates additional network object data or resource required for the primary network object to function correctly.

Device list

The Device list catalogs all devices that Enterprise Manager remotely manages. Adding devices to the Device list is the first step in centrally managing the devices in the network.

discovery

Discovery is the process by which the Enterprise Manager successfully logs on to available devices with an administrator user name and password that you supply. Enterprise Manager adds discovered devices to the Device List screen.

failover

Failover is the process in which a standby unit in a redundant system configuration takes over when a software or hardware failure is detected on the active unit. See also *redundant system configuration*.

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.

Logical Volume Management (LVM)

Logical Volume Management is a hardware virtualization tool that dynamically adds virtual storage space to the operating system. See also, *volume*.

maintenance mode

Maintenance mode is a device state in which communications between Enterprise Manager and the managed device are suspended, so that you do not receive unnecessary alerts or configure tasks for the device when you know it is offline.

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 template or changeset. See also *object instance*.

object instance

An object instance is the specific network object that you want to include in the template or changeset. See also *object class*.

partition

A partition is a logical division of storage space on a hard disk, containing a defined set of BIG-IP system objects. You use partitions to control user access to the BIG-IP system.

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 configuration

A redundant system configuration is a pair of BIG-IP systems configured for failover. In a redundant system configuration, 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 that Enterprise Manager creates at a regularly-scheduled interval. See also *user configuration set (UCS)*.

security policy changeset deployment task

A security policy changeset deployment task is a series of tasks that you configure to stage and deploy a security policy on one or more managed Application Security Manager devices.

SNAT (Secure Network Address Translation)

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. You configure a SNAT on a BIG-IP system.

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 task 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 utility

The **syslog-ng** utility is an enhanced version of the standard UNIX and Linux logging utility, **syslog**. Enterprise Manager uses this utility to log system events.

system certificates

System certificates are the web certificates that allow client systems to log into the BIG-IP system Configuration utility.

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 UCS is a backup file that you create for 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*.

volumes

A volume is a specific section of a hard drive that can hold a complete version of software.

warm backup

A warm backup a system that duplicates the configuration information of its peer device, and performs all of the functions of its peer. A warm backup requires manual intervention to maintain the integrity of the backup configuration information.

Index