Security Products

Upgrade Guide

ScreenOS 6.1.0, Rev. 03

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-022770-01, Revision 03

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment 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 users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Table of Contents

About This Guide

This guide contains procedures for upgrading existing firmware to ScreenOS 6.1.0.

Conventions

This guide uses the conventions described in the following sections:

- Web User Interface Conventions on page 5
- Command Line Interface Conventions on page 6
- Naming Conventions and Character Types on page 6

Web User Interface Conventions

The Web user interface (WebUI) contains a navigational path and configuration settings. To enter configuration settings, begin by clicking a menu item in the navigation tree on the left side of the screen. As you proceed, your navigation path appears at the top of the screen, with each page separated by angle brackets.

The following example shows the WebUI path and parameters for defining an address:

Policy > Policy Elements > Addresses > List > New: Enter the following information, then click **OK**:

```
Address Name: addr_1
IP Address/Domain Name:
    IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust
```

To open online Help for configuration settings, click on the question mark (?) in the upper left of the screen.

The navigation tree also provides a Help > Config Guide configuration page to help you configure security policies and Internet Protocol Security (IPSec). Select an option from the list, and follow the instructions on the page. Click the **?** character in the upper left for online Help on the Config Guide.

Command Line Interface Conventions

The following conventions are used to present the syntax of command line interface (CLI) commands in text and examples.

In text, commands are in **boldface** type and variables are in *italic* type.

In examples:

- Variables are in *italic* type.
- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example, the following command means "set the management options for the ethernet1, the ethernet2, *or* the ethernet3 interface":

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

NOTE: When entering a keyword, you only have to type enough letters to identify the word uniquely. Typing **set adm u whee j12fmt54** will enter the command **set admin user wheezer j12fmt54**. However, all the commands documented in this guide are presented in their entirety.

Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations:

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes; for example:

  set address trust "local LAN" 10.1.1.0/24

- Any leading spaces or trailing text within a set of double quotes are trimmed; for example, **" local LAN "** becomes **"local LAN"**.
- Multiple consecutive spaces are treated as a single space.
- Name strings are case-sensitive, although many CLI keywords are case-insensitive. For example, **"local LAN"** is different from **"local lan"**.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.
- ASCII characters from 32 (0x20 in hexadecimals) to 255 (0xff), except double quotes ("), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NOTE: A console connection supports only SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your browser supports.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings—http://www.juniper.net/customers/support/
- Find product documentation—http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base—http://kb.juniper.net/
- Download the latest versions of software and review your release notes—http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications—http://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum—http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Manager—http://www.juniper.net/customers/cm/
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool—https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Manager tool in the CSC at http://www.juniper.net/customers/cm/.
- Call 1-888-314-JTAC (1-888-314-5822—toll free in USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/customers/support/requesting-support/.

Document Feedback

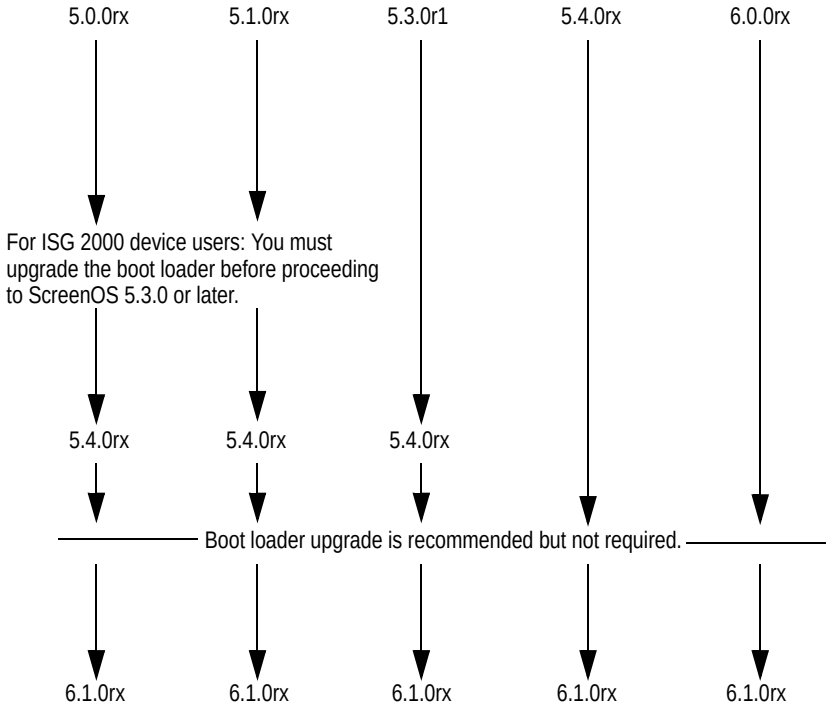
If you find any errors or omissions in this document, contact Juniper Networks at techpubs-comments@juniper.net.

ScreenOS Upgrade Procedures

This guide contains procedures for upgrading existing firmware to ScreenOS 6.1.0.

Before you upgrade a security device, you must have the most recent ScreenOS firmware stored on your local drive. Depending on the platform and the firmware your security device is currently running, you also might need intermediate (or step-up) firmware, new boot-loader firmware, or both. Figure 1 illustrates the various firmware upgrade paths to ScreenOS 6.1.0.

Figure 1: Firmware Upgrade Path



CAUTION: Before upgrading or downgrading a security device, save the existing configuration file to avoid losing any data. During the upgrade or downgrade process, the device might remove part or all of the configuration file.

Table 1 lists the recommended upgrade path to ScreenOS 6.1.0 based on device model and firmware version. For example, if you are running ScreenOS 4.0 on a NetScreen-5000 Series, you need to upgrade to ScreenOS 5.4r8 or later before upgrading to ScreenOS 6.1.0. Table 1 also lists boot-loader upgrade recommendations for each ScreenOS platform.

NOTE: For the SSG 500/500M and SSG 300M Series devices, we strongly recommend that you upgrade the boot loader. For other devices, we recommend that you try to upgrade and if you run into issues, then upgrade your boot loader.

Table 1: Upgrade Paths to ScreenOS 6.1.0

Platform	Intermediate Firmware	Upgrade Recommendation (Boot-Loader Filename)
ISG 1000	5.4r8 or later	Load1000v102
ISG 1000-IDP	5.4r8 or later	Load1000v102
ISG 2000	5.4r8 or later	Load2000v116
ISG 2000-IDP	5.4r8 or later	Load2000v116
NetScreen-5000 Series using 5000-M2 NS-5000-8G2 NS-5000-2XGE	5.4r8 or later	Load5000v103 See the Caution following Table 1.
NetScreen-5000 Series using 5000-M3 NS-5000-8G2G4	6.1r1 or later	Load5000v103
SSG 5	5.4r8 or later	Loadssg5ssg20v132
SSG 20	5.4r8 or later	Loadssg5ssg20v132
SSG 140	5.4r8 or later	Loadssg140v324
SSG 320M	6.0r1 or later	Loadssg300v306
SSG 350M	6.0r1 or later	Loadssg300v306
SSG 520	5.4r8 or later	Loadssg500v105
SSG 550	5.4r8 or later	Loadssg500v105
SSG 520M	5.4r8 or later	Loadssg500v105
SSG 550M	5.4r8 or later	Loadssg500v105

CAUTION: This release requires the SIMM DRAM upgrade to 1GB on NetScreen-5000 Series devices. Secure Port Modules (SPMs) affected are NS-5000-8G2 and NS-5000-2XGE manufactured before February 1, 2006. If your NS-5000 modules qualify for a memory upgrade, contact Juniper Networks at 1-866-369-5418 or email junipermem@onprocess.com for a memory-upgrade kit. The memory upgrade is free for qualified users.

Device-Specific Requirements

The NetScreen-5400 device supports two million sessions (the default) in version 6.1.0. When upgrading from 5.4 or 6.0r1 to 6.1 or 6.0r2, make sure your device has a minimum of 450 MB of free memory. One million sessions requires approximately 340 MB of memory.

Requirements for Upgrading Device Firmware

This section lists what is required to perform the upgrade of security device firmware. The information in this section and the procedures in this guide apply whether you are moving to a later release than what you are currently running or to an earlier release. However, it is not recommended that you downgrade because some configuration can be lost.

NOTE: You can upgrade some security devices locally or remotely, but we recommend that you perform the upgrade of a security device at the device location.

You can use any of the following methods to upgrade a security device:

- WebUI
- CLI
- Boot loader

To use the WebUI, you must have the following access:

- Root privilege to the security device
- Network access to the security device from a computer that has a browser
- New ScreenOS firmware (downloaded from the Juniper Networks Web site and saved locally)

NOTE: After upgrading from a previous release of ScreenOS to ScreenOS 6.1, you might need to either clear the cookies in your Web browser or press the default Help Link Path button in the WebUI, located in Configuration > Admin > Management. Because of cookies set when managing a device, you might receive the prior version of the Help files when selecting WebUI online Help.

To use the CLI, you must have the following access:

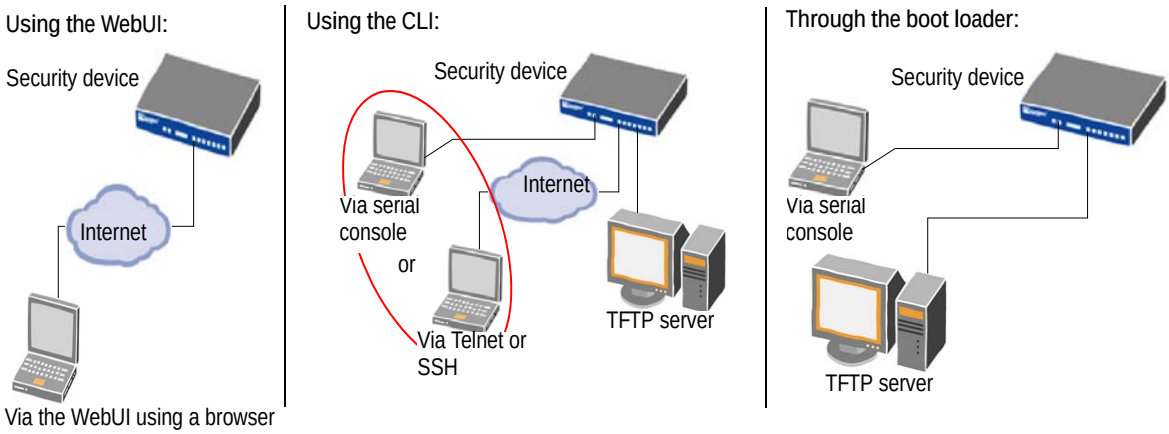
- Root or read-write privileges to the security device
- Console connection or Telnet access to the security device from a computer
- TFTP server installed locally and to which the security device has access
- New ScreenOS firmware (downloaded from the Juniper Networks Web site and saved to a local TFTP server directory)

To upgrade through the boot loader, you must have the following access:

- Root or read-write privileges to the security device
- TFTP server installed locally that has an IP address in the same subnet as the security device (255.255.255.0)
- Ethernet connection from a computer to the security device (to transfer data, namely from a local TFTP server)
- Console connection from the computer to the security device (to manage the device)
- New ScreenOS firmware saved to a local TFTP server directory

Figure 2 illustrates the three different ways by which you can upgrade a security device.

Figure 2: ScreenOS Upgrade Methods



To upgrade a security device, see the step-by-step procedures in "Upgrading to the New Firmware" on page 19 or "Upgrading Devices in an NSRP Configuration" on page 23.

Upgrading Boot Loaders

Some devices require that you upgrade the boot loader before or during the firmware upgrade. Depending on the device, you upgrade boot loaders (if needed) in one of two ways.

- Method 1—upgrading the boot loader, and then upgrading the firmware
- Method 2—upgrading the boot loader and, after rebooting, using the boot loader to upgrade the firmware

You can view the boot-loader version for ISG and NS-5000 Series devices by entering the **get envar** command. For SSG devices, reboot the device by using the console connection, and then checking the boot messages.

Method 1

The devices for which you upgrade the boot loader, and then upgrade the firmware are as follows:

- ISG 1000, ISG 2000, NS-5200/NS-5400

NOTE: For these devices, you only need to upgrade the boot loader if after you try to upgrade the firmware, you run into issues.

The sample procedure shows the boot loader upgrade steps for an ISG 2000.

- SSG 320M, SSG 350M, SSG 520, SSG 520M, SSG 550, SSG 550M

NOTE: For these devices, you should upgrade the boot loader to the latest version.

The sample procedure shows the boot loader upgrade steps for an SSG 500 device.

ISG 2000

To upgrade the boot loader for an ISG 2000 device to v1.1.6:

1. Download the boot loader from the Juniper Networks support site.
   a. Navigate your browser to http://www.juniper.net/customers/support/. The Support page appears.
   b. Locate the DOWNLOAD SOFTWARE section, and click **ScreenOS**. Enter your user ID and password in the LOGIN page that appears, and then click the **LOGIN** button. The ScreenOS page appears.
   c. In the table of software download versions, locate ISG-2000 and click version 6.1.
   d. In the Software tab (under Package), click ISG-2000_Boot_loader.
2. Save and extract the boot loader zip file and put it in the root directory of your TFTP server.
3. Start the TFTP server, if necessary.
4. Make an Ethernet connection from the device hosting the TFTP server to the MGT port on the ISG 2000 and a serial connection from your workstation to the console port on the ISG 2000.
5. Restart the ISG 2000 by entering the **reset** command. When prompted to confirm the command, press **y**. The following system output appears:

```
NetScreen NS-ISG 2000 BootROM V1.0.0 (Checksum: 8796E2F3)
Copyright (c) 1997-2004 NetScreen Technologies, Inc.
Total physical memory: 2048MB
Test - Pass
Initialization..... Done
```

6. Press the X and A keys sequentially to update the boot loader.

7. Enter the filename for the boot loader software you want to load (for example, enter load200v116.d.S), the IP address of the ISG 2000, and the IP address of your TFTP server. The following system output appears:

```
Serial Number [0079082004000043]: READ ONLY
BOM Version [E01]: READ ONLY
Self MAC Address [0010-db7a-bd80]: READ ONLY
OS Loader File Name [eng/n2000idp-PEK0z0gi]: load2000v116.d.S
Self IP Address [10.155.102.103]:
TFTP IP Address [10.155.127.253]:
```

8. Press **Enter** to load the file. The following system output appears:

```
Save loader config (112 bytes)... Done
Loading file "load2000v116.d.S"...
rtatatatatata...
Loaded successfully! (size = 383,222 bytes)
Ignore image authentication!
Program OS Loader to on-board flash memory...
++++++++++++++++++++++++Done!
Start loading...
.....
Done.
```

You have completed the upgrade of the boot loader and can now proceed to “Downloading New Firmware” on page 18.

SSG 500

To upgrade the boot loader for an SSG 500 device to v1.0.5:

1. Download the boot loader from the Juniper Networks support site.

   a. Navigate your browser to http://www.juniper.net/customers/support/. The Support page appears.

   b. Locate the DOWNLOAD SOFTWARE section, and click **ScreenOS**. Enter your user ID and password in the LOGIN page that appears, and then click the **LOGIN** button. The ScreenOS page appears.

   c. In the table of software download versions, locate SSG-500 and click version 6.1.

   d. In the Software tab (under Package), click SSG-500_Boot_loader.

2. Save and extract the boot loader zip file and put it in the root directory of your TFTP server.

3. Start the TFTP server, if necessary.

4. Make an Ethernet connection from the device hosting the TFTP server to the MGT port on the SSG 500 and a serial connection from your workstation to the console port on the SSG 500.

5. Restart the SSG 500 by entering the **reset** command. When prompted to confirm the command, press **y**. The following system output appears:

```
NetScreen SSG500 BootROM V1.0.2 (Checksum: 8796E2F3)
Copyright (c) 1997-2004 NetScreen Technologies, Inc.
Total physical memory: 512MB
Test - Pass
Initialization..... Done
```

6. Press the X and A keys sequentially to update the boot loader.

7. Enter the filename for the boot loader software you want to load (for example, enter loadssg500v105), the IP address of the SSG 500, and the IP address of your TFTP server. The following system output appears:

```
File Name [boot2.1.0.2]: loadssg500v105
Self IP Address [10.150.65.152]:
TFTP IP Address [10.150.65.151]:
```

8. Press **Enter** to load the file. The following system output appears:

```
Save loader config (112 bytes)... Done
Loading file "loadssg500v105"...
/
Loaded successfully! (size = 125,512 bytes)
Ignore image authentication!
...
.....................
Done.
```

You have completed the upgrade of the boot loader and can now proceed to “Downloading New Firmware” on page 18.

Method 2

The devices for which you upgrade the boot loader and, after rebooting, use the boot loader to upgrade the firmware are as follows:

- SSG 5, SSG 20, and SSG 140

NOTE: For these devices, you only need to upgrade the boot loader if after you try to upgrade the firmware, you run into issues.

The sample procedure shows the boot loader upgrade steps for an SSG 140 device.

To upgrade the boot loader for an SSG 140 device to v3.2.4:

1. Download the boot loader from the Juniper Networks support site.

   a. Navigate your browser to http://www.juniper.net/customers/support/. The Support page appears.

   b. Locate the DOWNLOAD SOFTWARE section, and click **ScreenOS**. Enter your user ID and password in the LOGIN page that appears, and then click the **LOGIN** button. The ScreenOS page appears.

c. In the table of software download versions, locate SSG-140 and click version 6.1.

d. In the Software tab (under Package), click SSG-140_6.1.0r1_Upgrade.

2. Save and extract the upgrade zip file and put it in the root directory of your TFTP server.

3. Start the TFTP server, if necessary.

4. Make an Ethernet connection from the device hosting the TFTP server to the MGT port on the SSG 140 and a serial connection from your workstation to the console port on the SSG 140.

5. Restart the SSG 140 by entering the **reset** command. When prompted to confirm the command, press **y**. The following system output appears:

```
Juniper Networks SSG-140 Boot Loader Version 3.2.3 (Checksum: ECD688CB)
Copyright (c) 1997-2006 Juniper Networks, Inc.
   Total physical memory: 512MB
   Test -  Pass
   Initialization - Done

Hit any key to run loader
Hit any key to run loader
```

6. At this point, press any key to run the loader. The following system output appears:

```
Serial Number [0185012007000097]: READ ONLY
HW Version Number [1010]: READ ONLY
Self MAC Address [0017-cb49-4d00]: READ ONLY
Boot File Name [release/firmware/6.1/ssg140]:
->: release/firmware/6.1/loadssg140v324.d
Self IP Address [10.150.35.229]:
TFTP IP Address [10.150.39.252]:
```

7. Press **Enter** to load the file. The following system output appears:

```
Save loader config (56 bytes)... Done
The configured TFTP server is connected to port 0

Loading file "release/firmware/6.1/loadssg140v324.d"...
r
Receiving data block ...
#448

Loaded Successfully! (size = 232,502 bytes)

Ignore image authentication

Save to on-board flash disk? (y/[n]/m)
```

8. At this point, when prompted to save to on-board flash disk, press **n**. (Because the boot loader upgrade is a one-time operation, you do not need to save it to on-board flash.) The following system output appears:

```
Run downloaded system image? ([y]/n)
```

9. At this point, when prompted to run the downloaded device image, press **y**. The following system output appears:

```
Start loading...
.............
Done.

*********************************************************
*       ==============================================      *
*            (c)1997-2006 Juniper Networks, Inc.          *
*                 All Rights Reserved                 *
*                                                     *
*       ____________________        *
*          SSG140 Boot Loader Version: 3.2.x              *
*       Compile Date: Dec  5 2007; Time: 13:45:25          *
*                                                     *
*       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!       *
*       !                                     !       *
*       ! Please don't power off during update.     !       *
*       ! Otherwise, the system can not boot again.  !       *
*       !                                     !       *
*       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!       *
*                                                     *
*      *** DON'T POWER OFF DURING BOOT LOADER UPDATE ***      *
*      *** DON'T POWER OFF DURING BOOT LOADER UPDATE ***      *
*      *** DON'T POWER OFF DURING BOOT LOADER UPDATE ***      *
*                                                     *
*********************************************************

Check on-board Boot Loader... Update needed!

Are you sure you want to update Boot Loader? (y/n)
```

10. At this point, when prompted to answer whether you want to update the boot loader, press **y**. The following system output appears:

```
Read product information of on-board boot flash device:
   Manufacturer ID = 01
   Device ID       = 4f

Boot flash device is Am29LV040B

Erase on-board boot flash device..... Done

Update Boot
Loader.....
Done

Verify Boot Loader... Done
Boot Loader has been updated successfully!
```

You have completed the upgrade of the boot loader. The system will reboot and you can now proceed to “Downloading New Firmware” on page 18.

Downloading New Firmware

You can obtain the ScreenOS firmware from the Juniper Networks Web site. To access firmware downloads, you must be a registered customer with an active user ID and password. If you have not yet registered your Juniper Networks product, then you must do so at the Juniper Networks Web site before proceeding.

NOTE: Before you begin a security device upgrade, you must have the most recent ScreenOS firmware. Check Table 1 on page 10 to make sure you have the required intermediate software, if any.

To get the latest ScreenOS firmware:

1. Navigate your browser to http://www.juniper.net/customers/support/. The Support page appears.

   a. Locate the DOWNLOAD SOFTWARE section, and click **ScreenOS**. Enter your user ID and password in the LOGIN page that appears, and then click the **LOGIN** button. The ScreenOS page appears.

   b. In the table of software download versions, locate the device for which you want to download software and click the version you want.

   c. In the Software tab (under Package), click the upgrade link. For some devices, you need to click the management module link before you can access the Software tab.

2. Click **Save**, then navigate to the location where you want to save the firmware zip file.

NOTE: Before loading the firmware, you must unzip the file.

You must save the firmware onto the computer from which you want to perform the upgrade.

If you want to upgrade the security device using the WebUI, save the firmware anywhere on the computer.

If you want to upgrade the security device using the CLI, save the firmware in the root TFTP server directory on the computer. If you do not have a TFTP server installed on your computer, then you can download one from the Internet. If no TFTP server is available, then you must use the WebUI to load the new firmware onto the security device.

Upgrading to the New Firmware

This section provides instructions for upgrading firmware on the security device using the WebUI, the CLI, and the boot loader. This section also describes how to save multiple firmware images with the boot loader.

CAUTION: Before upgrading a security device, save the existing configuration file to avoid losing any data.

Check Table 1 on page 10 to determine whether you need to install intermediate firmware or a boot-loader upgrade before installing ScreenOS 6.1.0. Use either the WebUI or CLI procedure to first install intermediate firmware (if required), and then install ScreenOS 6.1.0 firmware.

Upgrading Using the WebUI

This section describes how to upgrade the firmware on the security device using the WebUI. Instructions include upgrading to an intermediate version of firmware, if required, and then upgrading to ScreenOS 6.1.0.

To upgrade firmware using the WebUI:

1. Log into the security device by opening a browser.
   a. Enter the management IP address in the Address field.
   b. Log in as the root admin or an admin with read-write privileges.
2. Save the existing configuration.
   a. Go to **Configuration > Update > Config File**, and then click **Save To File**. The File Download dialog box appears.
   b. Click **Save**.
   c. Navigate to the location where you want to save the configuration file (cfg.txt), and then click **Save**.
3. Upgrade to intermediate firmware, if required.

   See Table 1 on page 10 to determine if intermediate firmware is required. If intermediate firmware is required, perform the following steps. Otherwise, proceed to Step 4.

   a. Go to **Configuration > Update > ScreenOS/Keys**, and then select **Firmware Update**.
   b. Click **Browse** to navigate to the location of the intermediate firmware. For example, if you upgrade a NetScreen-5000 running ScreenOS 5.4r1, you must upgrade to ScreenOS 5.4r3 or later, and then continue this procedure.
   c. Click **Apply**.

NOTE: This process takes some time. Do not click **Cancel** or the upgrade will fail. If you do click **Cancel** and the upgrade fails, power off the device, then power it on again. Restart the upgrade procedure beginning with Step 3.

d. Click **OK** to continue.

The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

e. Log into the security device. You can verify the version of the security device ScreenOS firmware in the Device Information section of the WebUI page.

4. Upgrade to the new ScreenOS firmware.

a. Go to **Configuration > Update > ScreenOS/Keys**, and then select **Firmware Update**.

b. Click **Browse** to navigate to the location of the new ScreenOS firmware, or enter the path to its location in the Load File field.

c. Click **Apply**.

A message box appears with information on the upgrade time.

d. Click **OK** to continue.

The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

5. Log into the security device. You can verify the version of the security device ScreenOS firmware in the Device Information section of the WebUI page.

Upgrading Using the CLI

This section describes how to upgrade the firmware on the security device using the CLI. Instructions include upgrading to an intermediate version of the firmware, if required, and upgrading to ScreenOS 6.1.0.

To upgrade firmware using the CLI:

1. Make sure you have the new ScreenOS firmware (or the intermediate firmware, if required) in the TFTP root directory. For information on obtaining the new firmware, see “Downloading New Firmware” on page 18.

2. Run the TFTP server on your computer by double-clicking the TFTP server application. You can minimize this window, but it must be active in the background.

3. Log into the security device using an application such as Telnet or SSH (or HyperTerminal if connected directly through the console port). Log in as the root admin or an admin with read-write privileges.

4. Save the existing configuration by running the following command:

   save config to { **flash** | **slot1** | **tftp** }...

5. Enter the following command on the security device and specify the filename of the firmware (if you are installing intermediate firmware, specify the filename of the intermediate firmware):

   save soft from tftp *ip_addr screenos_filename* **to flash**

   where *ip_addr* is the IP address of your computer and *screenos_filename* is the filename of the ScreenOS 6.1.0 firmware.

NOTE: If this upgrade requires intermediate firmware and you have not already upgraded to that firmware, enter the intermediate firmware filename when entering this command.

---

6. Reset the security device when the upgrade is complete. Run the **reset** command and enter **y** at the prompt to reset the device.

7. Wait a few minutes, and then log into the security device again.

8. Use the **get system** command to verify the version of the security device ScreenOS firmware.

   If you upgraded to intermediate firmware, repeat Steps 5 through 8 to install the ScreenOS 6.1.0 firmware.

9. If necessary, download the configuration file that you saved in Step 4 by executing the following command:

   save config from tftp to { **flash** | **slot1** | **tftp** }...

Upgrading Using the Boot Loader

The boot loader brings up the hardware system, performs basic and sometimes critical hardware configurations, and loads system software used to run a security device.

To upgrade firmware using the boot loader:

1. Connect your computer to the security device.

   a. Using a serial cable, connect the serial port on your computer to the console port on the security device (refer to your hardware manual for console settings). This connection, in combination with a terminal application, enables you to manage the security device.

   b. Using an Ethernet cable, connect the network port on your computer to port 1 or to the management port on the security device. This connection enables the transfer of data among the computer, the TFTP server, and the security device.

2. Make sure you have the new ScreenOS firmware stored in the TFTP server directory on your computer. For information on obtaining the new firmware, see “Downloading New Firmware” on page 18.

3. Run the TFTP server on your computer by double-clicking the TFTP server application. You can minimize this window, but it must be active in the background.

4. Log into the security device using a terminal emulator such as HyperTerminal. Log in as the root admin or an admin with read-write privileges.

5. Restart the security device.

6. Press any key on your computer when you see “Hit any key to run loader” or “Hit any key to load new firmware” on the console display. This interrupts the startup process.

NOTE: If you do not interrupt the security device in time, it loads the firmware saved in flash memory.

---

7. Enter the filename of the ScreenOS firmware that you want to load at the Boot File Name prompt.

NOTE: If Table 1 on page 10 lists an intermediate firmware requirement, enter that filename at this step.

   If you enter **slot1:** before the specified filename, then the loader reads the specified file from the external compact flash or memory card. If you do not enter **slot1:** before the filename, then the file is downloaded from the TFTP server. If the security device does not support a compact flash card, then an error message is displayed and the console prompts you to reenter the filename.

8. Enter an IP address that is on the same subnet as the TFTP server at the Self IP Address prompt.

9. Enter the IP address of the TFTP server at the TFTP IP Address prompt.

NOTE: The self IP address and TFTP IP address must be in the same subnet; otherwise, the TFTP loader rejects the self IP address and then prompts you to reenter it.

   An indication that the firmware is loading successfully is the display of a series of “rtatatatatatata…” running on the terminal-emulator screen and a series of symbols running on the TFTP server window. When the firmware installation is complete, a message informs you that the installation was successful. Repeat these steps if your first firmware upgrade was to an intermediate version.

Upgrading Devices in an NSRP Configuration

For security devices in a NetScreen Redundancy Protocol (NSRP) configuration, you must upgrade each device individually. There are two different NSRP configurations: NSRP active/passive and NSRP active/active. The following sections describe the procedures for each of these NSRP configurations.

The procedures apply only to firmware upgrades, and assume that the devices are identical and that there are no hardware changes. If there is any hardware change, you should consult the corresponding hardware guide for each platform.

CAUTION: Before upgrading a security device, save the existing configuration file to avoid losing any data.

Upgrading Devices in an NSRP Active/Passive Configuration

This section describes the steps for upgrading a basic NSRP active/passive configuration, where device A is the primary device and device B is the backup device. Before you begin, read "Requirements for Upgrading Device Firmware" on page 11. Also make sure you download the ScreenOS firmware to which you are upgrading each device.

WARNING: Do not power off your security device while it is upgrading to new firmware. Doing so could permanently damage the device.

To upgrade two devices in an NSRP active/passive configuration (some steps require CLI use):

1. Upgrade device B to ScreenOS 6.1.0.

From the WebUI

a. Make sure you have the new ScreenOS firmware (and the intermediate firmware, if required). For information on obtaining the firmware, see "Downloading New Firmware" on page 18.

b. Log into device B by opening a browser and entering the management IP address in the Address field. Log in as the root admin or an admin with read-write privileges.

c. Save the existing configuration:

1. Go to **Configuration > Update > Config File,** and then click **Save to File**.
2. Click **Save** in the File Download dialog box.
3. Navigate to the location where you want to save the configuration file (cfg.txt), and then click **Save**.

d. Click **Configuration > Update > ScreenOS/Keys**, and then select **Firmware Update**.

e. Click **Browse** to navigate to the location of the ScreenOS 6.1.0 firmware, or enter the path to its location in the Load File box.

f. Click **Apply**.

A message box appears with information on the upgrade time.

g. Click **OK** to continue.

The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

h. Verify the version of the ScreenOS firmware, by logging into the security device and locating the Device Information section of the WebUI page.

From the CLI

a. Make sure you have the ScreenOS 6.1.0 firmware (and the intermediate firmware, if required). For information on obtaining the firmware, see "Downloading New Firmware" on page 18.

b. Log into device B using an application such as Telnet or SSH (or HyperTerminal if directly connected through the console port). Log in as the root admin or an admin with read-write privileges.

c. Save the existing configuration by running the following command:

save config to { **flash** | **slot1** | **tftp** }...

d. Run the TFTP server on your computer by double-clicking the TFTP server application.

e. Enter the following command on the security device:

save soft from tftp *ip_addr filename* **to flash**

where *ip_addr* is the IP address of your computer and *filename* is the filename of the ScreenOS 6.1.0 firmware.

f. Enter the **reset** command when the upgrade is complete, and then enter **y** at the prompt to reset the device.

g. Wait a few minutes, and then log into the security device.

h. Enter the **get system** command to verify the version of the security device ScreenOS firmware.

2. Manually fail over the primary device to the backup device (CLI only).

From the CLI

a. Log into the primary device (device A).

b. Issue one of the following CLI commands. The command that you need to run depends on whether or not the **preempt** option is enabled on the primary device.

- If the **preempt** option is enabled:

exec nsrp vsd-group 0 mode ineligible

- If the **preempt** option is not enabled:

  exec nsrp vsd-group 0 mode backup

  Either command forces the primary device to step down and the backup device to immediately assume the primary device role.

3. Upgrade the primary device (device A) to ScreenOS 6.1.0.

From the WebUI

a. Make sure you have the ScreenOS 6.1.0 firmware. For information on obtaining the firmware, see "Downloading New Firmware" on page 18.

b. Log into security device A.

c. Save the existing configuration:

   1. Go to **Configuration > Update > Config File**, and then click **Save to File**.
   2. Click **Save** in the File Download dialog box.
   3. Navigate to the location where you want to save the configuration file (cfg.txt), and then click **Save**.

d. Click **Configuration > Update > ScreenOS/Keys**, and then select **Firmware Update**.

e. Click **Browse** to navigate to the location of the ScreenOS 6.1.0 firmware or enter the path to its location in the Load File box.

f. Click **Apply**.

   A message box appears with information on the upgrade time.

g. Click **OK** to continue.

   The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

h. Verify the version of the ScreenOS firmware, by logging into the security device and locating the Device Information section of the WebUI page.

From the CLI

a. Make sure you have the ScreenOS 6.1.0 firmware. For information on obtaining the firmware, see "Downloading New Firmware" on page 18.

b. Log into security device A.

c. Save the existing configuration by running the following command:

   save config to { **flash** | **slot1** | **tftp** }...

d. Run the TFTP server on your computer by double-clicking the TFTP server application.

e. Run the following command on the security device:

save soft from tftp *ip_addr screenos_filename* **to flash**

where *ip_addr* is the IP address of your computer, and *screenos_filename* is the filename of the ScreenOS 6.1.0 firmware.

f. Reset the security device when the upgrade is complete. Run the **reset** command and enter **y** at the prompt to reset the device.

g. Wait a few minutes, and then log into the security device again. You can verify the security device ScreenOS firmware version by using the **get system** command.

4. Synchronize device A (CLI only).

From the CLI

After you complete the upgrade of device A to ScreenOS 6.1.0, manually synchronize the two devices. On device A (backup), issue the **exec nsrp sync rto all from peer** command from the peer CLI to synchronize the RTOs from device B (primary device).

5. Manually fail over the primary device to the backup device (CLI only).

From the CLI

a. Log into the primary device (device B).

b. If the **preempt** option is enabled on device A, no action is needed. If the **preempt** option is not enabled on device A, issue the following command:

exec nsrp vsd-group 0 mode backup

Either command forces the primary device to step down and the backup device to immediately assume the primary device role.

Upgrading Devices in an NSRP Active/Active Configuration

This section applies to an NSRP configuration where you paired two security devices into two virtual security device (VSD) groups, with each physical device being the primary in one group and the backup in the other. To upgrade, you first have to fail over one of the devices so that only one physical device is the primary of both VSD groups. You then upgrade the backup device first and the primary device second.

The following illustrates a typical NSRP active/active configuration where device A is the primary device for VSD 0 and the backup for VSD 1, and device B is the primary device for VSD 1 and the backup for VSD 0.

Before you begin, see “Requirements for Upgrading Device Firmware” on page 11. Also make sure you download the ScreenOS 6.1.0 firmware (and intermediate firmware, if required).

WARNING: Do not power off your security device while it is upgrading to new firmware. Doing so could permanently damage the device.

To upgrade two devices in an NSRP active/active configuration (some steps require CLI use):

From the CLI

1. Manually fail over the master device B in VSD group 1 to the backup device A in VSD group 1 (CLI only):

   a. Log into device B using an application such as Telnet or SSH (or HyperTerminal if directly connected through the console port). Log in as the root admin or an admin with read-write privileges.

   b. Issue one of the following CLI commands. The command you need to run depends on whether or not the **preempt** option is enabled on the master device.

      - If the **preempt** option is enabled:

        exec nsrp vsd-group 1 mode ineligible

      - If the **preempt** option is not enabled:

        exec nsrp vsd-group 1 mode backup

   Either command forces device B to step down and device A to immediately assume the primary role of VSD 1. At this point, device A is the primary of both VSD 0 and 1 and device B is the backup for both VSD 0 and 1.

2. Upgrade device B to the ScreenOS 6.1.0 firmware.

From the WebUI

   a. Make sure you have the 6.1.0 ScreenOS firmware (and the intermediate firmware, if required). Check Table 1 on page 10 for details. For information on obtaining the firmware, see "Downloading New Firmware" on page 18.

   b. Log into security device B by opening a browser and entering the management IP address in the Address field. Log in as the root admin or an admin with read-write privileges.

   c. Save the existing configuration:

      1. Go to **Configuration > Update > Config File**, and then click **Save to File**.
      2. Click **Save** in the File Download dialog box.
      3. Navigate to the location where you want to save the configuration file (cfg.txt), and then click **Save**.

   d. Click **Configuration > Update > ScreenOS/Keys**, and then select **Firmware Update**.

   e. Click **Browse** to navigate to the location of the ScreenOS 6.1.0 firmware or enter the path to its location in the Load File box.

   f. Click **Apply**.

      A message box appears with information on the upgrade time.

g. Click **OK** to continue.

The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

h. Verify the version of the ScreenOS firmware, by logging into the security device and locating the Device Information section of the WebUI page.

From the CLI

a. Make sure you have the ScreenOS 6.1.0 firmware. For information on obtaining the firmware, see "Downloading New Firmware" on page 18.

b. Log into device B.

c. Save the existing configuration by running the following command:

save config to { **flash** | **slot1** | **tftp** }...

d. Run the TFTP server on your computer by double-clicking the TFTP server application.

e. Enter the following command on the security device:

save soft from tftp *ip_addr screenos_filename* **to flash**

where *ip_addr* is the IP address of your computer and *screenos_filename* is the ScreenOS 6.1.0 firmware.

f. Reset the security device when the upgrade is complete. Run the **reset** command and enter **y** at the prompt to reset the device.

g. Wait a few minutes, and then log into the security device again. You can verify the security device ScreenOS firmware version by using the **get system** command.

3. Manually fail over device A completely to device B (CLI only).

From the CLI

a. Log into device A.

b. Fail over primary device A in VSD 0 to backup device B in VSD 0 by issuing one of the following CLI commands. The command you need to run depends on whether or not the **preempt** option is enabled on the primary device.

- If the **preempt** option is enabled:

  exec nsrp vsd-group 0 mode ineligible

- If the **preempt** option is not enabled:

  exec nsrp vsd-group 0 mode backup

c. If the **preempt** option is enabled on device A, no action is needed. If the **preempt** option is not enabled on device A, issue the following command:

```
exec nsrp vsd-group 1 mode backup
```

At this point, device B is the primary device for both VSD 0 and 1, and device A is backup for both VSD 0 and 1.

4. Upgrade device A to ScreenOS 6.1.0.

From the WebUI

a. Make sure you have the ScreenOS 6.1.0 firmware (and the intermediate firmware, if required). Check Table 1 on page 10 for software details. For information on obtaining the firmware, see "Downloading New Firmware" on page 18.

b. Log into security device A.

c. Save the existing configuration:

1. Go to **Configuration > Update > Config File**, and then click **Save to File**.
2. Click **Save** in the File Download dialog box.
3. Navigate to the location where you want to save the configuration file (cfg.txt), and then click **Save**.

d. Click **Configuration > Update > ScreenOS/Keys**, and then select **Firmware Update**.

e. Click **Browse** to navigate to the location of the ScreenOS 6.1.0 firmware, or enter the path to its location in the Load File box.

f. Click **Apply**.

A message box appears with information on the upgrade time.

g. Click **OK** to continue.

The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

h. Verify the version of the ScreenOS firmware, by logging into the security device and locating the Device Information section of the WebUI page.

From the CLI

a. Make sure you have the ScreenOS 6.1.0 firmware. For information on obtaining the firmware, see "Downloading New Firmware" on page 18.

b. Log into device A.

c. Save the existing configuration by running the following command:

save config to { **flash** | **slot1** | **tftp** }...

d. Run the TFTP server on your computer by double-clicking the TFTP server application.

e. Enter the following command on the security device:

save soft from tftp *ip_addr screenos_filename* **to flash**

where *ip_addr* is the IP address of your computer, and *screenos_filename* is the filename of the ScreenOS 6.1.0 firmware.

f. Reset the security device when the upgrade is complete. Run the **reset** command, and then enter **y** at the prompt to reset the device.

g. Wait a few minutes, and then log into the security device again. You can verify the security device ScreenOS firmware version by using the **get system** command.

5. Synchronize device A (CLI only).

From the CLI

After you complete the upgrade of device A to ScreenOS 6.1.0, manually synchronize the two devices. On device A, issue the **exec nsrp sync rto all** command from the peer to synchronize the RTOs from device B.

6. Fail over device B in VSD 0 to device A in VSD 0 (CLI only).

As the final step, return the devices to an active/active configuration.

a. Log into device A.

- If the **preempt** option is enabled on device A, no action is needed. If the **preempt** option is not enabled on device A, issue the following command:

exec nsrp vsd-group 1 mode backup

Now device A is the primary device for VSD 0 and the backup for VSD 1, and device B is the primary device for VSD 1 and the backup for VSD 0.

Scan Manager Profile

The global **scan-mgr** command controls the embedded scan manager, which is the AV component that interacts with the scan engine. For example, the **set** or **get av scan-mgr** CLI command sets the global commands that control parameters, such as max-content-size, max-msgs, pattern-type, pattern-update, and queue-size.

In ScreenOS 5.3.0 and later, some of the previous global settings are now configured from within a profile context. For example, global commands such as **timeout** and **max-decompress-layer** are no longer global; they are now set within the profile for each protocol. Commands such as **max-content-size** and **max-msgs**, which configure the embedded scan manager, are global and are now set using the **set av scan-mgr** command.

When you upgrade to ScreenOS 5.3.0 or later, a scan manager profile named **scan-mgr** is automatically generated to migrate the global **scan-mgr** commands. The **scan-mgr** profile runs the following commands:

```
set ftp decompress-layer 2
set http decompress-layer 2
set imap decompress-layer 2
set pop3 decompress-layer 2
set smtp decompress-layer 2
set http skipmime enable
set http skipmime mime-list ns-skip-mime-list
```

Table 2 shows the updated commands in ScreenOS 6.1.0. Updated commands are now entered from within a policy context.

Table 2: Command Updates

Commands Previous to ScreenOS 5.3.0	Commands for ScreenOS 5.3.0 and Later Within a Profile Context
set av http skipmime	set av profile scan-mgr set http skipmime mime-list ns-skip-mime-list set http skipmime enable exit
unset av http skipmime	set av profile scan-mgr unset http skipmime enable exit
set av scan-mgr content { FTP | HTTP | IMAP | POP3 | SMTP } [timeout *number*] }	set av profile scan-mgr set { FTP | HTTP | IMAP | POP3 | SMTP { enable | timeout *number* } } exit
unset av scan-mgr content { FTP | HTTP | IMAP | POP3 | SMTP }	set av profile scan-mgr unset { FTP | HTTP | IMAP | POP3 | SMTP } enable exit

AV Pattern Update URL

The locations for AV pattern updates can be found at:

www.update.juniper-updates.net/AV/SSG5_SSG20/
www.update.juniper-updates.net/AV/SSG100/
www.update.juniper-updates.net/AV/SSG500/
www.update.juniper-updates.net/AV/SSG300/

If you have upgraded your ScreenOS release, you might want to check that the pattern update URL has been modified by using the **get av scan-mgr** command. For example:

```
ssg5-serial-> get av scan-mgr
<AV scan engine info>
AV Key Expire Date: 11/21/2009 00:00:00
Update Server: http://update.juniper-updates.net/AV/SSG5_SSG20/
interval: 10 minutes
auto update status: next update in 10 minutes
last result: download list file failed
```

pattern update proxy status: OFF
AV signature version: 12/25/2007 09:33 GMT, virus records: 149961
Scan Engine Info: last action result: No error(0x00000000), memory left 55084kB
Scan engine default file extension list:
386;ACE;ARJ;ASP;BAT;BIN;BZ2;CAB;CHM;CLA;CMD;COM;CPL;DLL;DOC;DOT;DPL;DRV;
DWG;ELF;EMF;EML;EXE;FON;FPM;GEA;GZ;HA;HLP;HTA;HTM;HTML;HTT;HXS;ICE;INI;
ITSF;JAR;JPEG;JPG;JS;JSE;LHA;LNK;LZH;MBX;MD?;MIME;MSG;MSI;MSO;NWS;OCX;
OTM;OV?;PDF;PHP;PHT;PIF;PK;PL;PLG;PP?;PRG;PRJ;RAR;REG;RTF;SCR;SH;SHS;SWF;
SYS;TAR;TGZ;THE;TSP;VBE;VBS;VXD;WSF;WSH;XL?;XML;ZIP;
pattern type: standard
max content size: 10000(k) (drop if exceeds)
max-msgs: 256 (drop if exceeds)
decompress layer: (drop if exceeds)
password file: (pass if occurs)
corrupt file: (pass if occurs)
out of resource: (drop if occurs)
scan engine is not ready: (drop if occurs)
timeout: (drop if occurs)