Platform Guide: 520/540

MAN-0067-00

Product Version

This manual applies to hardware platforms 520 and 540 created by F5 Networks, Inc..

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 herein.

F5 reserves the right to change specifications at any time without notice.

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, GLOBAL-SITE, SEE-IT, EDGE-FX, FireGuard, Internet Control Architecture, and IP Application Switch are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. All other product and company names are registered trademarks or trademarks of their respective holders. F5 trademarks may not be used in connection with any product or service except as permitted in writing by F5.

Patents

This product protected by U.S. Patent 6,374,300; Pending U.S. Patent 20020040400. Other patents pending.

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.

Export 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 generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause 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 I CES-003.

Standards Compliance

The product conforms to ANSI/UL Std 1950 and Certified to CAN/CSA Std. C22.2 No. 950.

Table of Contents

1
Introducing the 520/540 Platform

2
Configuring the FIPS 140 Hardware

3
Additional Hardware Specifications

Glossary

Index

1

Introducing the 520/540 Platform

- Reviewing the 520/540 platform
- Getting started
- Familiarizing yourself with the controller
- Environmental requirements
- Installing and connecting the hardware
- Interfaces
- Activating the license
- Using the Setup utility
- Additional resources

Reviewing the 520/540 platform

The 520 and 540 platforms are powerful systems capable of managing traffic for medium to large enterprises.

Externally, the 520 and 540 platforms look the same (Figure 1.1). However, there are internal differences. The 540 is a dual-processor platform with more memory than the 520 platform. For details, see *Reviewing hardware specifications*, on page 3-1.

Three PCI expansion slots are available on both the 540 and 520. These PCI slots provide the option to add SSL accelerator cards, additional 10/100 network interface cards, or Gigabit Ethernet interfaces.

Figure 1.1 *An example of the 520/540 platform. In this case, a BIG-IP Controller*

Getting started

There are several basic tasks you must complete to get the 520/540 platform installed and set up.

- Review the hardware requirements.
- Familiarize yourself with the controller hardware.
- Review the environmental requirements.
- Connect the controller to the network, and optionally connect the peripheral hardware.
- Activate the license.

The controller comes with the hardware that you need for installation and maintenance. However, you must also provide standard peripheral hardware, such as a keyboard or serial terminal, if you want to administer the controller directly.

Components provided with the controller

When you unpack the controller, you should make sure that the following components, shown in Figure 1.2, are included:

- One power cable
- Four rack-mounting screws
- Documentation and Software CD

If you purchased a hardware-based redundant system, you also received one fail-over cable to connect the two controller units together (network-based redundant systems do not require a fail-over cable).

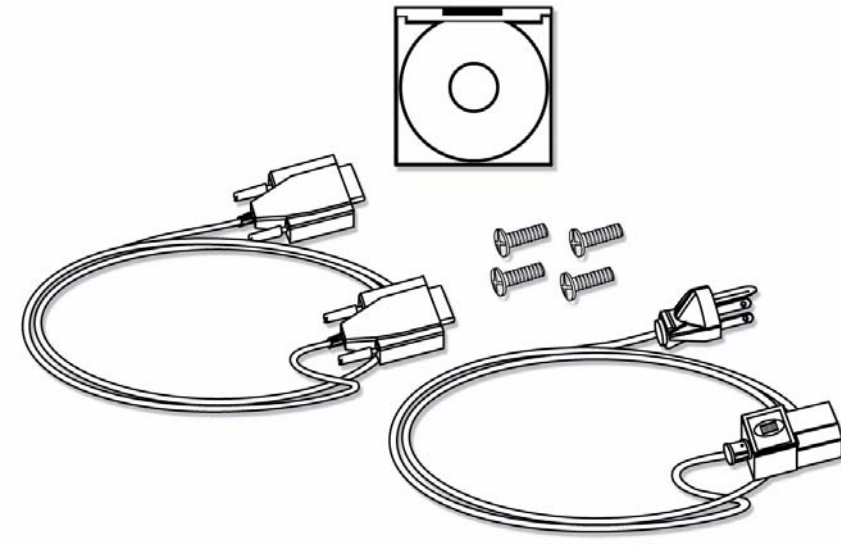


Figure 1.2 *Components included with the controller*

Peripheral hardware that you provide

For each controller in the system, you need to provide the following peripheral hardware:

- If you plan to use direct administrative access to the controller, you need standard input/output hardware. Either of the following options is acceptable:
  - A VGA monitor and PC/AT-compatible keyboard.
  - Optionally, a serial terminal and a null modem cable. For serial terminal configuration information, refer to the ***BIG-IP Reference Guide***, Chapter 3, *Post-Setup Tasks* in the section *Using a serial terminal with the BIG-IP system*.
- If you want to use the default controller configuration, you must have an administrative workstation on the same IP network as the Controller.
- You also need network hubs, switches, or concentrators to connect to the controller network interfaces. The devices you select must be compatible with the network interface cards installed in the controller. The devices can support 10/100 Ethernet or Gigabit Ethernet.
  - Ethernet requires either a 10 Mbps or 100 Mbps hub or switch.
  - Gigabit Ethernet requires a compatible Gigabit Ethernet switch.

If you plan on doing remote administration from your own PC workstation as most users do, we recommend that you have your workstation already in place. Keep in mind that the Setup utility prompts you to enter your workstation's IP address when you set up remote administrative access.

Familiarizing yourself with the controller

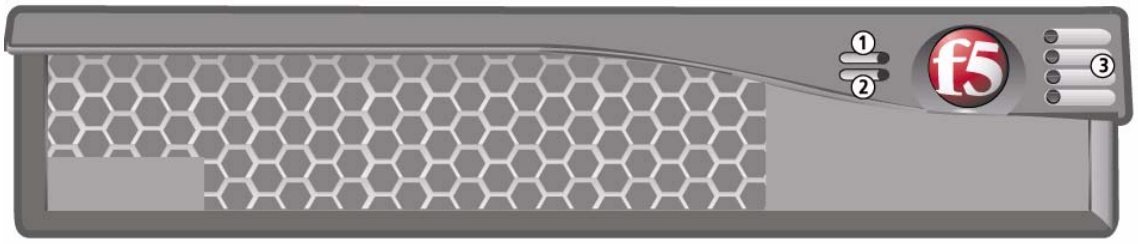
The controller is offered in 520 and 540 hardware configurations. Before you begin to install the controller, you may want to quickly review the following figures that illustrate the controls and ports on both the front and the back of a 520 controller and a 540 controller.

Using the 520/540 hardware

This section describes the front and back layout of a 520/540 controller. Figure 1.3 illustrates the front of a 520/540 controller. On the front of the unit, you can turn the unit off and on, or you can reset the unit. You can also view the indicator lights for hard disk access.

Note

The interfaces on every controller are labeled, so it should be clear what each port is, no matter which hardware configuration you have purchased.



1. Reset button
2. Netboot button
3. Status LEDs

Figure 1.3 Front view of a 520/540 controller

If you have a special hardware configuration, such as one that includes more than two interfaces, the ports on the back of your unit differ slightly from those shown in Figure 1.4, on page 1-6.

Table 1.1 describes the behavior of the LEDs in normal startup and in error conditions.

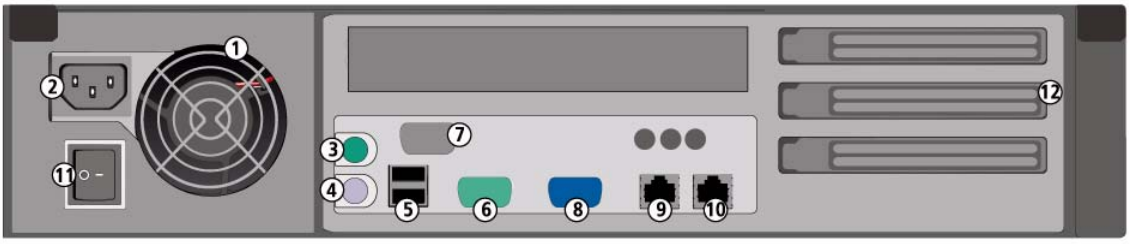
Description	Power LED	Status LED	Activity LED	Alarm LED
Normal Startup:				
Power is off	Black	Black	Black	Black
Starting Up - BIOS	Green	Black	Black	Yellow
Starting Up - Loader	Green	Black	Yellow	Yellow
Starting Up - Kernel	Green	Blink Yellow	Flicker Yellow* for storage device	Yellow
System ready - (standby mode)	Green	Yellow	Flicker Green** for Traffic	Black
System ready - (active mode)	Green	Green	Flicker Green for Traffic	Black
Error Conditions:				
Overtemp or fan failure	Green	Yellow or Green	Flicker Green for Traffic	Blink Red
Out of memory or other serious condition	Green	Yellow or Green	Flicker Green for Traffic	Red
One or more virtual servers have all nodes down	Green	Yellow or Green	Flicker Green for Traffic	Blink Yellow
One or more health monitors failed	Green	Yellow or Green	Flicker Green for Traffic	Yellow
Self Test Failed in Phase 1	Green	Black	Black	Red
Self Test Failed in Phase 2	Green	Black	Black	Black
Self Test Failed in Phase 3	Green	Blink Yellow	Black	Red

*After startup, LED3 never flickers yellow, even though the storage device may be accessed.

**Flicker Green means traffic is being load balanced or routed.

Table 1.1 *Behavior of the status LEDs*

Figure 1.4, following, illustrates the back of a 520/540 controller. Note that all ports are labeled, even those which are not intended to be used. Ports marked with an asterisk (*) in the list following do not need to be connected to any peripheral hardware.



1. Fan	7. Fail-over port
2. Power in	8. Video (VGA) port
3. Mouse port*	9. Net1 interface (1.1)
4. Keyboard port	10. Net2 interface (1.2)
5. Universal serial bus ports*	11. On/off button
6. Serial terminal port	12 PCI expansion slots

**Not to be connected to any peripheral hardware.*

Figure 1.4 *Back view of a 520/540 controller*

Environmental requirements

Before you install the controller, review the following guidelines to make sure that you are installing and using the controller in the appropriate environment.

General guidelines

A controller is an industrial network appliance, designed to be mounted in a standard 19-inch rack. To ensure safe installation and operation of the unit:

- Install the rack according to the manufacturer's instructions, and check the rack for stability before placing equipment in it.
- Build and position the rack so that once you install the controller, the power supply and the vents on both the front and back of the unit remain unobstructed. The controller must have adequate ventilation around the unit at all times.
- Do not allow the air temperature in the room to exceed 40° C.
- Do not plug the unit into a branch circuit shared by more electronic equipment than the circuit is designed to manage safely at one time.

- Verify that the voltage selector is set appropriately before connecting the power cable to the unit.

The unit must be connected to Earth ground, and it should have a reliable ground path maintained at all times.

The controller contains a lithium battery. There is danger of an explosion if you replace the lithium battery incorrectly. We recommend that you replace the battery only with the same type of battery originally installed in the unit, or with an equivalent type recommended by the battery manufacturer. Be sure to discard all used batteries according to the manufacturer's instructions.

This equipment is not intended for operator serviceability. To prevent injury and to preserve the manufacturer's warranty, allow only qualified service personnel to service the equipment.

Guidelines for DC-powered equipment

A DC-powered installation must meet the following requirements:

- Install the unit using a 20 Amp external branch circuit protection device.
- For permanently connected equipment, incorporate a readily accessible disconnect in the fixed wiring.
- Use only copper conductors.

Install DC powered equipment only in restricted access areas, such as dedicated equipment rooms, equipment closets, or similar locations.

Installing and connecting the hardware

There are two basic tasks required to install the hardware. You simply need to install the controller in a rack, and then connect the peripheral hardware and the interfaces.

WARNING

Do not turn on a controller until all peripheral hardware is connected to the unit.

To install the hardware in a rack

1. Lift the unit into place. This requires more than one person.
2. Secure the unit using the four rack-mounting screws that are provided.
   Figure 1.5 shows the orientation of the controller and the mounting screws for installation in a standard 19" rack. Figure 1.6 shows the controller installed in the rack.

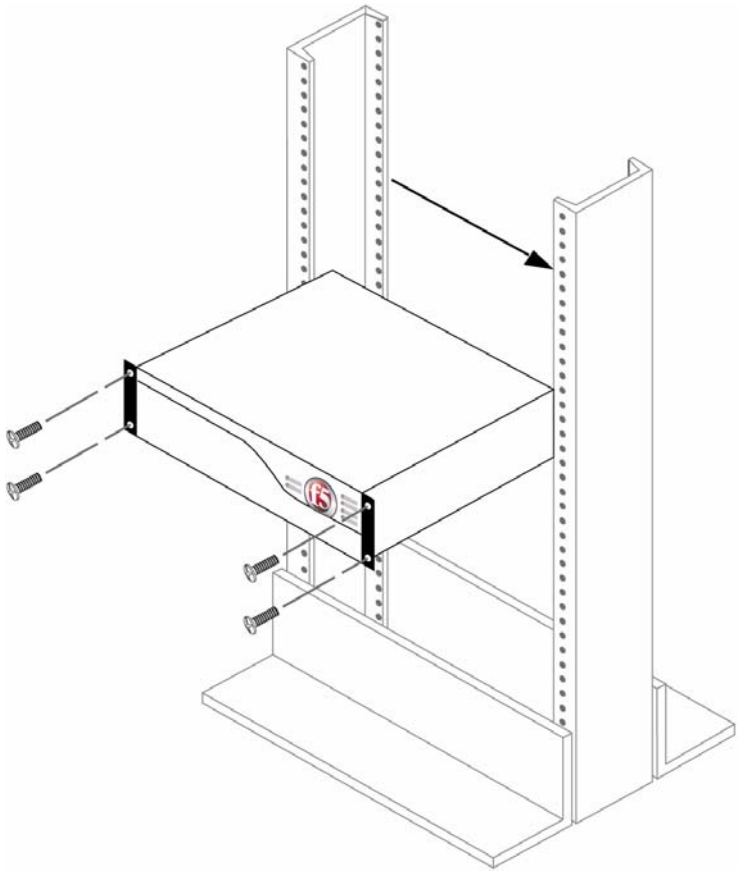


Figure 1.5 *Platform orientation for rack mounting*

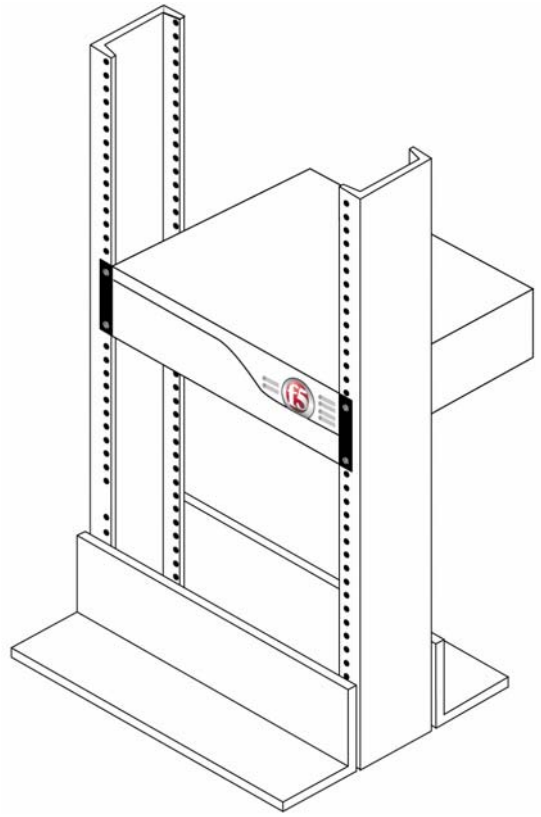


Figure 1.6 *Platform installed in a 19" rack*

To connect the cables and hardware for input/output

1. Connect the hardware that you have chosen to use for input/output:
   - If you are using a VGA monitor and keyboard, connect the monitor connector cable to the video port (number 8 in Figure 1.4), and connect the keyboard connector cable to the keyboard port (number 4 in Figure 1.4).
   - Optionally, if you are using a serial terminal as the console, connect the serial cable to the terminal serial port (number 6 in Figure 1.4). In this case, you should not connect a keyboard to the controller. If there is no keyboard connected to the controller when it is started or rebooted, the controller defaults to using the serial port as the console.
2. Connect the interface labeled Net1 (number 9 in Figure 1.4) to the network from which the controller receives connection requests.

   If you have purchased a unit with three or more network interface cards (NICs), be sure to note or write down how you connect the cables to the interfaces. When you run the Setup utility, it automatically detects the number of interfaces that are installed, and

prompts you to configure more external interfaces if you want. It is important to select the correct interfaces based on the way you have connected the cables to the back of the unit. For more information about interfaces, see *Interfaces*, following.

3. Connect the interface labeled Net2 (number 10 in Figure 1.4) to the network that houses the array of servers, routers, or firewalls that the controller load balances.
4. If you have a hardware-based redundant system, connect the fail-over cable to the fail-over port on each unit (number 7 in Figure 1.4).
5. Connect the power cable to the controller power in (number 2 in Figure 1.4), and then connect it to the power source.

Interfaces

This platform can have as few as one network interface. It is helpful to understand interface naming conventions before you perform configuration tasks such as displaying interface status and settings, setting the media type, and setting the duplex mode.

Interface naming conventions

By convention, the Ethernet interfaces on the platform take the name **<s>.<p>**, where **s** is the slot number of the NIC, and **p** is the port number on the NIC. As shown in Figure 1.7, for the 520/540 platform, slot numbering is top-to-bottom, and port numbering is left-to-right. Note that **slot 1** contains the two onboard NICs numbered 1.1 and 1.2. The numbers **2**, **3**, and **4** in Figure 1.7 illustrate the slot numbering for the PCI expansion slots. For example, if you installed a single port NIC in the PCI slot marked **2**, the port number would be 2.1.

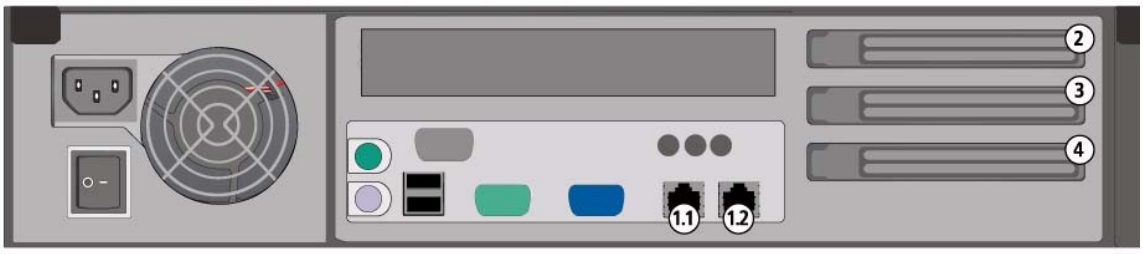


Figure 1.7 *520/540 platform slot and port numbering*

Displaying status and settings for interfaces

From the command line interface, use the following syntax to display the current status and the settings for all installed interfaces:

```
b interface show
```

Figure 1.8 shows an example of the output you see when you issue this command on an active/standby unit in active mode.

```
interface  speed   pkts   pkts   pkts   pkts   bits   bits errors trunk STP
            Mb/s     in    out   drop   coll     in    out
  1.1 UP  100 HD      0    213      0      0      0  74.2K      0
  1.2 UP  100 HD     20     25      0      0  28.6K  33.9K      0
```

Figure 1.8 *The* ***bigpipe interface show*** *command output*

Use the following syntax to display the current status and the setting for a specific interface:

```
b interface <if_name> show
```

Media type and duplex mode

Properties that are configurable on the interfaces include media type and duplex mode, as shown in Table 1.2.

Interface Properties	Description
media	You may specify a media type or use **auto** for automatic detection.
duplex	You may specify a full or half duplex mode, or use **auto** for automatic selection.

Table 1.2 *The attributes you can configure for an interface*

Setting the media type

You can set the media type to that of the interface, or to **auto** for auto-detection. If the media type is set to **auto** and the card does not support auto-detection, the default type for that interface is used, for example **100BaseTX**.

Use the following syntax to set the media type:

```
b interface <if_name> media <media_type> | auto
```

(Default media type is **auto**.)

To view the valid media types for an interface, type the following command:

```
b interface <if_name> media show
```

Note

If the platform is inter-operating with an external switch, the media setting should match that of the switch.

Setting the duplex mode

You can set duplex mode to full or half duplex. If the media type does not allow duplex mode to be set, this is indicated by an onscreen message. If media type is set to **auto**, or if setting duplex mode is not supported for the interface, the duplex setting is not saved to **bigip_base.conf**.

Use the following syntax to set the duplex mode:

```
b interface <if_name> duplex  full | half | auto
```

(Default mode is **auto**.)

Activating the license

Once the platform is installed in the rack and connected to the network, you need a valid license certificate to activate the software. To gain a license certificate, you need to provide two items to the license server: a registration key and a dossier.

The ***registration key*** is a 25-character string. In some cases, you may have received the key by email. If you received a CD, the number is on the back of the CD case. The registration key lets the license server know which F5 products you are entitled to license.

The ***dossier*** is obtained from the software, and is an encrypted list of key characteristics used to identify the platform

You can obtain a license certificate using one of the following methods:

- **Automatic license activation**
  You perform automatic license activation from the command line, the License utility on an unlicensed unit, or from the web-based Configuration utility of an upgraded unit. The automatic method automatically retrieves and submits the dossier to the F5 license server, as well as installing the signed license certificate. In order for you to use this method, the unit must be installed on a network with Internet access.
- **Manual license activation**
  You perform manual license activation from the License utility on an unlicensed unit, or from the web-based Configuration utility of an upgraded unit. With the manual method, you submit the dossier to, and retrieve the signed license file from, the F5 license server manually. In order for you to use this method, the administrative workstation must have Internet access.

◆ Note

You can open the Configuration utility with Netscape Navigator version 4.7, or Microsoft Internet Explorer version 5.0 or 5.5. The Configuration utility is not supported in Netscape Navigator version 6.0.

Automatically activating a license

You can perform automatic license activation from the command line, the License utility on an unlicensed unit, or from the web-based Configuration utility of an upgraded unit. This section describes the automatic license activation process in the following cases:

- From the web-based License utility or Configuration utility.
- From the command line, first-time installation.
- From the command line, upgrading a current installation.

To automatically activate a license using the Configuration utility

1. Open the Configuration utility according to the type of BIG-IP unit you are licensing:
   - If you are licensing a previously configured BIG-IP unit, open the Configuration utility using the configured address.
   - If you are licensing a new BIG-IP unit, from the administrative workstation, open the Configuration utility using one of the the following addresses:
     https://192.168.1.245
     https://192.168.245.245.
     These are default addresses on the unit's local area network.
2. Type the name and password, based on the type of BIG-IP unit you are licensing:
   - If you are licensing a previously configured BIG-IP unit, type your user name and password at the log on prompt.
   - If you are licensing a new BIG-IP system, type the user name **root**, and the password **default** at the log on prompt.

   The product welcome screen displays.
3. Access the License utility based on the type of BIG-IP unit you are licensing:
   - If the unit does not have a license from a previouse version, click **License Utility** to open the License Administration screen.
   - If the unit has a license from a previous version, or an evaluation license, click **Configuration Utility**. In the navigation pane, click **System Admin**, and then click the License Administration tab.
4. In the **Registration Key** box, type the 25-character registration key that you received. If you have more than one key to install, click **Enter More Keys** to install multiple keys. Once you have entered all registration keys, click **Automated Authorization**.

   The License Status screen displays status messages, and **Process complete** appears when the licensing activation is finished.
5. Click **License Terms**, review the EULA, and accept it.
6. At the Reboot Prompt screen, select when you want to reboot the platform.
   License activation is complete only after rebooting.

To automatically activate a license from the command line for first time installation

1. Type the user name **root** and the password **default** at the logon prompt.

2. At the prompt, type **license**.
   The following prompts appear:

   ```
   IP:
   Netmask:
   Default Route:
   Select interface to use to retrieve license:
   ```

   The platform uses this information to make an Internet connection to the license server.

3. After you type the Internet connection information, continue to the following prompt:

   ```
   The Registration Key should have been included with the
   software or given when the order was placed.

   Do you have your Registration Key? [Y/N]:
   ```

4. Type **Y**, and the following prompt appears:

   ```
   Registration Key:
   ```

5. Type the 25-character registration key you received.

   After you press Enter, the dossier is retrieved and sent to the F5 license server, and a signed license file is returned and installed. A message displays indicating the process was successful. If the licensing process is not successful, contact your vendor.

6. You are asked to accept the End User License Agreement.
   The system will not be fully functional until you accept this agreement.

7. You are prompted to reboot the system. Press Enter to reboot. The system will not be fully functional until you reboot.

To automatically activate a license from the command line for upgrades

1. Type your user name and password at the log on prompt.
2. At the prompt, type **setup**.
3. Choose menu option **L**.
4. The following prompt displays:

   ```
   Number of keys: 1
   ```

   If you have more than one registration key, enter the appropriate number.

5. The following prompt displays:

   ```
   Registration Key:
   ```

6. Type the 25-character registration key you received. If you received more than one key, enter all of the keys separated by blanks.

   After you press Enter, the dossier is retrieved and sent to the F5 license server, and a signed license file is returned and installed. A message displays indicating the process was successful.

7. If the licensing process is not successful, contact your vendor.
8. When you are finished with the licensing process, type the following command to restart the services on the system:

   ```
   bigstart restart
   ```

Manually activating a license

You can perform manual license activation from the License utility on an unlicensed unit, or from the web-based Configuration utility of an upgraded unit. With this method, you submit the dossier to, and retrieve the signed license file from, the F5 license server manually. This section describes the manual license activation process using the Configuration utility or License utility.

To manually activate a license using the License utility or Configuration utility

1. Open the Configuration utility according to the type of BIG-IP unit you are licensing:
   - If you are licensing a previously configured BIG-IP unit, open the Configuration utility using the configured address.
   - If you are licensing a new BIG-IP unit, from the administrative workstation, open the Configuration utility using one of the following addresses:
     https://192.168.1.245
     https://192.168.245.245.
     These are default addresses on the unit's local area network.
2. Type the name and password, based on the type of BIG-IP unit you are licensing:
   - If you are licensing a previously configured BIG-IP unit, type your user name and password at the log on prompt.
   - If you are licensing a new BIG-IP system, type the user name **root**, and the password **default** at the log on prompt.

   The product welcome screen displays.
3. Access the License utility based on the type of BIG-IP unit you are licensing:
   - If the unit does not have a license from a previouse version, click **License Utility** to open the License Administration screen.
   - If the unit has a license from a previous version, or an evaluation license, click **Configuration Utility**. In the navigation pane, click **System Admin** and then click the License Administration tab.
4. In the **Registration Key** box, type the 25-character registration key that you received. If you have more than one key to install, click **Enter More Keys** to install multiple keys. Once you have entered all registration keys, click **Manual Authorization**.

5. At the Manual Authorization screen, retrieve the dossier using one of the following methods:
   - Copy the entire contents of the **Product Dossier** box.
   - Click **Download Product Dossier**, and save the dossier to the hard drive.
6. Click the link in the **License Server** box.
   The Activate F5 License screen opens in a new browser window.
7. From the Activate F5 License screen, submit the dossier using one of the following methods:
   - Paste the data you just copied into the **Enter your dossier** box, and click **Activate**.
   - At the **Product Dossier** box, click **Browse** to locate the dossier on the hard drive, and then click **Activate**.

   The screen returns a signed license file.
8. Retrieve the license file using one of the following methods:
   - Copy the entire contents of the signed license file.
   - Click **Download license**, and save the license file to the hard drive.
9. Return to the Manual Authorization screen, and click **Continue**.
10. At the Install License screen, submit the license file using one of the following methods:
    - Paste the data you copied into the **License Server Output** box, and click **Install License**.
    - At the **License File** box, click **Browse** to locate the license file on the hard drive, and then click **Install License**.

    The License Status screen displays status messages, and **Process complete** appears when licensing activation is finished.
11. Click **License Terms**, review the EULA, and accept it.
12. At the Reboot Prompt screen, select when you want to reboot the platform.
    License activation is complete only after rebooting.

Using the Setup utility

Once you install the platform and obtain a license, you can configure the software with the Setup utility. The Setup utility defines the initial configuration settings required to install the platform into the network.

See the ***BIG-IP Reference Guide***, Chapter 2, *Using the Setup Utility* for full details and instructions. You can download the guide from the CD.

Additional resources

You can find additional technical information about this product in the following resources:

- **CD**
  You can download additional documentation such as the ***BIG-IP Reference Guide*** and the ***BIG-IP Solutions Guide***.
- **Release notes**
  Release notes for the current version of this product are available from the product web server home page, and are also available on the technical support site. The release notes contain the latest information for the current version, including a list of new features and enhancements, a list of fixes, and, in some cases, a list of known issues.
- **Online help**
  You can find help online in three different locations:
  - The web server on the product has PDF versions of the guides included on the Software and Documentation CD.
  - The web-based Configuration utility has online help for each screen. Simply click the **Help** button.
  - Individual **bigpipe** commands have online help, including command syntax and examples, in standard UNIX man page format. Simply type the command followed by the word **help**, and the BIG-IP software displays the syntax and usage associated with the command.
- **Third-party documentation for software add-ons**
  The Product and Documentation CD contains online documentation for all third-party software, such as the Advanced Routing Modules.
- **Technical support through the World Wide Web**
  The F5 Networks Technical Support web site, **http://tech.f5.com**, provides the latest technical notes, answers to frequently asked questions, updates for administrator guides (in PDF format), and the Ask F5 natural language question and answer engine. To access this site, you need to register at **http://tech.f5.com**.

2

Configuring the FIPS 140 Hardware

- Introducing FIPS 140 hardware security module support
- Initializing the FIPS 140 hardware security module and creating the security world
- Using the key utilities to generate keys
- Additional configuration options

Introducing FIPS 140 hardware security module support

The 520/540 platform, with BIG-IP software installed, supports a hardware security module (HSM) that is certified at the Federal Information Processing Standards (FIPS) 140-1 level 3. The FIPS standard is a set of requirements designed to facilitate the construction, and measure the security of cryptographic modules, and define methods for protecting cryptographic keys from unauthorized access. Typically, the cryptographic keys are generated inside the FIPS 140 certified hardware security module (HSM), and never leave except when in encrypted form.

With this HSM installed, you can encrypt private keys on the 520/540 platform with a 3-DES key that resides only on the FIPS 140 module. The 3-DES key is further encrypted with a key spread across one to five smart cards.

In order to configure FIPS 140 hardware support, you need to complete the following tasks:

- Initialize the FIPS 140 hardware and set up the security world.
- Generate keys using **genkey** and **genconf** utilities.
- Configure the SSL Accelerator.

Note

All BIG-IP products except the BIG-IP LoadBalancer, BIG-IP FireGuard Controller, and the BIG-IP Cache Controller support this configuration.

The following sections in this chapter provide the information to configure FIPS 140 hardware support in various scenarios.

Initializing the FIPS 140 hardware security module and creating the security world

After you install the 520/540 platform in the network and run the Setup utility, you can initialize the FIPS 140 hardware security module (HSM). This is how you prepare the HSM for the security world. The ***security world*** is the environment you create for secure life-cycle management of keys based on nCipher technology. To create the security world, you run various utilities from the command line on the 520/540 platform. You can initialize the HSM and set up the security world in a number of different situations:

- On a single unit or primary unit of a redundant system
- On a redundant system with one HSM in each 520/540 platform (only required if you have a redundant system)
- On a single 520/540 platform with two HSMs
- On a single or redundant system, adding another HSM to an existing security world

◆ Note

You will need a paper clip or ballpoint pen and at least two of the smart cards provided with the security module (three are recommended) before you begin the initialization process.

Creating the security world on a single unit or the primary unit of a redundant system

This section describes how to create the security world on a single unit or the primary unit of a redundant system.

To create the security world on a single unit or the primary unit of a redundant system

1. Locate the switch labeled **M-O-I** on the FIPS 140 card at the back of the controller (see Figure 2.1). Then using a paper clip or your finger tip, move the switch to the **I** position.
2. With a ballpoint pen tip, gently push the reset button (Figure 2.2). If you have done this correctly, the LED blinks quickly for a moment and then blinks slowly again.
3. Type the following command to start the **sw-init** utility:

   ```
   sw-init
   ```

   Figure 2.3 is an example session of the **sw-init** utility.

4. When the **sw-init** utility prompts you for the Administrator Cards, we recommend that you type **2** for the total number, and **1** for the required number. This creates a cardset that requires only one card to be present for card or module management, but also provides the other card as a backup of the first.

   Figure 2.4 demonstrates the proper orientation of the smart card before you insert it into the card reader.

   For more information about card sets, please refer to the nCipher manual, ***Key management user guide***, *Chapter 6: Managing cards*. This manual is included on the Software and Documentation CD.

5. Move the **M-O-I** switch to **O** (Figure 2.1) and, with the paperclip, press the reset button (Figure 2.2)

6. Generate keys by running **genconf** and then **genkey**. For detailed information, see *Using the key utilities to generate keys*, on page 2-11.

7. After you generate the keys, your next task depends on what type of system you are configuring:

   - If this is a single unit, after you create the the security world, you can configure the SSL Accelerator. For more information, see *Additional configuration options*, on page 2-14.
   - If this is a primary unit in a redundant system, complete the tasks described in the section *Configuring the security world on the second unit in a redundant system*, on page 2-5.

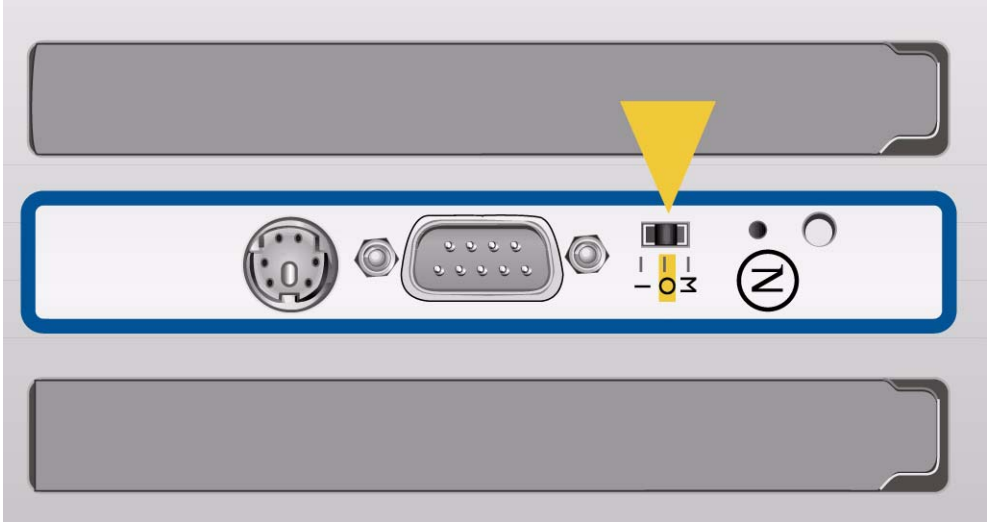


Figure 2.1 *This figure shows the M-O-I switch on the FIPS 140 security module*

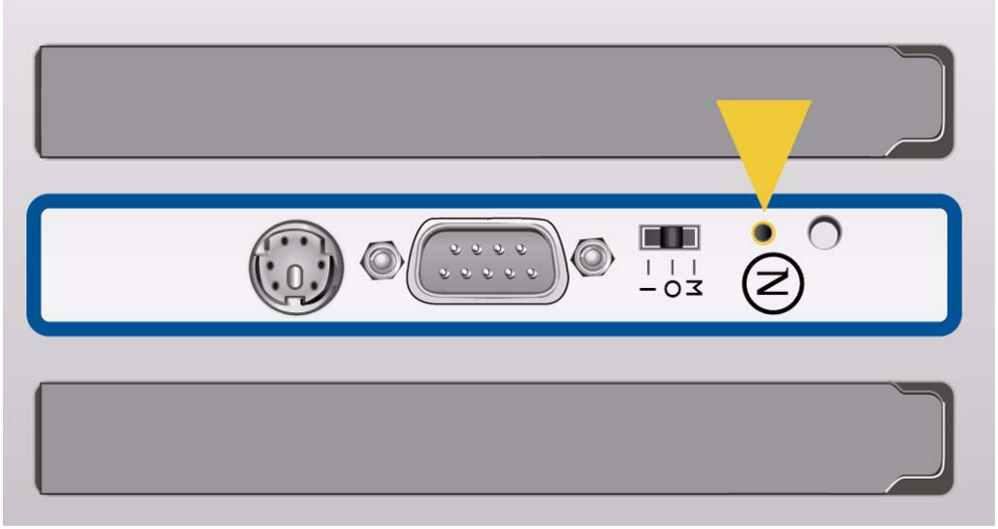


Figure 2.2 *The reset button on the FIPS 140 security module*

```
# sw-init
Key management data not yet set up (at least on this computer).
Modules ready for (re)programming:
      Serial no.       Firmware version
  #1  CBF9-187E-D9ED   1.71.11 built on Mar 21 2001 16:01:57
Please confirm - Initialize new security system and program these module(s) ?  yes
How many Administrator Cards in total ?  2
How many Administrator Cards will be required ?  1
Enable future key recovery using administrator cards ?
 (This cannot be enabled retrospectively.  Answering `no' may require you
  to discard your keys when you upgrade the support software, or if cards
  or pass phrases are lost.  Consult the manual for full documentation.)
Enable recovery ?  [yes]  yes
Using module #1.
Please insert new administrator card #1 in module #1.  [enter]
Now, please enter new pass phrase for this card: ****** [enter]
Initialization of security system on module #1 complete.
Initialization complete.
```

Figure 2.3 *Example of a security world initialization session with the* ***sw-init*** *utility*

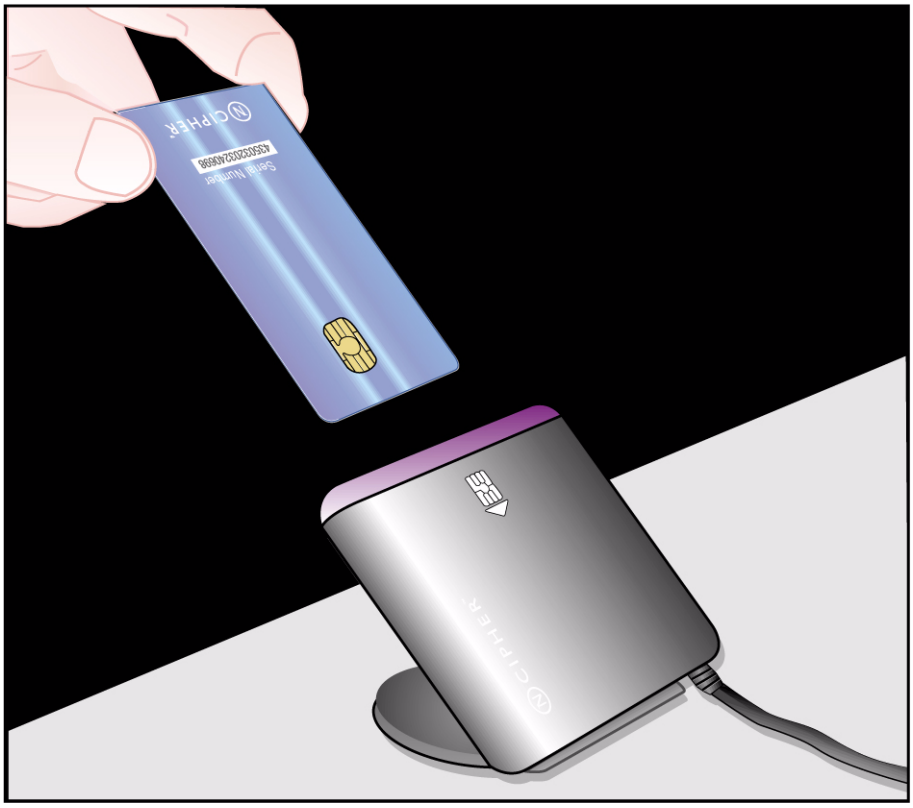


Figure 2.4 *The proper way to insert a smart card in the card reader*

Configuring the security world on the second unit in a redundant system

The second unit in the redundant system must be brought into the same security world as your primary unit. This is a simple process, but one that must be done after you run the Setup utility and synchronize the configurations of the units in the redundant system. This means that both 520/540 platforms in the redundant system must be synchronized in order to synchronize the SSL keys. This section describes how to synchronize the 520/540 redundant system, and how to configure the security world on the second unit in a redundant system.

◆ Note

You must configure the 520/540 redundant system for fail-over for this configuration to function properly. If you have not configured the redundant system, refer to Chapter 13, ***Configuring a Redundant System****, in the* ***BIG-IP Reference Guide****.*

To synchronize the 520/540 configuration from the command line

Before you configure the security world on the redundant system, synchronize the 520/540 configuration. To synchronize the 520/540 configuration from the command line, type the following command on the primary unit:

```
b config sync all
```

To configure the security world on the redundant system

After you synchronize the 520/540 configuration, you need to initialize the HSM and configure the security world on the second unit in the redundant system. You will need a ballpoint pen, or other fine-tipped implement to press the reset button.

Before you start, you need the required number of administrator smart cards from the administrator cardset you created when initializing the security world on the primary unit.

1. At the back of the second unit in the redundant system, locate the switch labelled **M-O-I** (Figure 2.1). Then using a paper clip or your fingernail, move the switch to the **I** position.
2. With the end of the ballpoint pen, gently push the reset button (Figure 2.2). If you have done this correctly, the LED blinks quickly for a moment, and then blinks slowly again.
3. Place your administrator smart card into the card reader attached to the FIPS 140 security module in the redundant unit. Figure 2.4 shows the proper orientation.
4. At the console of the second unit in the redundant system, run the **sw-rest** command from **/config/bigconfig** (See Figure 2.5 for an example session).
5. Return to the back of the controller. Move the **M-O-I** switch to **O** (Figure 2.1) and, with the ballpoint pen, press the reset button in the hole above the switch (Figure 2.2).

After you bring the second controller into the security world, you can configure the SSL Accelerator. For more information, see *Additional configuration options*, on page 2-14.

```
# sw-rest
Key management security system data found.

Modules ready for (re)programming:
      Serial no.       Firmware version
  #1  CBF9-187E-D9ED   1.71.11 built on Mar 21 2001 16:01:57

Please confirm - Program these module(s) into existing KM infrastructure ?  yes

Programming module #1. [enter]
Using slot #0, type SmartCard.

Please insert administrator card in module #1.  [enter]
Initialisation of module #1 complete.
```

Figure 2.5 *An example session with the* ***sw-rest*** *utility*

Configuring multiple FIPS 140 hardware security modules in a single 520/540

To achieve a faster transaction per second (TPS) rate in a controller, you can install two hardware security modules (HSMs). You may do this in two ways:

- Install two security modules and create the security world at the same time.
- Add a second security module to and existing security world.

Installing two security modules and creating the security world at the same time

This section describes how to install two security modules and create the security world at the same time in a single 520/540. This procedure assumes that you have not established a security world.

◆ Note

Connect a card reader to each of the security modules for this configuration.

To install both security modules and create the security world at the same time

To bring two HSMs installed in one 520/540 into the security world, you need a paper clip or other fine-tipped implement and at least two smart cards.

1. On **each** HSM, locate the switch labeled **M-O-I** (Figure 2.1). Using a paper clip or your fingernail, move the switch on each HSM to the **I** position.

2. On **each** HSM, gently push the reset button with the tip of the ballpoint pen. If you have done this correctly, the LEDs blink quickly for a moment, and then blink slowly again.
3. From the console, run the **sw-init** command. Figure 2.6 is an example session.
4. When you are prompted for the Administrator Cards, we recommend that you enter the value **2** for the total number, and **1** for the required number. This creates a cardset that requires only one card to be present to do any card or module management, but also provides the other card as a backup. Lock one of the cards away in a secure place (after you complete the configuration).

   The utility prompts you to insert the blank cards into the reader of the first HSM to create the operator card set. Figure 2.4 shows how to orient the card before inserting it in the reader.

   The utility also prompts you to to insert the same cards into the reader attached to the second HSM to bring it into the security world at the same time.
5. Return to the back of the controller with your pen. On each HSM, move the M-O-I switch to the **O** position, then, with the pen, press the reset button on both HSMs (Figure 2.2).
6. Generate keys as normal by running **genconf** and then **genkey**. For detailed information, see *Using the key utilities to generate keys*, on page 2-11.
7. After you generate the keys, your next task depends on what type of system you are configuring:
   - If this is a single unit, after you create the the security world, you can configure the SSL Accelerator. For more information, see *Additional configuration options*, on page 2-14.
   - If this is a primary unit in a redundant system, complete the tasks described in the section *Configuring the security world on the second unit in a redundant system*, on page 2-5.

```
bigip2:~# sw-init
Key management data not yet set up (at least on this computer).
Modules ready for (re)programming:
     Serial no.       Firmware version
  #1  AE63-178B-1234   1.65.8 built on Aug 21 2000 16:52:57
  #2  CBF9-187E-5678   1.71.11 built on Mar 21 2001 16:01:57
Please confirm - Initialise new security system and program these module(s) ?  yes
How many Administrator Cards in total ?  2
How many Administrator Cards will be required ?  1
Enable future key recovery using administrator cards ?
 (This cannot be enabled retrospectively.  Answering `no' may require you
  to discard your keys when you upgrade the support software, or if cards
  or passphrases are lost.  Consult the manual for full documentation.)
Enable recovery ?  [yes]  [enter]
Using module #1.
Please insert new administrator card #1 in module #1.  [enter]
Now, please enter new passphrase for this card: *****
Then, please reenter the passphrase for this card: *****
Initialization of security system on module #1 complete.
Programming module #2.
Using slot #0, type SmartCard.
Please insert administrator card in module #2.  [enter]
Please enter passphrase for this card: *****
Initialization of module #2 complete.
Initialization complete.
```

Figure 2.6 *A sample session for* ***sw-init*** *for configuring two HSMs in one 520/540*

Adding a second security module to an existing security world

This section describes how to add an additional hardware security module (HSM) to a 520/540 that already has an HSM and an established security world. Note that these instructions assume you have already installed the HSM in the 520/540. You can use this procedure to add a second HSM to a single 520/540 or to a primary controller in a redundant system. You need a ballpoint pen or other fine-tipped implement to activate the reset button.

To add a second security module to an existing security world

Before you start, gather the smart cards from the administrator card set you created when initializing the security world on the first HSM in the system.

1. At the back of the system, locate the switch labeled **M-O-I** (Figure 2.1).
   - Then, on the HSM you are adding to the system, move the switch to the **I** position.
   - Leave the M-O-I switch on the original HSM at the **O** setting.
2. On the new HSM, with the end of the ballpoint pen, gently push the reset button (shown in Figure 2.2). If you have done this correctly, the LED blinks quickly for a moment and then blinks slowly again.

3. At the console, run the **sw-rest** command.
   For an example session with this utility, see Figure 2.7.
4. When prompted, insert the administrator card(s) into the card reader attached to the HSM you added to the system. Make sure you insert the card correctly. See Figure 2.4 for details.
5. Return to the back of the controller. On the HSM you added to the system, move the M-O-I switch to the **O** position, then press the reset button.
6. Generate keys as usual by running **genconf** and then **genkey**. For detailed information, see *Using the key utilities to generate keys*, on page 2-11.
7. After you generate the keys, your next task depends on what type of system you are configuring:
   - If this is a single unit, after you create the the security world, you can configure the SSL Accelerator. For more information, see *Additional configuration options*, on page 2-14.
   - If this is a primary unit in a redundant system, complete the tasks described in the section *Configuring the security world on the second unit in a redundant system*, on page 2-5.

```
# sw-rest
Key management security system data found.
Modules NOT ready for (re)programming:
      Serial no.       Reason why module not ready
  #1  AE63-178B-1234   Initialisation link not fitted
Modules ready for (re)programming:
      Serial no.       Firmware version
  #2  CBF9-187E-5678   1.71.11 built on Mar 21 2001 16:01:57
Please confirm - Program these modules(s) into existing KM infrastructure? yes
Programming module #2.
Using slot #0, type SmartCard.
Please insert administrator card into module #2. [enter] (fig 4)
Please enter passphrase for this card: ****** [enter]
Initialisation of module #2 complete.
```

Figure 2.7 *An example session with the* ***sw-rest*** *utility*

Using the key utilities to generate keys

To obtain a valid certificate, you must have a private key. If you do not have a key, you can use the **genconf** and **genkey** utilities on the 520/540 to generate a key and a temporary certificate. The **genkey** and **gencert** utilities automatically generate a request file that you can submit to a certificate authority (CA). If you have a key, you can use the **gencert** utility to generate a temporary certificate and request file.

These key utilities have specific funtions:

- **genconf**
  This utility creates a key configuration file that contains specific information about your organization. The **genkey** utility uses this information to generate a certificate.
- **genkey**
  After you run the **genconf** utility, run this utility to generate a temporary 10-year certificate for testing the SSL Accelerator on the 520/540. This utility also creates a request file that you can submit to a certificate authority (CA) to obtain a certificate.
- **gencert**
  If you already have a key, run this utility to generate a temporary certificate and request file for the SSL Accelerator.

WARNING

After you import or generate keys on a redundant system, make sure you synchronize the 520/540 configurations. To synchronize the 520/540 configuration, see ***To synchronize the 520/540 configuration from the command line****, on page 2-6.*

Generating a key configuration file and a key

If you do not have a key, you can generate a key configuration file using the **genconf** utility, and use the file to generate a key with the **genkey** utility. You can also use these utilities to create a new key configuration file.

To generate a key configuration file using the genconf utility

To generate a key and certificate, first run the **genconf** utility from the command line with the following command:

```
/usr/local/bin/genconf
```

The utility prompts you for information about the organization for which you are requesting certification. This information includes:

- The fully qualified domain name (FQDN) of the server. Note that this FQDN must be RFC1034/1035-compliant, and cannot be more than 63 characters long (this is an x509 limitation).

- The two-letter ISO code for your country
- The full name of your state or province
- The city or town name
- The name of your organization
- The division name or organizational unit

Figure 2.8 contains example entries for the server **my.server.net**.

```
Common Name (full qualified domain name): my.server.net
Country Name (ISO 2 letter code): US
State or Province Name (full name): WASHINGTON
Locality Name (city, town, etc.): SEATTLE
Organization Name (company): MY COMPANY
Organizational Unit Name (division): WEB UNIT
```

Figure 2.8 *Example entries for the* ***genconf*** *utility*

To generate a key using the genkey utility

After you run the **genconf** utility, you can generate a key with the **genkey** utility. From the command line, type the following command to run the **genkey** utility:

`/usr/local/bin/genkey <server_name>`

For the **<server_name>**, type the FQDN of the server to which the certificate applies. After the utility starts, it prompts you to verify the information created by the **genconf** utility. After you run this utility, a certificate request form is created in the following directory:

/config/bigconfig/ssl.csr/<fqdn>.csr

The **<fqdn>** is the fully qualified domain name of the server. Please contact your certificate authority (CA) and follow their instructions for submitting this request form.

In addition to creating a request form that you can submit to a certificate authority, this utility also generates a temporary certificate. The temporary certificate is located in:

/config/bigconfig/ssl.crt/<fqdn>.crt

The **<fqdn>** is the fully qualified domain name of the server.

Note that you must copy the key and certificate to the other 520/540 in a redundant system.

This temporary certificate is good for ten years, but for an SSL proxy, you should have a valid certificate from your certificate authority (CA).

WARNING

Be sure to keep your previous key if you are still undergoing certification. The certificate you receive is valid only with the key that originally generated the request.

Generating a certificate request file and temporary certificate

This section describes how to use the key you generated, or an existing key, to generate a certificate request file and a temporary certificate with the **gencert** utility.

To generate a certificate with an existing key using the gencert utility

To generate a temporary certificate and request file to submit to the certificate authority with the **gencert** utility, you must first copy an existing key for a server into the following directory on the 520/540:

/config/bigconfig/ssl.key/

After you copy the key into this directory, type the following command at the command line:

```
/usr/local/bin/gencert <server_name>
```

For the **<server_name>**, type the FQDN of the server to which the certificate applies. After the utility starts, it prompts you for various information. After you run this utility, a certificate request form is created in the following directory:

/config/bigconfig/ssl.crt/<fqdn>.csr

The **<fqdn>** is the fully qualified domain name of the server. Please contact your certificate authority (CA) and follow their instructions for submitting this request form.

Importing existing public keys and certificates

No additional software is needed to import an existing private key. Change to the **/config/bigconfig/ssl.key** directory (or the directory that contains the private key you want to import). Identify the key you want to import. It must be in PEM format. From the command line, run the **generatekey** command with the following command:

```
generatekey
```

WARNING

After you import or generate keys on a redundant system, make sure you synchronize the 520/540 configuration. To synchronize the 520/540 configuration, see ***To synchronize the 520/540 configuration from the command line****, on page 2-6*

Figure 2.9 is an example session with the **generatekey** utility.

```
bigip:/config/bigconfig/ssl.key# generatekey --import ssleay protect=module
nCipher KM key generation/import utility
Site domain name ? [ ]  host.company.com
Key file to import:  bigip.key
Recovery feature ? (y/n) [y]  y
key generation/import parameter(s):
 protect         Protected by                        MODULE
 x509dnscommon   Site domain name                    host.company.com
 ssleayconvfile  Key file to import                  bigip.key
 recovery        Recovery feature                    1
Importing existing key ...
Key imported into key management system.
```

Figure 2.9 *An example session where the existing key* ***bigip.key*** *is imported using the* ***generatekey*** *utility*

WARNING

From a security standpoint, it is better to generate a new key instead of importing a plain text key which may have already been compromised. To generate a new key, see ***Using the key utilities to generate keys****, on page 2-11*.

Additional configuration options

After you complete the 520/540 configuration, you have a number of options:

- After you have initialized the security world and generated keys, you can manage the keys with the Key Management System. For more information about the Key Management System, see the ***BIG-IP Reference Guide***, Chapter 7, *Using the Key Management System*, under the *Authentication* section.
- There are additional SSL Accelerator options you can configure. For more information, see the ***BIG-IP Reference Guide***, Chapter 7, *SSL Accelerator Proxies.*
- All configurations have health monitoring options. Refer to the ***BIG-IP Reference Guide***, Chapter 11, *Monitors*.
- When you create a pool, there is an option to set up persistence and a choice of load balancing methods. Refer to the ***BIG-IP Reference Guide***, Chapter 4, *Pools*.

3

Additional Hardware Specifications

- Reviewing hardware specifications
- 520 specifications
- 540 specifications

Reviewing hardware specifications

The following section contains additional information about the 520/540 hardware platforms.

Specification	Description
Server/Node Operating System Compatibility	Load balancing of any TCP/IP OS, including Windows NT, Windows 95, all UNIX platforms, and Mac/OS
Internet/Intranet Protocol Support	All TCP services, UDP, SIP, and SSL; nearly all IP-based protocols
Administrative Environment Support	DNS proxy, SMTP, F-secure SSH, SNMP, dynamic/static network monitoring, scheduled batch job processing, system status reports, and alarms event notification
Network Management & Monitoring	Secure SSL browser-based interface, remote encrypted login and file transfer using F-secure SSH monitor, BIG-IP system network monitoring utilities and additional contributed software; SNMP gets and traps, iControl API using CORBA & SOAP/XML
Dynamic Content Support	ASP (active server pages),VB (visual basic script), ActiveX, JAVA,VRML, CGI, Cool Talk, Net Meeting, Real Audio, Real Video, Netshow, Quick Time, PointCast, any HTTP encapsulated data
BIG-IP Device Redundancy	Watchdog timer card, fail-safe cable (primary & secondary)
Web Server Application Compatibility	Any IP-based web or application server
Routing Protocols	RIP, OSPF, BGP
Operating Temperature	23° to 122° F (-5° to 50° C) per Telcordia GR-63-CORE 5.1.1 and 5.1.2
Relative Humidity	10 to 90% @ 40º C, per Telcordia GR-63-CORE 5.1.1 and 5.1.2
Power Supply	350W 110/220 VAC AUTO Switching
Safety Agency Approval	UL 60950 (UL1950-3) CSA-C22.2 No. 60950-00 (Bi-national standard with UL 60950) CB TEST CERTIFICATION TO IEC 950 EN 60950
Electromagnetic Emissions Certifications	EN55022 1998 Class A EN55024 1998 Class A FCC Part 15B Class A

Table 3.1 *General 520/540 platform specifications*

520 specifications

The following specifications apply to only the 520 platform.

Specification	Description
Dimensions	3.5"H x 19"W x 21.7"D (per unit) 2U industry standard rack-mount chassis
Weight	26 lbs. (per unit)
Processor	Single PIII 1 GHz
Network Interface	2x10/100 with option for additional 10/100 and Gb interfaces
Hard Drive Capacity	30 GB
RAM	256 MB (expandable to 2 GB)

Table 3.2 *The 520 platform specification*

Important

Specifications are subject to change without notification.

540 specifications

The following specifications apply to only the 540 platform.

Specification	Description
Dimensions	3.5"H x 19"W x 21.7"D (per unit) 2U industry standard rack-mount chassis
Weight	26 lbs. (per unit)
Processor	Dual PIII 1 GHz
Network Interface	2x10/100 with option for additional 10/100 and Gb interfaces
Hard Drive Capacity	30 GB
RAM	512 MB (expandable to 2 GB)

Table 3.3 *The 540 platform specification*

Important

Specifications are subject to change without notification.

Glossary

bigpipe

The **bigpipe** utility provides command line access to the BIG-IP software.

BIOS

BIOS stands for Basic Input/Output System. The BIOS is software that is built-in to the computer and determines what the computer can do without accessing programs from a disk.

Configuration utility

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

DHCP

DHCP stands for Dynamic Host Configuration Protocol. It is a protocol used to assign dynamic IP addresses to network devices. When using DHCP, a network device can have a different IP address each time it connects to the network.

DNS

DNS stands for Domain Name System. It is a service that translates domain names into IP addresses. For example, the domain name **www.sample.com** might translate to **101.102.103.104**.

dossier

A dossier is an encrypted list of key platform characteristics used to identify the platform, and to enforce or restrict activation on the platform.

host

A host is a network server that manages one or more virtual servers that the BIG-IP software uses for load balancing.

license certificate

A license certificate is a digital file created by the F5 license server. The license server uses your product registration key and dossier to process the file, which is stored on the BIG-IP system. See also *registration key* and *dossier*.

network boot

A network boot is a method of starting up a computer–loading the operating system and other basic software–from a network, rather than from a source within the computer itself, such as the hard drive or CD-ROM.

NIC

NIC stands for Network Interface Card. It is an expansion board used to connect a computer to a network.

port

A port is represented by a number that is associated with a specific service supported by a host. Refer to the Services and Port Index for a list of port numbers and corresponding services.

PXE

PXE stands for Pre-Boot Execution Environment, a network boot method. It allows you to boot a computer from a server on a network before you boot the operating system on the local hard drive. See also *network boot*.

registration key

The registration key is a 25-character string that you need in order to license your F5 products. You may have received it from F5 by email, or you may find it on the back of the CD case.

Setup utility

The Setup utility guides you through the initial system configuration process. The Setup utility is available from the command line, or as a web-based wizard from the product splash screen.

SSH

SSH is a protocol for secure remote login and other secure network services over a non-secure network.

SSL

SSL stands for Secure Sockets Layer. It is a protocol that uses a public key to encrypt data transmitted through the Internet over an SSL connection. URLs using an SSL connection start with **HTTPS:** instead of **HTTP:**.

subnetwork

The portion of a network that shares a common address component. For instance, on TCP/IP networks, a subnetwork is all devices whose IP addresses have the same prefix segment.

Telnet

Telnet is a terminal emulation program for TCP/IP networks. Telnet runs on your computer and connects it to a server on the network. It then allows you to enter and execute commands as though you were directly connected to the server console.

terminal emulator

A terminal emulator is a program that mimics a terminal.

virtual server

Virtual servers are a specific combination of virtual address and virtual port, associated with a content site that is managed by BIG-IP software or other type of host server.

Index