Image Authentication Readme

November 2008

Part No. 530-028084-01
Revision 02

ScreenOS includes the ability to determine the authenticity of binary images provided by Juniper Networks. An image authentication signature has been incorporated into each ScreenOS build since version 2.6.1r1. When the ScreenOS authentication certificate (imagekey.cer) has been loaded beforehand onto a Juniper Networks firewall or VPN device, each time the device is rebooted, ScreenOS will validate the authenticity of the image saved in flash. If the validation fails, the device will not load the image.

Validating the authenticity of an image enhances security and stability. When this feature is enabled, ScreenOS rejects illegitimate or damaged images before they will be booted onto the device, forcing the system administrator to save an authentic software image in the device before it will boot, and thereby protecting the device against unsafe and potentially unstable software.

Loading the Image Authentication Certificate

It is important to ensure the integrity of the certificate itself before you load it on the Juniper Networks security device. You can confirm the certificate's integrity by comparing the MD5 Checksum of the imagekey.cer certificate file to the value below. A tool such as FastSum for Windows (www.fastsum.com) or md5sum for Unix/Linux can be used.

```
CCFCD027E20C9CC38B5D8DAC17C7199F
```

When you feel confident about the integrity of the certificate file, you can load it on the Juniper Networks security device through either the WebUI or the CLI.

WebUI

To load the authentication certificate using the WebUI, do the following:

1. Save the **imagekey.cer** file to accessible local storage.
2. Login to the device.
3. Navigate to **Configuration** > **Update > ScreenOS/Keys** using the navigation tree on the left side of the screen.

4. Select the **Image Signature Key Update** radio button and click **Browse**.
5. Navigate to the location where you saved the certificate and click **Open**.
6. Click **Apply**.

CLI

To load the authentication certificate using the CLI, do the following:

1. Save **imagekey.cer** to the root directory of a TFTP server.
2. Start the TFTP server.
3. Make a console, Telnet, or SSH connection to the Juniper Networks security device, log in, and enter the following CLI command:

   save image-key tftp *ip_addr* **imagekey.cer**

   in which *ip_addr* is the address of the TFTP server.

Checking that an Image Authentication Certificate is Installed

You can ensure that the authentication key is properly installed on the firewall device from the CLI by running the following command.

```
exec pki test skey
```

If the key is installed, you will see output similar to the below. The output should show non-zero values. If the output shows all zeros (0), then the certificate is not installed.

Example: The following example shows that a certificate is installed.

```
SSG140-> exec pki test skey
exec pki test <skey>.
Flash base = 0xd1000000, Flash end = 0x0, sector size= 0x20000

KEY1  N/A len =432
 308201ac02010002818100fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c
31e3f80b651     magic1 = f7e9294b magic2=0

KEY2  N/A len =432
 308201ac02010002818100fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400
c31e3f80b651     magic1 = f7e9294b magic2=0

KEY3  N/A len =432
 308201ac02010002818100fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400
c31e3f80b651     magic1 = f7e9294b magic2=0
```

Example: The following example shows that a certificate is NOT installed.

```
nshsc-> exec pki test skey

exec pki test <skey>.

Flash base = 0x51000000, Flash end = 0x0, sector size= 0x4000

KEY1  N/A len =0

00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000

000     magic1 = f7e9294b magic2=0



KEY2  N/A len =0


00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000

000     magic1 = f7e9294b magic2=0



KEY3  N/A len =0


00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000

00      magic1 = f7e9294b magic2=0
```

Authenticating a ScreenOS Image

Every time your device boots a ScreenOS image from flash, it uses the authentication certificate (if installed) to check the ScreenOS signature embedded in the file. The authentication effort produces one of the following two results:

- If you are logged in through a console connection and the Juniper Networks security device can successfully authenticate the image, the image loader displays the following message during the reboot sequence:

  ```
  Loaded Successfully! . . .
  Image authenticated!
  ```

- If the Juniper Networks security device cannot authenticate the ScreenOS image, it does not boot it and instead either prompts you to load another image or automatically reboots and loads the previously saved image. When logged in through a console connection, you see the following when the device prompts you to load another image:

```
********Invalid DSA signature
*******Bogus Image - not authenticated
Serial Number [ . . . ]: READ ONLY
HW Version Number [ . . . ]: READ ONLY
Self MAC Address [ . . . ]: READ ONLY
Boot File Name [ . . . ]:
```

If this occurs, you must load a valid ScreenOS build.

- To reload the image previously running on the device, reboot the device by either powering it off and on or by typing ++++ at the prompt.

- To load a different image, delete the corrupted image file, download another ScreenOS build to the root directory of your TFTP server, and type its file name at the prompt before pressing Enter.

  NOTE: If the authentication certificate is not loaded, the Juniper Networks security device does not attempt to authenticate a ScreenOS image and will display the message "Ignore Image authentication!" message during bootup. To remove the certificate, enter the "delete crypto auth-key" command.

Juniper Networks Documentation

To obtain technical documentation for any Juniper Networks security product, visit www.juniper.net/techpubs/.

If you find any errors or omissions in the following content, please contact us at the following e-mail address: techpubs-comments@juniper.net.