# Enterprise Manager™ Getting Started Guide

Version 2.3

IT agility. Your way.

# Table of Contents

## Table of Contents

# Legal Notices

## Publication Date

This document was published on November 28, 2011.

## Publication Number

MAN-0384-00

## 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.

## 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 Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

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

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

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

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

This product includes software developed by Jared Minch.

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

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

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

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

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

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

This product includes Hypersonic SQL.

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

This product includes software developed by the Internet Software Consortium.

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

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

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes the GeoPoint Database developed by Quova, Inc. and its contributors.

This software incorporates JFreeChart, ©2000-2007 by Object Refinery Limited and Contributors.

This product contains software developed by the Mojarra project. Source code for the Mojarra software may be obtained at https://javaserverfaces.dev.java.net/.

# Chapter 1

# Enterprise Manager Overview

**Topics:**

# Overview of Enterprise Manager

Enterprise Manager™ is an appliance that helps you streamline the administrative tasks associated with managing multiple network devices. These administrative tasks include: performance monitoring, software installation and upgrades, configuration archival and restoration, certificate monitoring, security policy management, software image storage, and user account management.

Enterprise Manager is robust and flexible, and works in many types of network topologies, including those in multi-tiered configurations containing multiple firewalls. You can use Enterprise Manager to manage networks with devices running the following software.

- BIG-IP® system version 9.3 and later
- BIG-IP® Local Traffic Manager™ Virtual Edition (VE) version 10.2 and later
- BIG-IP® Secure Access Manager™ version 8.0 and later
- WANJet® version 5.0 and later
- Enterprise Manager™ version 1.0 and later

***Note:*** *Although Enterprise Manager works with previous software releases, we recommend that you upgrade your managed devices to the current software version to ensure optimal performance.*

## About Enterprise Manager documentation

You can access all of the following Enterprise Manager™ documentation from the AskF5™ Knowledge Base located at `http://support.f5.com/`. Procedures and examples described in all documentation and online help are written for administrator-level users with full access (non-restricted) privileges to Enterprise Manager.

| Document | Description |
|---|---|
| *Enterprise Manager™ Getting Started Guide* | This guide provides you with the basic concepts and tasks required to set up your Enterprise Manager and start managing devices. |
| *Enterprise Manager™ Administrator Guide* | This guide includes more in-depth information about the basic concepts of device management and configuration options. |
| *Enterprise Manager™ New Features Guide* | This guide introduces you to new features included in the latest release of Enterprise Manager. |
| Enterprise Manager 3000, and Platform Guide: Enterprise Manager™ 4000 | These guides include Enterprise Manager system hardware platform specifications, installation instructions, and important environmental warnings. |
| *BIG-IP® Systems: Getting Started Guide* | This guide contains specific information required to install and license BIG-IP systems. |
| *TMOS® Management Guide for BIG-IP® Systems* | This guide provides you with the information you need to configure VLANs, SNMP traps, redundant BIG-IP systems, BIG-IP system logging features, and so on. |
| Release notes | Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues and available workarounds, as well as installation and upgrade instructions. |

| Document | Description |
|---|---|
| Solutions and Tech Notes | Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information. |

## Understanding how to incorporate Enterprise Manager into your network

You incorporate Enterprise Manager™ into your network as you would any F5 Networks device. However, it is important to keep in mind that Enterprise Manager requires bilateral communication with each device for successful management. Therefore, you must select a network configuration option that ensures Enterprise Manager has open communication with your devices and is able to translate a device's IP address into an address it can use.

The most common network configurations for address translation are:

**Tiered network, BIG-IP® Local Traffic Manager™ performs address translation**
A tiered network configuration where a BIG-IP Local Traffic Manager system (or a non-F5 device) manages load balances requests for multiple devices and translates the IP addresses for those devices through a firewall.

**Tiered network, a SNAT performs network translation**
A tiered network configuration where a BIG-IP Local Traffic Manager (located in front of Enterprise Manager) load balance requests for multiple devices, and a SNAT translates the IP addresses for those devices.

***Tip:*** *Place the Enterprise Manager system on a management subnet that is separate from traffic management to keep device management and communication independent from traffic management activities.*

## About interfaces used for communication

Enterprise Manager™ communicates with devices in your network through the following physical ports, also called *interfaces*.

**Management (MGMT) interface**
F5 devices use the *management (MGMT) interface* port exclusively for administrative traffic and do not forward user application traffic, such as traffic slated for load balancing, through this interface.

**TMM switch interface**
F5 devices typically use the *TMM switch interface* only to send or receive application traffic for load balancing; however, it can be used for communication between Enterprise Manager and a managed device. If you choose to dedicate a TMM switch interface for management communication, do not use that same interface for managing traffic.

## Ports required for two-way communication

For Enterprise Manager™ to properly manage devices, the ports in this list are open by default to facilitate two-way communication.

| Open port | Used for | Purpose |
|---|---|---|
| 443 | Communication between managed devices and the Enterprise Manager system | Device management |
| 4353 | Communication between Enterprise Manager and a managed device's big3d agent | Collecting statistics |
| 3306 | Communication between Enterprise Manager and a remote statistics database | Storing and reporting statistics on a remote database |

## About device management through the management (MGMT) interface

When you use the management (MGMT) interface for enterprise management communication, you do not have to dedicate a TMM switch interface for device management, and less configuration is required when you add new devices on the same subnet. Using the management interface on Enterprise Manager and managed devices for communication is preferable.

***Attention:*** *The only exception is for high availability configurations. Peer devices in a high availability configuration must use a floating self IP address to communicate with the active device. If you have a high availability configuration, use the TMM switch port on each device because it can support floating self IP addresses.*

## About device management through the TMM switch interface

Although typically used to send or receive application traffic for load balancing, you can use a dedicated TMM switch port for communication between Enterprise Manager ™and managed devices. However, if you use the TMM switch interface on managed devices, you cannot use it for managing traffic, because Enterprise Manager sends software upgrades to the managed device on this interface.

Use the TMM switch interface option for device management if have a high availability system configuration (for both static and floating self IP address support).

# Chapter 2

# Initial Setup and Configuration

**Topics:**

# Overview of initial setup tasks

After you configure one or more F5 devices in your network and determine how you want to incorporate Enterprise Manager™, you can perform specific tasks to complete the initial setup of your Enterprise Manager.

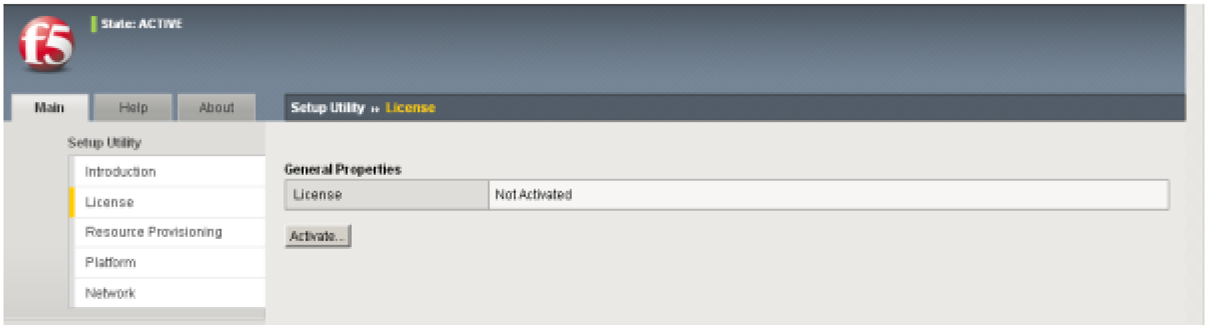
### Task summary

*Activating the Enterprise Manager license*
*Specifying initial configuration settings*
*Configuring a basic network*

## Activating the Enterprise Manager license

To activate the Enterprise Manager license, you must have the base registration key. The *base registration key* is a character string that the license server uses to verify the type and number of F5 Networks products that you are entitled to license. If you do not have a base registration key, contact the F5 Networks sales group (`http://www.f5.com`).

You license the Enterprise Manager from the License screen of the Setup Utility.



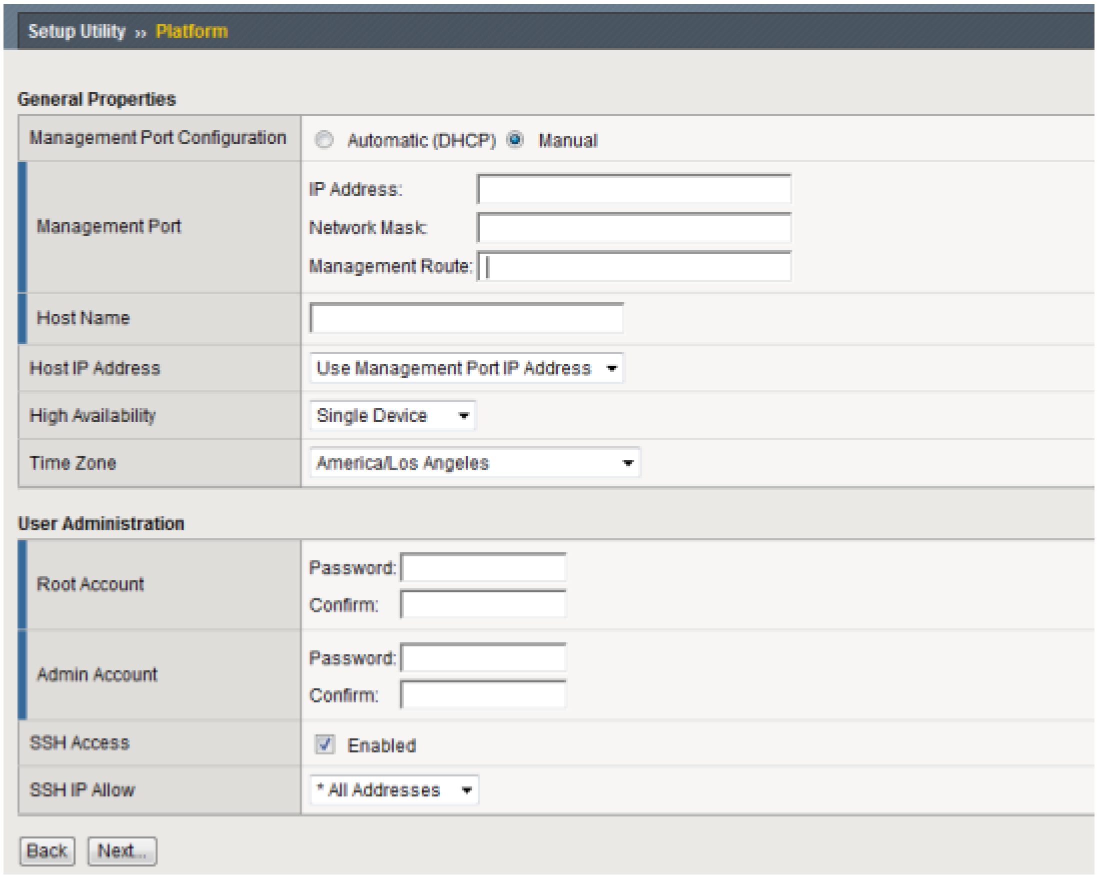
| | |
|---|---|
| License | Not Activated |

**Figure 1: Setup Utility License screen**

1. From a workstation attached to the network on which you configured the management interface, type the following URL syntax where `<management_IP_address>` is the address you configured for device management:
   `https://<management_IP_address>`
2. At the prompts, type the user name `admin` and the password `admin`.
3. Click **Log in**.
   The Setup Utility screen opens.
4. Click **Activate**.
   The License screen opens.
5. In the **Base Registration Key** field, paste your base registration key.
6. Click **Next**.
   The End User License Agreement (EULA) displays.
7. Review the EULA.
   When you click **Accept**, the Platform screen opens.

## Specifying initial configuration settings

You specify the initial configuration settings from the Setup Utility Platform screen.



Setup Utility » Platform

General Properties

| | |
|---|---|
| Management Port Configuration | ○ Automatic (DHCP) ● Manual |
| Management Port | IP Address:<br>Network Mask:<br>Management Route: |
| Host Name | |
| Host IP Address | Use Management Port IP Address |
| High Availability | Single Device |
| Time Zone | America/Los Angeles |

User Administration

| | |
|---|---|
| Root Account | Password:<br>Confirm: |
| Admin Account | Password:<br>Confirm: |
| SSH Access | ☑ Enabled |
| SSH IP Allow | * All Addresses |

**Figure 2: Setup Utility's Platform screen for basic configuration settings**

1. For the **Management Port Configuration** setting, select **Manual**.
2. For the **Management Port** setting, type the IP address, network mask, and the management route.
3. In the **Host Name** field, type a fully-qualified domain name (FQDN) for the system.

   The FQDN can consist of letters, numbers, and/or the characters underscore ( _ ), dash ( - ), or period ( . ).
4. For the **Host IP Address** setting, retain the default value of **Use Management Port IP Address**.
5. For the **High Availability** setting, select an option.

   Keep in mind that the function of Enterprise Manager's high availability feature is different than that of a BIG-IP® system. The purpose of Enterprise Manager's high availability feature is to provide access to a current backup of the active Enterprise Manager system's configuration.
6. From the **Time Zone** list, select a time zone that reflects the location of the Enterprise Manager system.
7. For the **Root Account** setting, type and confirm a password for the `root` account.

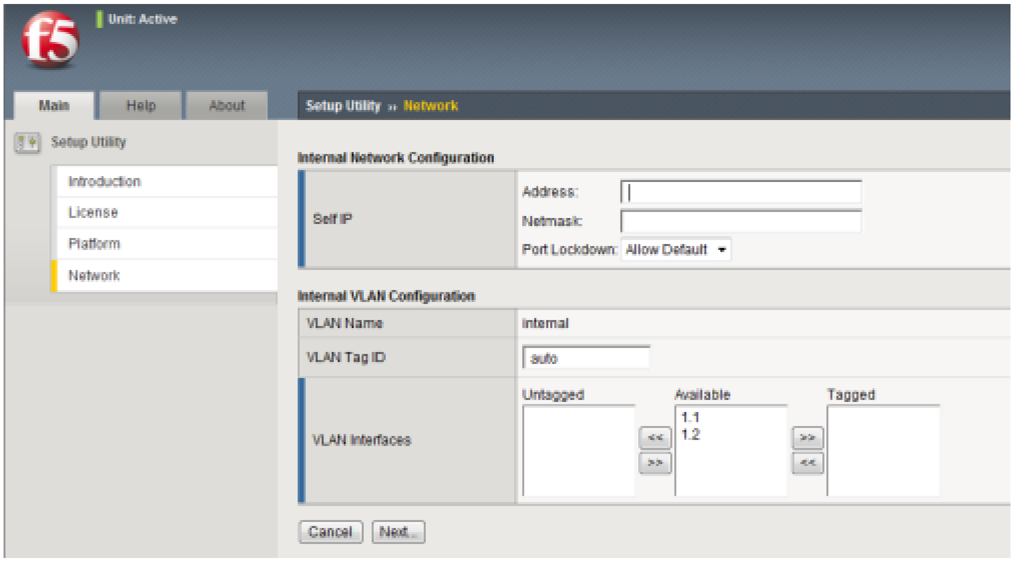
   The `root` account provides console access only.
8. For the **Admin Account** setting, type and confirm a password.
9. For the **SSH Access** setting, select or clear the check box.

10. For the **SSH IP Allow** setting, retain the default of ***All Addresses**, or specify a range.
11. Click **Next**.
    The system terminates your login session.
12. Log in to the system again using the new password that you specified.
    The Network screen opens.

> ***Tip:*** *If you need to reconfigure any of the basic configuration settings, you can click the* ***Run the Setup Utility*** *link from the Configuration utility's Welcome screen.*

## Configuring a basic network

When you click **Next** from the Platform screen, the Basic Network Configuration wizard screen opens.



Internal Network Configuration

| | |
|---|---|
| Self IP | Address: <br> Netmask: <br> Port Lockdown: Allow Default |

Internal VLAN Configuration

| | |
|---|---|
| VLAN Name | internal |
| VLAN Tag ID | auto |
| VLAN Interfaces | Untagged: <br> Available: 1.1, 1.2 <br> Tagged: |

**Figure 3: Basic Network Configuration wizard (Network screen)**

Perform these steps to continue through the Basic Network Configuration wizard screens and specify the settings for the internal and external VLANs. For additional information about the settings on these screens, click the Help tab.

1. For the **Self IP** settings, type the IP addresses specific to the Enterprise Manager™ system in the **Address** and **Netmask** fields.
2. For the **Port Lockdown** setting, retain the default**Allow Default** to ensure that the required ports are open for communication between the Enterprise Manager and the managed devices.
3. If you are configuring a high availability system, perform these steps, which display only if you specified a high availability system during the initial configuration.
    a) In the Floating IP area, type the Enterprise Manager's floating IP address in the **Address** field.
    b) To enable configuration synchronization between the peers in a redundant/high availability system, leave the **Port Lockdown** setting at **Allow Default**.

       If you select any other option, the configuration synchronization process will fail.
4. For the **VLAN Tag ID** setting, retain the default **auto** to allow Enterprise Manager to select one for you, or type a value in the field between 1 and 4094.

5. For the **VLAN Interfaces** settings, you can specify the interfaces you want this VLAN to use for traffic management.
6. Click **Next**.
   The screen refreshes to display the external VLAN options.
7. For the **Self IP** settings, in the **Address** and **Netmask** fields, type the IP addresses specific to the Enterprise Manager system.
8. For the **Port Lockdown** setting, retain the default **Allow Default** to ensure that the ports that are required for communication between managed devices and Enterprise Manager are open.
9. In the **Default Gateway** field, type the IP address or route of the default gateway.
10. Click **Next** to save the configuration.

# Chapter 3

## Device Discovery and Importation

**Topics:**

# Overview of device discovery and device importation

Before you can use Enterprise Manager™ to manage devices in your network, you must add the devices. For BIG-IP® devices in your network, you can use the discovery method to search specific IP addresses or IP subnets in your network, and add those devices to Enterprise Manager. During the *discovery* process, Enterprise Manager attempts to log on to available devices with an administrator user name and password that you supply. If Enterprise Manager succeeds in logging on to devices that it discovers, it adds those devices to the list on the Device List screen.

For non-BIG-IP devices, such as WANJet® systems, you create a `.csv` file to import the devices and then discover them.

## Discovering BIG-IP devices

After you license and perform initial configuration for Enterprise Manager™, you can discover BIG-IP® devices in your network.

***Note:*** *For non-BIG-IP devices, such as WANJet®systems, you must import the devices before performing the discovery task.*

Discovering devices is the first step toward central device management.

***Important:*** *To successfully discover devices and receive the user name and password combination, the device must have an active SSL server listening for traffic on port* `443`.

1. On the Main tab, click **Enterprise Management** > **Devices**.
   The Device List screen opens.
2. Click the **Discover** button located on the upper right-side of the screen.
   The Discover Device(s) screen opens.
3. For the **Scan Type** setting, select one of the following options:
   - **Address List**
   - **Subnet**

   The screen refreshes to display settings specific to the selected option.
4. If you selected the **Address List** option, perform the following steps:
   a) In the **User Name** and **Password** fields, type a user name and password to use to log on to the discovered device.
   b) Click **Add**.
5. If you selected the **Subnet**, option perform the following steps:
   a) In the **IP Address** field, type the device IP address.
   b) In the **Network Mask** field, type the netmask that you want Enterprise Manager to use when searching the network.

      You can search by class B or C network.
   c) In the **User Name** and **Password** fields, type a user name and password to use to log on to each device discovered in the subnet.
6. Click the **Discover** button.

The Task Properties screen opens and discovered devices appear below the Properties area. The list refreshes until all specified devices are discovered, or until you click **Cancel Pending Items**.

## Importing non-BIG-IP devices

For non-BIG-IP® devices, such as WANJet® systems, you must create a comma-separated value (CSV) file on your local system and import the file into the device list.

1. Create a .csv file on your local system that contains each non-BIG-IP device's IP address, user name, and password on a separate line in the following format: `<device IP address>, <username>, <password>`
   For example:

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

2. On the Main tab, click **Enterprise Management** > **Devices**.
   The Device List screen opens.
3. Click the **Discover** button located on the upper right-side of the screen.
   The Discover Device(s) screen opens.
4. Click the **Import From File** button.
   The Import Address List screen opens.
5. Click **Browse**.
6. Browse to the location of the `.csv` file you created for the non-BIG-IP devices, and click **Open**.
   The path and file name display in the **File Name** field.
7. Click **Import**.
   The screen refreshes to display the import status. When the importation finishes, the Device Discover screen opens and a list of imported IP addresses and user names appears in the **Address List** field.
8. Click **Start Task** to add the devices in the **Address List** field to the device list.

# Chapter 4

## Optional Configuration

**Topics:**

# Overview of configuration customization options

After you activate the license, complete the initial setup, and specify your network configuration options, you can customize settings for other Enterprise Manager™ features.

**Customizable features:**

## About UCS archive storage

A benefit of using Enterprise Manager is the ability to store, or archive, the user configuration set (UCS) for each managed device in your network. A *UCS archive* is a compressed file that contains all of the information required to restore a managed device's configuration, and consists of:

- System-specific configuration files
- License
- User account and password information
- DNS zone files
- NameSurfer configuration
- SSL certificates and keys

Each time you create a new configuration for a device, Enterprise Manager also creates a UCS archive of that configuration. You can also create and store UCS archives for managed devices on demand. These UCS archives are referred to as *pinned* and are saved until you delete them. The third option is to create a task to save UCS archives on a specified schedule. These archives are called *rotating archives*.

Enterprise Manager saves multiple archives and cycles out the oldest UCS archive when it saves a new one. By default, Enterprise Manager stores ten rotating and ten pinned UCS archives in its database.

It is best practice to create a rotating UCS archive schedule so that you always have a copy of the most recent configuration for any given device. When Enterprise Manager is prompted to store a UCS archive on a schedule, it compares the UCS archive file to the current configuration at the specified interval. If there are any differences, Enterprise Manager stores a copy of the current configuration. If there are no differences, Enterprise Manager does not create an additional copy of the current configuration.

***Note:*** *For additional information about UCS archive features, including information specific to pinned archives and instructions about changing the default number of archives saved, see the Enterprise Manager™ Administrator Guide.*

### Creating a rotating UCS archive schedule

The benefit of creating a scheduled rotating archive is that you always have the current configurations stored for your devices without storing duplicate archives. This leaves you room to store a higher number of historical UCS archive files.

1. On the Main tab, click **Enterprise Management** > **Tasks** > **Schedules** > **Archive Collection**.
   The Archive Collection screen opens.
2. Click the **Create** button.
3. In the **Archive File Name** field, type a name for the rotating archive schedule.
4. From the **Check for Changes** list, select the frequency that you want Enterprise Manager to check the configurations of your managed devices.

Depending on your selection, the screen refreshes to display associated options.

5. Specify the day of the week or month, and the time of day that you want Enterprise Manager to check for device configuration changes.
6. From the **Private Keys** list, select an option to include or exclude private SSL keys in the rotating archive.
7. From the **Status** list, select an option to enable or disable the rotating archive schedule after you create it.
8. For the **Devices** or **Devices Lists** setting, in the Available list, select a device or device list and click the **Move** button to move the selected devices or device list to Assigned.
9. Click **Finished** to save the settings.

The Archive Collection list screen opens and the new rotating archive schedule appears in the list. If a device in the Assigned list changes its configuration 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.

### Changing private key archive settings

When Enterprise Manager™ creates a configuration archive, it stores the private keys in an archive by default. If you would prefer not to have the system store the private keys in an archive, you can change this default behavior.

***Important:*** *If you choose not to have Enterprise Manager™ store the private keys when a configuration archive is created, you must manually restore the keys if you restore the archive.*

1. From the Main tab, click **Enterprise Management** > **Options** > **Certificates** > **SSL Private Keys**.
2. From the **Private Keys in Archives** list, select an option:

| Options | Description |
|---|---|
| **Include** | Select this option if you want the system to store private key data when it creates a configuration archive. This is the default setting. |
| **Exclude** | Select this option if you do not want the system to store private key data when it creates a configuration archive. Note that if you select this option, you must manually restore the keys if you restore the archive. |

3. Click **Save Changes**.

## About the health and performance monitoring database

When statistics data collection is enabled, Enterprise Manager™ stores the following information in its statistics database for each managed device on which the Data Collection Agent is installed:

- Specifics about the managed devices, such as host name, IP address, and software version
- Details, such as object type and name, about any enabled network objects associated with a managed device
- Performance and health data for managed devices and associated network objects.

You can use the collected statistics to display standardized reports about the health and performance of managed devices in your network. This helps you identify any systems that are not performing at full capacity and assists you in determining when you should add new devices.

***Important:*** *Enterprise Manager collects statistics only from devices that have BIG-IP® Local Traffic Manager™ 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 start collecting statistics, you must enable the collect statistics data feature and install the Data Collection Agent.

***Note:*** *For additional information about the health and performance monitoring feature, see the Enterprise Manager™ Administrator Guide.*

### Enabling statistics data collection

To collect statistics you must enable data collection, which is disabled by default.

***Important:*** *Due to the processing power required to collect and store statistics data, only Enterprise Manager™ 3000 and 4000 platforms and Enterprise Manager Virtual Edition (VE) support statistics data collection. If you are upgrading from a version of Enterprise Manager that is earlier than 1.7, you must re-license the system before enabling data collection.*

1. On the Main tab, click **Enterprise Management** > **Options** > **Statistics** > **Data Collection**.
2. For the **Collect Statistics Data** setting, select **Enabled**.
3. Click the **Save Changes** button.

When you enable statistics collection, Enterprise Manager verifies that each managed device has a compatible version of the Data Collection Agent installed.

### Installing the Data Collection Agent

When data collection is enabled, Enterprise Manager™ collects health and performance monitoring statistics data for each managed device in your network on which the most current version of the Data Collection Agent is installed. If a device on which statistics is enabled requires a more recent version of the Data Collection Agent, Enterprise Manager displays that device as **Impaired** in the device list, and indicates that an upgrade is required.

You can use the Data Collection Agent Installation wizard to update and install the Data Collection Agent.

1. On the Main tab, click **Enterprise Management** > **Tasks** > **Task List**.
2. Click the **New Task** button.
3. For the **Software Installation** setting, click **Install Data Collection Agent**, and then click **Next**.
   The Data Collection Agent Installation screen opens.
4. For the **Device Filter** setting, click the **Devices with data collection enabled requiring update** option.
   The screen refreshes to display the devices that require an update.
5. Select the check box next to each device on which you want to install the most recent version of the Data Collection Agent, and click **Next**.
   The Task Options screen opens.
6. From the **Configuration Archive** list, select an option to include or exclude private SSL keys in the configuration archive.
7. From the **Device Error Behavior** list, select an option to specify how you want the system to proceed if an error occurs during the Data Collection Agent installation task.
8. Click **Next**.
   The Task Review screen opens.

9. In the **Task Name** field, you can type a new name to customize the name that displays in the task list.
10. Click the **Start Task** button.
    The Task Properties screen opens, displaying the progress of the task. The task progress displays as Finished when the Data Collection Agent is installed.

Enterprise Manager starts collecting and storing health and performance monitoring statistics for the devices on which data collection is enabled and the Data Collection Agent is installed.

## About the startup screen

Each time you log on to Enterprise Manager™ a startup screen displays. By default, the startup screen is the Welcome screen, but you have the option to change this screen if you find an alternative screen more useful.

### Changing the default startup screen

To change the default screen, perform these steps.

1. On the Main tab, click **System** > **Preferences**.
2. From the **Start Screen** list, select the default screen that you want displayed at startup.

### Default startup screen options

You can use this table to determine which screens are most relevant to your needs.

| Default startup screen option | Description | To access |
|---|---|---|
| Welcome | Contains links to setup, support, plug-ins, and additional downloads. | Click **Overview** and **Welcome**. |
| Performance | Displays statistics related to the Enterprise Manager system performance. | Click **Overview** and **Performance**. |
| Device List | Displays a list of all of the devices you are managing with Enterprise Manager. | Click **Enterprise Management** and **Devices**. |
| Task List | Displays a list of running and completed tasks. | Click **Enterprise Management** and **Tasks**. |
| Device Statistics | Displays a summary of statistics graphs for all managed devices. | Click **Enterprise Management**, **Statistics**, and **View**. |
| Custom Lists | Displays a customizable list of objects. | Click **Enterprise Management** and **Custom Lists**. |

## About alert management

You can configure Enterprise Manager™ to manage alerts in these ways:

- Send SNMP traps to a remote SNMP server
- Send email alerts to a specific recipient

*Simple Network Management Protocol (SNMP)* is an industry-standard protocol that gives an SNMP management system the ability to remotely manage a device on your network. You have the option to configure alerts that prompt Enterprise Manager™ to send SNMP traps to a remote SNMP server.

To send SNMP traps in this manner, you provide the SNMP agent and SNMP client access to the Enterprise Management system. As Enterprise Manager system shares the same operating system as a BIG-IP® system, you can configure SNMP on the Enterprise Manager system in the same way that you do on a BIG-IP system. For detailed information about how to configure SNMP traps, see the *TMOS® Management Guide for BIG-IP® Systems*. The SNMP versions that the Enterprise Manager system supports are: SNMP v1, SNMP v2c, and SNMP v3.

If you want to have a specific recipient receive an email message when an alert is triggered, you must complete specific tasks so that Enterprise Manager™ can deliver locally generated email messages.

***Attention:***

*To perform the specific tasks, you must have administrator privileges with root access for the Configuration utility.*

#### Task summary:

### Verifying that the postfix service is enabled

Use this procedure to confirm that the postfix mail server service is enabled.

1. On the Main tab, click **System** > **Services**.
   The Services List screen opens.
2. Locate the postfix service in the list.
3. Verify that postfix is running by viewing the History column.
4. If postfix is not running, select the check box next to **postfix** and click the **Start** button.

### Specifying the IP address of your DNS server

Enterprise Manager™ must specify the IP address of your DNS server in order to set up and send an email alert.

1. On the Main tab, click **System** > **Configuration** > **Device** > **DNS**.
2. In the DNS Lookup Server List area, in the **Address** field, type the IP address of your DNS server(s).
3. Click the **Add** button.
4. Click **Update** to save the changes.

### Verifying DNS resolution

After you specify the IP address of your DNS server, you can verify that the address properly resolves.

1. Log in as `root` at the command line.
2. Type the following command: `dig <domain>`
   For example, to query `MX` and `siterequest.com`, you would type `dig siterequest.com mx`. The result to this query should appear similar to this example, indicating that Enterprise Manager™ is able to resolve the email exchanger.

```
; << >> DiG 9.2.2 << >> siterequest.com mx
                ;; global options:  printcmd
                ;; Got answer:
                ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
16174
                ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY:
0, ADDITIONAL: 0
```

```
                ;; QUESTION SECTION:
                ;siterequest.com.                     IN      MX
;; ANSWER SECTION:
siterequest.com.              86400   IN      MX      10
mail.siterequest.com.
;; Query time: 65 msec
;; SERVER: 172.16.100.1#53(172.16.100.1)
;; WHEN: Mon Nov  8 14:32:07 2011
;; MSG SIZE  rcvd: 51
```

### Specifying alert defaults

It is important to specify default behavior for alerts before you enable the alert options.

1. On the Main tab, click **Enterprise Management** > **Options** > **Alerts**.
2. In the **Email Recipient** field, type the email address of the user, or the alias, that you want to Enterprise Manager™ to send the alert to by default.
3. If you want to log alert events to a syslog file:
   a) In the **Syslog Server Address** field, type the IP address of the remote server where you want to store alert event logs.
   b) In the **Maximum History Entries** field, type the maximum number of alerts that you want stored in the syslog file.

      If the alert history reaches the limit you set, Enterprise Manager deletes the oldest entries to create room for newer entries.
4. Click **Save Changes**.

### About modifications for email alerts

The postfix mail server is initiated by default when you start Enterprise Manager™. You can, however, customize the configuration for email notification from the Enterprise Manager system's command line.

### Modifying the postfix configuration file for email notification

You can modify the postfix configuration file to specify variables required for your email domain, host, and interface.

1. Using a text editor, such as vi or pico, edit the configuration file: `/etc/postfix/main.cf`.
2. Find the variable *mydomain*, and change it to specify the domain for your site. For example, for domain `siterequest.com` you would type the following command:
   `mydomain = siterequest.com.`
3. Set the *relayhost* variable as in the following example.
   `relayhost = $mydomain`
4. If you want only the local host to send email, set the *inet_interfaces* variable to local host by typing the following command:
   `inet_interfaces = localhost`
5. Save and exit the file.

### Specifying a mailserver domain

After you modify the postfix configuration file, you can then specify your mailserver domain name in the hosts files.

You need to perform several steps from the command line in order to specify the mailserver domain and configure your email alert.

1. Using a text editor, such as vi or pico, edit the `/etc/hosts` file.
2. Create a record for the fully qualified domain name (FQDN) of your mail server by typing the following command: `echo "<yourmailserver_IP_address> <your_mailserver_fqdn>" >>` For example: `echo "10.10.65.1 mail.siterequest.com" >> /etc/hosts`
3. Save and exit the file.
4. Send a test email by typing the following command: `echo test | mail <your email address>`
5. View the email queue by typing the following command: `mailq`
6. To send any unsent email, type the following command: `postfix flush`
7. In the `/etc/postfix/aliases` file, locate the following entry:

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

8. Change the *root* alias to the email account to which you want mail to be sent.
   For example: `root: helpdesk@postfix.fix`
9. Save and exit the file.
10. Type the following command: `newaliases`
11. Send a test email by typing the following command:
    `t>echo test | mail <your email address>`

    If configured properly, the email is delivered to the address that you specified in the `/etc/postfix/aliases` file.
12. Type the `service postfix restart` command and press Enter.

## Understanding user roles

Enterprise Manager™ classifies the permissions for the user roles as either non-restricted or restricted. These user roles are defined as:

| | |
|---|---|
| **Administrator** | This role (non-restricted) can perform all management functions available to Enterprise Manager, including managing other user accounts and roles. |
| **Operator and Application Editor** | By default, these roles (restricted) perform fewer management tasks than the Administrator. You can customize each role by specifying the tasks that the role is allowed to perform. |

### Customizing user role permissions

When you initially set up Enterprise Manager™, you configure a default administrator-level user account that permits you to configure and start working with the system through the web interface. You can use this procedure to customize permissions for users, defining which user role (Operator or Application Editor) can perform specific device management tasks.

1. On the Main tab, click **Enterprise Management** > **Access Control** > **Role Permissions**.
2. For each restricted user role, select or clear the check box next to the permission you want to modify.
3. Click **Apply** to save your changes.

### User role permissions and management tasks

There are eight different types of permissions that you can specify for each restricted user role. You can specify any of these management task permissions to the Operator and Application Editor user roles.

| Permission | Management task |
|---|---|
| Manage Device Configuration Archives | Create and manage UCS archives for all managed devices |
| Browse Device Configurations | View device configuration settings using the Enterprise Manager configuration browser |
| Compare Device Configuration Archives | Compare UCS configuration files between two devices |
| Stage Changesets for Deployment from Published Templates | Create a new staged changeset from a published template |
| Deploy Staged Changesets | Deploy a staged changeset created by the user, or another user |
| Administer Device Lists | Manage device list members |
| Synchronize Device Configuration with Peer | Synchronize peer device configurations |
| Failover Devices | Initiate a failover to a peer managed device |

## Overview of communication settings

Enterprise Manager™ communicates with devices in your network and F5 servers through a secure HTTPS connection. You can also use a proxy server for communication with network devices to download licensing information, support information, or Application Security Manager™attack signature files and an FTP proxy to send support data in a support data collection task.

### Specifying a proxy server for downloading files and information

When you specify a proxy server address, it applies only to tasks configured through Enterprise Manager™ task wizards, such as the Licensing wizard. For example, if you specify a proxy server address and select **License** option from the **System** menu on the Main tab to update the licensing information for a device, Enterprise Manager does not send the licensing information through the proxy. However, if you create a task to update the licensing information for a device instead, Enterprise Manager sends the licensing information through the specified proxy.

1. On the Main tab, click **Enterprise Management** > **Options** > **Proxies**.
2. On the menu bar, click **Options**.
3. In the Internet Proxy area, select the **Use Proxy** check box.
   The screen refreshes, displaying additional options.
4. In the **SSL Proxy Address** field, type the address of the SSL proxy server.
5. If you want to use a separate SSL proxy for FTP connections:
   a) Clear the **Also use this proxy address for FTP protocol** check box.
   b) In the **FTP Proxy Address** field, type the FTP proxy server address.
6. Click **Save Changes**.

### Specifying a proxy server for communication between Enterprise Manager and devices

By default, Enterprise Manager™ communicates with devices through HTTPS. You have the option to specify a proxy server for communication between Enterprise Manager and your network devices.

1. On the Main tab, click **Enterprise Management** > **Options** > **Proxies**.
2. In the Device Proxy area, select the **Use Proxy** check box.
   The screen refreshes, displaying additional options.
3. In the **EM-side SSL Proxy Address** field, type the SSL proxy server address that you want to use for Enterprise Manager.
4. If you want to use the same SSL proxy address for the device side, select the **Also use this proxy address for the device-side connections** check box.
5. To specify a separate device-side SSL proxy address, in the **Device-side SSL Proxy Address** field, type the SSL proxy server address that you want to use for your devices.
6. Click **Save Changes**.

# Index