



Security Threat Response Manager

Managing Vulnerability Assessment

Release 2009.2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Published: 2010-09-16

Copyright Notice

Copyright © 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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 NetScreen's 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.

Managing Vulnerability Assessment
Release 2009.2

Copyright © 2010, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

September 2010—Revision 2

The information in this document is current as of the date listed in the revision history.

CONTENTS

ABOUT THIS GUIDE

Conventions	5
Documentation Feedback	5
Requesting Technical Support	6

1 OVERVIEW

Configuring Vulnerability Assessment	7
Installing Scanners	8
Viewing Scanners	9

2 MANAGING NCIRCLE IP360 SCANNERS

Adding an ip360 Scanner	12
Editing an ip360 Scanner	14
Deleting an ip360 Scanner	15
Exporting Scan Reports	15

3 MANAGING NESSUS SCANNERS

Adding a Nessus Scanner	18
Editing an Nessus Scanner	20
Deleting a Nessus Scanner	21

4 MANAGING NESSUS SCAN RESULT IMPORTERS

Adding a Nessus Scan Result Importer	23
Editing a Nessus Scan Result Importer	25
Deleting a Nessus Scan Result Importer	26

5 MANAGING NMAP SCANNERS

Adding a Nmap Scanner	27
Editing an Nmap Scanner	29
Deleting an Nmap Scanner	30

6 MANAGING QUALYS SCANNERS

Adding a Qualys Scanner	31
Editing a Qualys Scanner	35
Deleting a Qualys Scanner	35

7 MANAGING FOUNDSCAN SCANNERS

- Adding a FoundScan Scanner 38
- Editing a FoundScan Scanner 40
- Deleting a FoundScan Scanner 40
- Using Certificates 41
 - Obtaining a Certificate 41
 - Importing Certificates 41
 - Example Of TrustedCA.pem File 43
 - Example of Portal.pem File 43

8 MANAGING JUNIPER NETWORKS NSM PROFILER SCANNERS

- Configuring a Juniper NSM Profile Scanner 47
- Adding a Juniper NSM Profiler Scanner 49
- Editing a Profiler Scanner 50
- Deleting a Profiler Scanner 50

9 MANAGING RAPID7 NEXPOSE SCANNERS

- Adding a Rapid7 NeXpose Scanner 53
- Editing a Rapid7 NeXpose Scanner 55
- Deleting a Rapid7 NeXpose Scanner 55

10 MANAGING NETVIGILANCE SECURESCOUT SCANNERS

- Adding a SecureScout Scanner 58
- Editing a SecureScout Scanner 59
- Deleting a SecureScout Scanner 60

11 MANAGING EYE REM SCANNERS

- Adding an eEye REM Scanner 62
- Editing an eEye REM Scanner 63
- Deleting an eEye REM Scanner 64

12 MANAGING PATCHLINK SCANNERS

- Adding a PatchLink Scanner 65
- Editing a PatchLink Scanner 67
- Deleting a PatchLink Scanner 67

13 MANAGING MCAFEE VULNERABILITY MANAGER SCANNERS

- Adding a McAfee Vulnerability Manager Scanner 70
- Editing a McAfee Vulnerability Manager Scanner 72
- Deleting a McAfee Vulnerability Manager Scanner 72
- Using Certificates 73
 - Obtaining Certificates 73
 - Processing Certificates 74
 - Importing Certificates into STRM 74

14 MANAGING SCAN SCHEDULES

Viewing Scheduled Scans 75

Scheduling a Scan 77

Editing a Scan Schedule 79

Deleting a Scheduled Scan 80

INDEX




ABOUT THIS GUIDE

The *Managing Vulnerability Assessment Guide* provides you with information for managing vulnerability scanners and scan schedules using STRM.

Conventions

[Table 1](#) lists conventions that are used throughout this guide.

Table 1 Icons

Icon	Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, device, or network.
	Warning	Information that alerts you to potential personal injury.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

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/us/en/local/pdf/resource-guides/7100059-en.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/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- 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 release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://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 Management tool: <http://www.juniper.net/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 Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

1

OVERVIEW

Vulnerability assessment integration enables vulnerability assessment data to build profiles of attackers and targets. Vulnerability assessment data uses correlated event data, network activity, and behavioral changes to remove false positives to determine the threat level for each critical business asset.

STRM's integration with vulnerability assessment tools allows you to schedule scans to keep your vulnerability assessment data up-to-date.



Note: You must have permissions to all CIDRs you want to scan. Also, do not include CIDRs in your vulnerability assessment that are configured in your global exclusions list. For more information on global exclusions, see the *Offense Resolutions Users Guide*.

This chapter provides an overview of configuring vulnerability assessment, including:

- [Configuring Vulnerability Assessment](#)
- [Installing Scanners](#)
- [Viewing Scanners](#)

Configuring Vulnerability Assessment

To configure vulnerability assessment, you must:

- Step 1** Install the scanner RPM, if necessary.
For more information, see [Installing Scanners](#).
- Step 2** Configure your scanner using one of the following supported scanners:
 - [Chapter 2 Managing nCircle ip360 Scanners](#)
 - [Chapter 3 Managing Nessus Scanners](#)
 - [Chapter 4 Managing Nessus Scan Result Importers](#)
 - [Chapter 5 Managing Nmap Scanners](#)
 - [Chapter 6 Managing Qualys Scanners](#)
 - [Chapter 7 Managing FoundScan Scanners](#)

- [Chapter 8 Managing Juniper NSM Profiler Scanners](#)
- [Chapter 9 Managing Rapid7 NeXpose Scanners](#)
- [Chapter 10 Managing netVigilance SecureScout Scanners](#)
- [Chapter 11 Managing eEye REM Scanners](#)
- [Chapter 12 Managing PatchLink Scanners](#)
- [Chapter 13 Managing McAfee Vulnerability Manager Scanners](#)

The scanner determines the tests performed during the scanning of a host. The selected scanner populates your asset profile data including the host information, ports, and potential vulnerabilities.

Step 3 Schedule vulnerability assessment. See [Chapter 14 Managing Scan Schedules](#).



Note: If you add, edit, or delete a scanner, you must click **Deploy Changes** from the Admin tab menu for the changes to take effect.

The results of the scan provides the operating system and version on each CIDR, server, and version of each port. Also, the scan provides the known vulnerabilities on discovered ports and services.

Installing Scanners To update or install a new scanner, you can install the scanner files located on the Juniper customer support web site.

To install a scanner:

Step 1 Download the file to your system hosting STRM.

Step 2 Log in to your STRM Console, as root.

Step 3 Navigate to the directory that includes the downloaded file.

Step 4 Enter the following command:

```
rpm -Uvh <filename>
```

Where **<filename>** is the name of the downloaded file. For example:

```
VIS-6.3-IP360-4.0-3.i386.rpm
```

Step 5 Log in to the STRM interface.

```
https://<IP Address>
```

Where **<IP Address>** is the IP address of the STRM system.

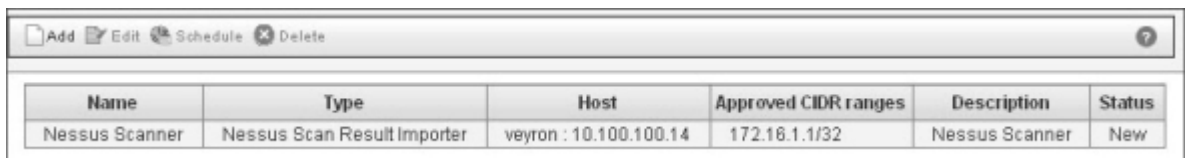
Step 6 Click the **Admin** tab.

The Administration interface appears.

Step 7 From the menu, click **Deploy Changes**.

Viewing Scanners To view currently configured scanners:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.



Name	Type	Host	Approved CIDR ranges	Description	Status
Nessus Scanner	Nessus Scan Result Importer	veyron : 10.100.100.14	172.16.1.1/32	Nessus Scanner	New

The VA Scanners window provides the following details for each scanner:

Table 1-1 Scanner Parameters

Parameter	Description
Name	Specifies the name of the scanner.
Type	Specifies the type of scanner, for example, Nessus Scan Results Importer.
Host	Specifies the IP address or host name of the host on which the scanner operates.
Approved CIDR ranges	Specifies the CIDR range(s) you want this scanner to consider. Multiple CIDR ranges are displayed using a comma separated list.
Description	Specifies a description for this scanner.
Status	Specifies the status of the scanner schedule.

2

MANAGING nCIRCLE ip360 SCANNERS

STRM uses SSH to access the remote server (SSH export server) then retrieves and interprets the scanned data. STRM supports VnE Manager version IP360-6.5.2 to 6.7.1.

You can configure an nCircle ip360 device to export scan results to a remote server. These scan results are exported, in XML format, to an SSH server. STRM periodically polls the SSH server for updates to the scan results and downloads the latest results for processing. To successfully integrate an ip360 device with STRM, these XML files must be read from the remote server (using SSH). The term remote server refers to a system that is separate from the nCircle device. STRM cannot connect directly with nCircle devices. For more information on exporting scan results, see [Exporting Scan Reports](#).

The scan results, in XML format, contains identification information regarding the scan configuration from which it was produced. The most recent scan results are used when a scan is requested from STRM. STRM only supports the XML2 format.

Once you configure your nCircle scanner, you can schedule a scan. However, we recommend that you wait until STRM downloads the exported scan results. This may take up to 15 minutes. The scan schedule configuration allows you to configure potency, however, the ip360 scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring an ip360 scanner including:

- [Adding an ip360 Scanner](#)
- [Editing an ip360 Scanner](#)
- [Deleting an ip360 Scanner](#)
- [Exporting Scan Reports](#)

Adding an ip360 Scanner

To add an ip360 scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 2-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select nCircle IP360 Scanner .

The list of parameters for the selected scanner type appears.

Path:	<input type="text" value="/var/ncircle2/"/>
SSH Server Host Name:	<input type="text" value="172.16.150.230"/>
Private Key Authorization:	<input type="text" value="No"/> ▼
SSH Username:	<input type="text" value="root"/>
Password:	<input type="password" value="*****"/>
Private Key Path:	<input type="text" value="/opt/qradar/conf/vis.ssh.key"/>
Polling Interval:	<input type="text" value="60"/>
File Pattern:	<input type="text" value="XML2_ip360.d_1.a_([0-9]*).xml"/>
Collection Type:	<input type="text" value="Bulk Import"/> ▼

Step 6 Enter values for the parameters:

Table 2-2 ip360 Parameters

Parameter	Description
Path	Specify the location (full directory path) on the remote server where the exported scan results are stored. The default is <code>/var/ncircle/</code> .
SSH Server Host Name	Specify the IP address or host name to the remote server hosting the exported scan data. We recommend using a UNIX-based system running SSH.
Private Key Authorization	Enable (Yes) or disable (No) private key authorization for the server. If set to Yes, the SSH authentication is completed using a private key and the password is ignored. The default value is No.
SSH Username	Specify the SSH remote server username.
Password	Specify the password to the remote server corresponding to the SSH Username. If the Private Key Authentication parameter is set to Yes, the password is ignored.
Private Key Path	Specify the private key path. The private key path is the full directory path on your STRM system where the private key to be used for SSH key-based authentication is stored. The default is <code>/opt/qradar/conf/vis.ssh.key</code> . However, by default, this file does not exist. You must create the <code>vis.ssh.key</code> file or enter another file name. If the Private Key Authorization parameter is set to No, this parameter is ignored.
Polling Interval	Specify the frequency, in seconds, that you want the STRM to poll the remote server for updates to scan results. The default value is 900 seconds.
File Pattern	The Vulnerability Assessment Integration Server (VIS) retrieves scan reports, at the configured polling interval, from the nCircle device. Specify the regular expression that you want to use to filter the list of files on the remote server to ensure that only the ip360 exported XML file is downloaded. It is important to ensure that only ip360 XML files are included in the listing. Typical values for this parameter are: <code>XML2_ip360.d_([0-9]*).a_([0-9]*).xml</code> We recommend that you use the above pattern, however, you can also use the default below pattern: <code>XML2_ip360.d_1.a_([0-9]*).xml</code> Note: We recommend that you only store a month of these files.

Table 2-2 ip360 Parameters (continued)

Parameter	Description
Collection Type	<p>There are two ways to configure a scanner to retrieve nCircle data. You can retrieve data using a Scheduled scan, or you can select Bulk Import. Bulk Import does not require a scheduled scan, since the data is retrieved on a polling interval and the received files are specified by the File Pattern.</p> <p>Using the drop-down list box, select the collection type:</p> <ul style="list-style-type: none"> • Scheduled - Imports data from selected devices on a scheduled interval based on the CIDR range of each device. The imported data is determined by the File Pattern. • Bulk Import - Imports data from all scanner devices in the network based on the specified polling interval. The imported data is determined by the File Pattern. <p>Note: For more information, see Chapter 14 Managing Scan Schedules.</p>



Note: If the scanner is configured to use a password, the SSH scanner server to which STRM connects must support password authentication. If it does not, SSH authentication for the scanner may fail. Make sure the following line appears in your `sshd_config` file, which is typically found in the `/etc/ssh` directory on the SSH server: `PasswordAuthentication yes`. If your scanner server does not use OpenSSH, the configuration may be slightly different.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - Click **Add**.



Note: If you select Bulk Import, data will be collected from all scanner devices in the network, but the interface requires at least one CIDR range. The CIDR range entered is ignored during the Bulk Import process.

Step 8 Click **Save**.

Step 9 From the Admin tab menu, click **Deploy Changes**.



Note: If you selected Scheduled as the Collection Type, you will need to schedule a scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

Editing an ip360 Scanner

To edit a scanner:

- Click the **Admin** tab.
- In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window appears.

Step 6 Update parameters, as necessary. See [Table 2-2](#).

Step 7 Click **Save**.

Step 8 From the Admin tab menu, click **Deploy Changes**.

Deleting an ip360 Scanner

To delete a scanner:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window appears.

Step 6 Click **Ok**.

Step 7 From the Admin tab menu, click **Deploy Changes**.

Exporting Scan Reports

To configure your nCircle device to export scan reports:

Step 1 Log in to the IP360 VNE Manager user interface.

Step 2 From the left menu, select **Administer > System > VNE Manager > Automated Export**.

The Automated Export menu appears.

Step 3 Click the **Export to File** tab.

Step 4 Configure the export settings.

For information on configuring the export settings, click the Help link. To integrate with STRM, the export must be configured to use the XML2 format.

Step 5 Record the Target settings that appear in the interface. These settings are necessary to configure STRM to integrate with your nCircle device.

3

MANAGING NESSUS SCANNERS

Nessus software includes separate client and server components. You can install the client on the same system as the server. However, for performance reasons, you can provide a dedicated Nessus server with distributed clients, which means a separate client and server. The Nessus client may consume significant system resources during large or detailed scans.



Note: *Since Nessus may require high CPU usage, we recommend that you do not install your Nessus software on a network critical system.*

When configuring your Nessus system, make sure your STRM system is granted appropriate access, which means creating a Nessus user account for your STRM system. After you create a user account for STRM, make sure the Nessus server is fully operational before starting a scan.

Once you configure the Nessus system and the Nessus scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the Nessus scanner uses the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

STRM supports Nessus version 4.0.2 on a Linux OS. STRM supports Nessus version 4.2.x on a Linux or Windows OS. For more information on installing and configuring Nessus, see your Nessus documentation.

This chapter provides information on managing your Nessus scanner including:

- [Adding a Nessus Scanner](#)
- [Editing an Nessus Scanner](#)
- [Deleting a Nessus Scanner](#)

Adding a Nessus Scanner

To add a Nessus scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 3-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select Nessus Scanner .

The list of parameters for the selected scanner type appears.

Path:

Server Host Name:

Server Port:

Username:

Password:

Disable Pixmaps:

Remote Hostname:

Login Username:

Enable Key Authentication:

Login Password:

Private Key File:

Remote Temp Dir :

- Step 6** Enter values for the parameters:

Table 3-2 Nessus Parameters

Parameter	Description
Path	Specify the location (full directory path including the filename) of the Nessus client executable file on the Nessus client host. The default is /usr/bin/nessus.
Server Host Name	Specify the IP address or host name of the Nessus server as seen by the Nessus client. If server process and the client are located on the same host, you can use localhost as the server host name. The default is localhost.
Server Port	Specify the port for the nessus server. The default is port 1241.
Username	Specify the Nessus username that the Nessus client uses to authenticate with the Nessus server.
Password	Specify the Nessus password that corresponds to the username. Note: Your Nessus server password must not contain the ! character to prevent authentication failures over SSH.
Disable Pixmaps	Enables (Yes) or Disables (No) pixmaps. The Disable Pixmaps parameter is a Nessus client parameter that overrides the default behavior of the graphical client if you want to use the command-line mode. If the Nessus installation includes a graphical client, set this parameter to Yes. The default is No. To determine if the Nessus client has graphical interface support, you must log in (using SSH or telnet) to the system that is hosting the Nessus client and execute the client with no parameters. The usage Help window appears if no graphical client is installed.
Remote Hostname	Specify the host name or IP address of the system hosting the Nessus client. This must be a UNIX-based system running SSH.
Login Username	Specify the username used by STRM to authenticate the SSH connection.
Enable Key Authentication	Enables (Yes) or disables (No) public/private key authentication. If enabled, STRM attempts to authenticate the SSH connection using the provided private key and the Login Password parameter is ignored. The default is Yes. For more information, see your SSH documentation for configuring public key authentication.
Login Password	If Enable Key Authentication is disabled, you must specify the password corresponding to the Login Username parameter that STRM uses to authenticate the SSH connection. If Enable Key Authentication is enabled, the Login Password parameter is ignored.

Table 3-2 Nessus Parameters (continued)

Parameter	Description
Private Key File	Specify the directory path to the file that contains the private key information. If you are using SSH key-based authentication, STRM uses the private key to authenticate the SSH connection. The default is /opt/qradar/conf/vis.ssh.key. However, by default, this file does not exist. You must create the vis.ssh.key file or enter another file name. This parameter is mandatory if the Enable Key Authentication parameter is set to Yes. If the Enable Key Authentication is set to No, this parameter is ignored.
Remote Temp Dir	Specify the directory on the Nessus client that STRM may use to store temporary files used during the execution of the Nessus client. These files are removed once the client has successfully executed. The default is /tmp.



Note: If the scanner is configured to use a password, the SSH scanner server to which STRM connects must support password authentication. If it does not, SSH authentication for the scanner will fail. Make sure the following line appears in your `sshd_config` file, which is typically found in the `/etc/ssh` directory on the SSH server: `PasswordAuthentication yes`. If your scanner server does not use OpenSSH, the configuration may be slightly different.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, click **Deploy Changes**.

Editing an Nessus Scanner

To edit a scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window appears.

- Step 6** Update parameters, as necessary. See [Table 3-2](#).
- Step 7** Click **Save**.
- Step 8** From the Admin tab menu, click **Deploy Changes**.

Deleting a Nessus Scanner

To delete a scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window appears.
- Step 6** Click **Ok**.
- Step 7** From the Admin tab menu, click **Deploy Changes**.

4

MANAGING NESSUS SCAN RESULT IMPORTERS

When you configure a Nessus Scan Result Importer, STRM connects to the host storing the Nessus scan results file. STRM then retrieves the previously run scan results for processing. STRM supports Nessus version 4.0.2 on a Linux OS. STRM supports Nessus version 4.2.x on a Linux or Windows OS. For more information on installing and configuring Nessus, see your Nessus documentation.

The Nessus Scan Results Importer supports output reports in the Nessus format. The Nessus File Importer receives a scan request one IP address at a time. This request contains the IP address, ports, and potency information, which is necessary for the scan.

Once you configure the Nessus Scan Result Importer device and the Nessus Scan Result Importers scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the Nessus Scan Result Importer scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter provides information on managing your Nessus Scan Result Importers including:

- [Adding a Nessus Scan Result Importer](#)
- [Editing a Nessus Scan Result Importer](#)
- [Deleting a Nessus Scan Result Importer](#)

Adding a Nessus Scan Result Importer

To add a Nessus Scan Result Importer:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.

The Add Scanner window appears.

Step 5 Enter values for the following parameters:

Table 4-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select Nessus Scan Result Importer .

The list of parameters for the selected scanner type appears.

Remote Hostname:	<input type="text"/>
Login Username:	<input type="text"/>
Enable Key Authentication:	<input type="button" value="No"/> ▾
Login Password:	<input type="text"/>
Private Key File:	<input type="text"/>
Remote results file:	<input type="text" value="/tmp/results.xml"/>

Step 6 Enter values for the parameters:

Table 4-2 Nessus Scan Result Importer Parameters

Parameter	Description
Remote Hostname	Specify the host name or IP address of the system hosting the Nessus scan results file.
Login Username	Specify the username used by STRM to authenticate the SSH connection.
Enable Key Authentication	Enables (Yes) or disables (No) public/private key authentication. If enabled, STRM attempts to authenticate the SSH connection using the provided private key and the Login Password parameter below is ignored. The default is Yes. For more information, see your SSH documentation for configuring public key authentication.

Table 4-2 Nessus Scan Result Importer Parameters (continued)

Parameter	Description
Login Password	Specify the password associated with the Login Username for SSH access. If Enable Key Authentication is enabled, this parameter is ignored. Note: Your Nessus server login password must not contain the ! character to prevent authentication failures over SSH.
Private Key File	Specify the directory path to the STRM system hosting the file that contains the private key information. STRM uses the private key to authenticate the SSH connection, if you are using SSH key based authentication. The default is /opt/qradar/conf/vis.ssh.key. However, by default, this file does not exist. You must create the vis.ssh.key file or enter another file name. This parameter is mandatory if the Enable Key Authentication parameter is set to Yes. If the Enable Key Authentication is set to No, this parameter is ignored.
Remote Results File	Specify the directory and filename on the Nessus server from which STRM retrieves the scan results.



Note: If the scanner is configured to use a password, the SSH scanner server to which STRM connects must support password authentication. If it does not, SSH authentication for the scanner will fail. Make sure the following line appears exactly as shown in your `sshd_config` file, which is typically found in the `/etc/ssh` directory on the SSH server. `PasswordAuthentication yes`. If your scanner server does not use OpenSSH, the configuration may be slightly different.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, click **Deploy Changes**.

Editing a Nessus Scan Result Importer

To edit a Nessus Scan Result Importer:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window appears.

Step 6 Update parameters, as necessary. See [Table 4-2](#).

Step 7 Click **Save**.

Step 8 From the Admin tab menu, click **Deploy Changes**.

Deleting a Nessus Scan Result Importer

To delete a Nessus Scan Result Importer:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

The confirmation window appears.

Step 6 Click **Ok**.

Step 7 From the Admin tab menu, click **Deploy Changes**.

5

MANAGING NMAP SCANNERS

You can integrate Network Mapper (Nmap) scanners (versions 3.7 to 4.68) with STRM. Since certain types of Nmap port scans require Nmap to be run as root, STRM must have access as root or you must operate the Nmap binary with setuid root. For assistance, contact your system administrator.

STRM uses SSH to communicate with a remote server (the scanner server) and executes the Nmap binary on that server.

Once you configure the Nmap system and the Nmap scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, which determines the aggressiveness of the scan. The Nmap scanner uses the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on managing your Nmap scanner including:

- [Adding a Nmap Scanner](#)
- [Editing an Nmap Scanner](#)
- [Deleting an Nmap Scanner](#)

Adding a Nmap Scanner

To add a Nmap scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 5-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select NMap Scanner .

The list of parameters for the selected scanner type appears.

The screenshot shows a configuration form with the following fields and values:

- Path:** /usr/bin/nmap
- Disable Ping:** No
- Remote Hostname:** (empty)
- Login Username:** (empty)
- Enable Key Authentication:** Yes
- Login Password:** (empty)
- Private Key File:** /opt/qradar/conf/vis.ssh.key

Step 6 Enter values for the parameters:

Table 5-2 Nmap Parameters

Parameter	Description
Path	Specify the full directory path and filename of the executable file for the Nmap application. The default is /usr/bin/nmap.
Disable Ping	In some networks, the ICMP protocol is partially or completely disabled. In situations where ICMP is not enabled, you may want to enable ICMP pings to enhance the accuracy of the scan. Using the drop-down list box, enable (Yes) or disable (No) ICMP pings. The default is No.
Remote Hostname	Specify the hostname or IP address of the remote system hosting the Nmap client. We recommend using a UNIX-based system running SSH.
Login Username	Specify the username to be used with SSH required to access the remote system hosting the Nmap client.
Enable Key Authentication	Enables (Yes) or disables (No) public/private key authentication. If enabled, STRM attempts to authenticate the SSH connection using the provided private key and the Login Password parameter is ignored. The default is Yes. For more information, see your SSH documentation for configuring public key authentication.

Table 5-2 Nmap Parameters (continued)

Parameter	Description
Login Password	<p>If Enable Key Authentication is disabled, you must specify the password corresponding to the Login Username parameter that STRM uses to authenticate the SSH connection.</p> <p>If Enable Key Authentication is enabled, the Login Password parameter is ignored.</p>
Private Key File	<p>Specify the directory path to the file that contains the private key information. If you are using SSH key based authentication, STRM uses the private key to authenticate the SSH connection. The default is /opt/qradar/conf/vis.ssh.key. However, by default, this file does not exist. You must create the vis.ssh.key file or enter another file name.</p> <p>This parameter is mandatory if the Enable Key Authentication parameter is set to Yes. If the Enable Key Authentication is set to No, this parameter is ignored.</p>



Note: If the scanner is configured to use a password, the SSH scanner server to which STRM connects must support password authentication. If it does not, SSH authentication for the scanner will fail. Make sure the following line appears in your `sshd_config` file, which is typically found in the `/etc/ssh` directory on the SSH server: `PasswordAuthentication yes`. If your scanner server does not use OpenSSH, the configuration may be slightly different.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click Browse to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, click **Deploy Changes**.

Editing an Nmap Scanner

To edit an Nmap scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window appears.
- Step 6** Update parameters, as necessary. See [Table 5-2](#).

Step 7 Click **Save**.

Step 8 From the Admin tab menu, click **Deploy Changes**.

Deleting an Nmap Scanner

To delete an Nmap scanner:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window appears.

Step 6 Click **Ok**.

Step 7 From the Admin tab menu, click **Deploy Changes**.

6

MANAGING QUALYS SCANNERS

A QualysGuard vulnerability scanner runs on a remote web server. STRM must access the remote web server through an HTTPS connection to run and retrieve scan results. STRM supports Qualys version 4.7 to 6.0.44-1. For more information, see your Qualys documentation.

Once you configure the Qualys device and the Qualys scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the Qualys scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring a Qualys scanner including:

- [Adding a Qualys Scanner](#)
- [Editing a Qualys Scanner](#)
- [Deleting a Qualys Scanner](#)

Adding a Qualys Scanner

To add a Qualys scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 6-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.

Table 6-1 Scanner Parameters (continued)

Parameter	Description
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select Qualys Scanner .

The list of parameters for the selected scanner type appears.

Qualys Server Host Name:
Qualys Username:
Qualys Password:
Scanner Name:
Results File:
Configured Options:
Cache Directory:
Cache Retention Period:
Bulk Import Interval (minutes):
Max Report Age (days):
Import File:
Collection Type:
Read Only:
Use Proxy:
Proxy Host Name:
Proxy Port:
Proxy Username:
Proxy Password:

Step 6 Enter values for the parameters:

Table 6-2 Qualys Parameters

Parameter	Description
Qualys Server Host Name	Specify the Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. When specifying the FQDN, you must specify the hostname and not the URL. For most deployments, enter qualysguard.qualys.com. However, if you are using the full scanning infrastructure including an internal management console, enter the hostname of the internal management console.

Table 6-2 Qualys Parameters (continued)

Parameter	Description
Qualys Username	Specify the username necessary for requesting scans. This is the login to the Qualys server.
Qualys Password	Specify the password that corresponds to the Qualys Username and is the login to the Qualys server.
Scanner Name	Specify the name of the scanner that you want to perform the scanning, as the name appears in the QualysGuard management interface. To obtain the scanner name, contact your network administrator. If you are using a public scanning appliance, you must leave the Scanner Name field blank.
Results File	Specify the temporary file name where you want to store the Qualys scan results. The default is qualys.results. We recommend that you use the default value.
Configured Options	Specify if you want the Qualys scanner to retrieve existing scans. When a scan is initiated, the Qualys scanner retrieves a list of scanners for the configured user from the Qualys server. The scanner then verifies if the CIDR and the configured options match the scan. If a match is found, the existing scan is used. If no matching scan is found, a new scan is initiated. The default is Initial Options. For more information, see your Qualys documentation. You can enter multiple configured options using a comma delimited list. For additional information regarding the configuration for an option profile, see the following web site: https://qualysguard.qualys.com/fo/tools/optionProfiles.php This web site requires login credentials. Contact your Qualys representative for access information.
Cache Directory	Specify the local directory where you want to store the scans. The default is /store/vis/qualys/
Cache Retention Period	Specify the period of time, in milliseconds, that you want to store scans before they are deleted. The default is 172,800,000 milliseconds (2 days).
Bulk Import Interval (minutes)	Specify the frequency, in minutes, that you want the importer to process a report.
Max Report Age (days)	Specify the maximum age of a report to include when performing a bulk import. Files that are older than specified time will be excluded from the bulk import.

Table 6-2 Qualys Parameters (continued)

Parameter	Description
Import File	<p>This parameter only applies if you select the Import - Technical Report option from the Collection Type drop-down list box.</p> <p>Specify the local path to store the report. If you select Import - Technical Report as the Collection Type and specify an import file, the Qualys scanner imports the entire contents to the file. If this field is blank, the Qualys scanner attempts to retrieve the latest technical report using the Qualys API.</p>
Collection Type	<p>Using the drop-down list box, select one of the following options:</p> <ul style="list-style-type: none"> • Scheduled - Specify if you want the scheduled scan to include the report data. • Import - Scan Report - Specify if you want the scan report list retrieved from Qualys and compile all the report results into one report. This option does not use the local file, as defined in the Import File parameter. • Import - Technical Report - Specify if you want to import all data from the file specified in the Import File parameter. If the Import File parameter is blank, the scanner retrieves the latest technical report from the Qualys web site and imports all the data. <p>For more information, see your Qualys documentation.</p>
Read Only	<p>Using the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • Yes - Specify if you want to limit the scanner to retrieving existing scans only. No new scans will be initiated. • No - Specify if you want to initiate a new scan if no existing scan is found for the IP address or CIDR.
Use Proxy	<p>Using the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • Yes - Specify if your scanner requires a proxy for communication or authentication. • No - Specify if your scanner does not require a proxy.
Proxy Host Name	Specify the host name or IP address of your proxy server if your scanner requires a proxy.
Proxy Port	Specify the port number of your proxy server if your scanner requires a proxy.
Proxy Username	Specify the username of your proxy server if your scanner requires a proxy.
Proxy Password	Specify the password of your proxy server if your scanner requires a proxy.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - Click **Add**.

Step 8 Click **Save**.

Step 9 From the Admin tab menu, click **Deploy Changes**.

Editing a Qualys Scanner

To edit a Qualys scanner:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window appears.

Step 6 Update parameters, as necessary. See [Table 6-2](#).

Step 7 Click **Save**.

Step 8 From the Admin tab menu, click **Deploy Changes**.

Deleting a Qualys Scanner

To delete an Qualys scanner:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window appears.

Step 6 Click **Ok**.

Step 7 From the Admin tab menu, click **Deploy Changes**.

7

MANAGING FOUNDSCAN SCANNERS

Once you install the STRM Foundstone FoundScan scanner, the scanner queries the FoundScan Engine using the FoundScan OpenAPI. The FoundScan scanner does not directly execute scans but gathers current scan results as displayed in the scanning application. STRM supports Foundstone FoundScan versions 5.0 to 6.5.

Your FoundScan system must include a configuration appropriate for STRM to use and a scan that runs regularly to keep the results current. To ensure that your FoundScan scanner is able to retrieve scan information, make sure your FoundScan system meets the following requirements:

- Since the API provides access to the FoundScan application, make sure the FoundScan application runs continuously on the FoundScan server. This means that the FoundScan application must be active on your desktop.
- The scan that includes the necessary configuration to connect with STRM must be complete and visible in the FoundScan interface for STRM to retrieve the scan results. If the scan does not appear in the FoundScan interface or is scheduled to be removed after completion, STRM needs to retrieve the results before the scan is removed or the scan will fail.
- The appropriate user privileges must be configured in the FoundScan application, which will allow STRM to communicate with FoundScan.

Since the FoundScan OpenAPI only provides host and vulnerability information to STRM, your STRM Asset Profile information will display all vulnerabilities for a host assigned to a port 0.

When using SSL (default) to connect to FoundScan, the FoundScan Engine requires STRM to authenticate using client-side certificates. By default, FoundScan includes default certificate authority and client certificates that are the same for all installations. The STRM FoundScan plugin also includes these same certificates for use with FoundScan 5.0. If the FoundScan Server uses custom certificates, or is using a version of FoundScan other than 5.0, you must import the appropriate certificates and keys on the STRM host(s). For more information, see [Importing Certificates](#).

Once you configure the FoundScan system and the FoundScan scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the FoundScan scanner does not consider the

potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring a FoundScan scanner including:

- [Adding a FoundScan Scanner](#)
- [Editing a FoundScan Scanner](#)
- [Deleting a FoundScan Scanner](#)
- [Using Certificates](#)

Adding a FoundScan Scanner

To add a FoundScan scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 7-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select FoundScan Scanner .

The list of parameters for the selected scanner type appears.

SOAP API URL:	<input type="text" value="https://localhost:3800"/>
Customer Name:	<input type="text"/>
User Name:	<input type="text"/>
Client IP Address:	<input type="text"/>
Password:	<input type="password"/>
Portal Name:	<input type="text"/>
Configuration Name :	<input type="text"/>
CA Truststore :	<input type="text" value="/opt/qradar/conf/foundscan.trustst"/>
Client Keystore :	<input type="text" value="/opt/qradar/conf/foundscan.keystc"/>

Step 6 Enter values for the parameters:

Table 7-2 FoundScan Parameters

Parameter	Description
SOAP API URL	Specify the web address for the Foundscan OpenAPI in the following format: <code>https://<foundstone IP address>:<SOAP port></code> Where: <foundstone IP address> is the IP address or hostname of the FoundScan scanner server. <SOAP port> is the port number for the FoundScan Engine. The default is <code>https://localhost:3800</code> .
Customer Name	Specify the name of the customer under which the Login User Name belongs.
User Name	Specify the user name you want STRM to use for authenticating the FoundScan Engine in the API. This user must have access to the scan configuration.
Client IP Address	Specify the IP address of the STRM server that you want to perform the scans. By default, this value is not used, however, is necessary for validating some environments.
Password	Specify the password corresponding to the Login User Name for access to the API.
Portal Name	Optional. Specify the portal name. This field may be left blank for STRM purposes. See your FoundScan administrator for more information.
Configuration Name	Specify the scan configuration name that exists in FoundScan and to which the user has access. Make sure this scan is active or at least runs frequently.
CA Truststore	Specifies the directory path and filename for the CA truststore file. The default is <code>/opt/qradar/conf/foundscan.keystore</code> .
Client Keystore	Specifies the directory path and filename for the client keystore. The default is <code>/opt/qradar/conf/foundscan.truststore</code> .

- Step 7** To configure the CIDR ranges you want this scanner to consider:
 - a In the text field, enter the CIDR range you want this scanner to consider or click Browse to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, select **Deploy Changes**.

Editing a FoundScan Scanner

To edit an FoundScan scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window appears.
- Step 6** Update parameters, as necessary. See [Table 7-2](#).
- Step 7** Click **Save**.
- Step 8** From the Admin tab menu, select **Deploy Changes**.

Deleting a FoundScan Scanner

To delete a FoundScan scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window appears.
- Step 6** Click **Ok**.
- Step 7** From the Admin tab menu, select **Deploy Changes**.

Using Certificates The FoundScan Engine uses a certificate to encrypt traffic and for authentication. During the initial installation of FoundScan, you can configure FoundScan to use the default certificate or you can use a custom certificate.

This section provides information on obtaining and importing the necessary certificates including:

- [Obtaining a Certificate](#)
- [Importing Certificates](#)

Obtaining a Certificate To obtain the necessary certificate:

Step 1 Run the FoundScan application.

Step 2 From the File menu, select **Preferences**.

Step 3 In the Preferences window, click the **Communication** tab.

Step 4 Locate the Authentication Scheme field.

If the field indicates FoundStone default-certificate, then the default certificate is in use.

Step 5 If you are using the default certificate, locate and obtain the **TrustedCA.pem** and **Portal.pem** files from the FoundScan configuration folder on your system.

For examples of the TrustedCA.pem and Portal.pem files, see [Example Of TrustedCA.pem File](#) and [Example of Portal.pem File](#).

Step 6 If you are using a custom certificate, generate a certificate using the FoundScan Certificate manager. Make sure you specify the IP address of the STRM host as the hostname for the certificate.

You are now ready to import the certificate on each STRM managed host that will host the VIS component. See [Importing Certificates](#).

Importing Certificates If the FoundScan Server uses custom certificates, or is using a version of FoundScan other than 5.0, you must import the appropriate certificates and keys on each STRM host(s) that will host the VIS component. Before you perform the below procedure, make sure the FoundScan scanner is installed.

To import the certificates:

Step 1 Obtain two certificate files and the pass phrase from your FoundScan administrator.

The first file is the CA certificate for the FoundScan engine. The second certificate is the private key plus certificate chain for the client.

Both of these files must be in PEM format. For examples of these files, see [Example Of TrustedCA.pem File](#) and [Example of Portal.pem File](#).

Step 2 Copy the two PEM files to your STRM system, either to the root user's home directory or to a new directory created for the certificates.

Step 3 On the STRM host, change the directory to where the two PEM files are copied.

Step 4 Remove the existing certificates:

```
rm -f /opt/qradar/conf/foundscan.keystore
rm -f /opt/qradar/conf/foundscan.truststore
```

Step 5 Enter the following command:

```
/opt/qradar/bin/foundstone-cert-import.sh <TrustedCA.pem>
<Portal.pem>
```

Where:

<TrustedCA.pem> is the CA certificate filename.

<Portal.pem> is the private keychain PEM file.

The output may resemble the following:

```
Certificate was added to keystore
Using keystore-file : /opt/qradar/conf/foundscan.keystore
One certificate, no chain.
Key and certificate stored.
Alias:Portal.pem Password:foundscan
Contents of Trust Store:
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: trustedca.pem
Creation date: Mar 8, 2007
Entry type: trustedCertEntry
Owner: CN=Foundstone CA
Issuer: CN=Foundstone CA
Serial number: 0
Valid from: Fri Sep 12 20:29:11 ADT 2003 until: Mon Oct 20
20:29:11 ADT 2008 Certificate fingerprints:
    MD5: 14:7E:68:02:38:EC:A5:A8:AE:3D:3C:C6:F5:F6:33:6C
    SHA1:
37:C3:48:36:87:B0:F2:41:48:6A:A2:F6:43:B7:76:55:92:C5:6E:11
*****
*****

Content of Key Store:
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: portal.pem
Creation date: Mar 8, 2007
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Foundstone Enterprise Manager
Issuer: CN=Foundstone CA
```

```

Serial number: 2
Valid from: Fri Sep 12 20:36:54 ADT 2003 until: Mon Oct 20
20:36:54 ADT 2008 Certificate fingerprints:
    MD5: 0A:CD:06:36:B2:ED:62:8C:98:8D:10:3C:99:95:BA:7D
    SHA1:
3A:B4:9C:59:D0:AD:26:C9:6D:B9:05:E9:F1:33:CB:23:F2:0A:E7:26
*****
*****

```

Step 6 Repeat for all managed hosts in your deployment, which will host the VIS.

Example Of TrustedCA.pem File

```

-----BEGIN CERTIFICATE-----
MIICFzCCAYCgAwIBAgIBADANBgkqhkiG9w0BAQQFADAYMRYwFAyDVQQDEw1Gb3Vu
ZHN0b251IENBMB4XDTAzMDkxMjIzMDkxMVoXDTA4MTAyMDIzMDkxMVowGDEWMBQG
J9PUXhzRqqh8yzz795R9D1oj7hsyZtq4My6gKu8RuHVBscYvJVWPMUkPmDHMnpj1
A1UEAxMNRm91bmRzdG9uZSBDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA
sWN8ZqqREM77qByvuIqr2q4XaP5Tfp3hRC08mjvqWsQjk2B8WMRAGzjHqvPN/qfG
5uZw5gm1M6IyoVbLkaQwDF34McRpqlTLVjeDadjPuRaZGVu4zVknC8s83EPqKU9+
fdqmhtCwwqVYq+sQFp1S3kKUvXIBEGV0r9mnFAD3InUCAwEAAANxMG8wHQYDVR0O
BBYEFQ8UJTPbqSP202Mygs2sqzU2h7LMEAGA1UdIwQ5MDeAFGQ8UJTPbqSP202M
ygs2sqzU2h7LoRykGjAYMRYwFAyDVQQDEw1Gb3VuZHN0b251IENBggEAMAWGA1Ud
j0ynMtEM2mtuf95uxeGFe581k31w9d3IGt19uahtyqG860kr4/ys3r7Lja0f9rjff
J9PUXhzRqqh8yzz795R9D1oj7hsyZtq4My6gKu8RuHVBscYvJVWPMUkPmDHMnpj1
4p7dh7GKk7ymFYs=
-----END CERTIFICATE-----

```

Example of Portal.pem File

```

-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQC5D0nQtMtDXAht/4M/li9gVlyoch9EYvCiAsZmtO2JMTjEDse
mH0DQkxSKv0gvsCqKXhx6nNegyyiCM1GuEDvFYPCI5FrkrzEwtndTILGXT5asDXu
ncnA1/9am4jAhADDPfb9ZRMoE6aFE13XD21o49gJG4sH+VkcQQDrf6OGfnR6YaYz
SbPTMrBKR5pfMJOPJ/Sjc0vf6A48Nn8FiYLDiyBLKhunzM03EZ22VrZxBwIDAQAB
AoGARZfkqzgdJZ8JnpJBahOPTFBEGodbbhiW+IPfW7Nc8fcjQPvDQuw3wHfSmDVTb
g6AZhyU1FBzvLIE6nOmggdMzn9KIN8WMD+XDAAR4AaWOGkn18Ib4h1VVnsa90hYS
BPIWVsfbAkeAysj6iwtolLVsXC5cIP4YzNzNs j2QBqeEhEfUmLtZl8vD1s j+EM2L
JggOcRPyMxIj64ob/hevavXew1CFermpRQJBAKaq6OKQsILEhUoGHLJTT2BtOpEs
3JP4BBUV7QE0VTTKxA8byQqjGSu6zh/JxWk9hTjo5oSmlcwahC5k104Cy0CQQct
vnwv7mncFtsB/3TJdk67Wxc7FRs59CRsEJKaXG80weVjtXRj1PSTo6+9ltCJQ+jM
fxxQaeq0SqqEWLb+UuClAkeAR6Z503v5p1rVUWTo+L8JaygumdzZRuBzi/EVuxqG
j79b6Xa+UvXtXquU2qlolweantry/Glm47qSwPbcFoOse4Q==
-----END RSA PRIVATE KEY-----
Certificate:

```

Data:

Version: 3 (0x2) Serial Number: 2 (0x2)
Signature Algorithm: md5WithRSAEncryption
Issuer: CN=Foundstone CA

Validity

Not Before: Sep 12 23:36:54 2003 GMT
Not After : Oct 20 23:36:54 2008 GMT

Subject: CN=Foundstone Enterprise Manager

Subject Public Key Info:

Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:b9:0c:e9:d0:b4:cb:43:5c:01:ed:87:fe:0c:fe:
52:3d:81:59:72:a1:c8:7d:11:8b:c2:88:0b:19:9a:
d3:b6:24:c4:e3:10:3b:1e:98:7d:03:42:4c:52:2a:
fd:20:be:c0:aa:29:71:f1:ea:73:5e:83:2c:a2:08:
cd:46:b8:40:ef:15:83:c2:23:91:6b:92:bc:c4:c2:
d9:dd:4c:82:c6:5d:3e:5a:b0:35:ee:49:b3:d3:32:
b0:4a:47:9a:5f:30:9a:0f:27:f4:a3:73:4b:df:e8:
0e:3c:36:7f:05:89:82:c3:8b:20:4b:2a:1b:a7:cc:
cd:37:11:9d:b6:56:b6:71:07

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

0D:52:54:EF:A0:B3:91:9D:3D:47:AC:D8:9E:62:2A:34:0F:09:FF:8D

X509v3 Authority Key Identifier:

keyid:64:3C:50:94:CF:6E:A4:8F:DB:4D:8C:CA:0B:36:B2:AC:D4:DA:
1E:CB

DirName:/CN=Foundstone CA

serial:00

Signature Algorithm: md5WithRSAEncryption

4a:88:3f:51:34:5b:30:3b:5b:7c:57:31:86:22:3b:00:16:61:
ac:7b:b7:ae:cd:68:11:01:a2:52:b7:59:1e:c6:5b:af:2a:ed:

```
f9:ee:ef:64:11:b2:b9:14:21:7d:2c:35:d3:cb:09:08:a1:ab:
26:93:0f:aa:97:eb:cc:65:ab:95:a3:0d:77:0b:23:20:4a:0d:
04:18:47:2d:58:a7:de:61:9f:aa:3c:da:a5:00:9d:b5:eb:52:
fb:e2:5b:56:45:02:02:79:df:0f:87:bc:f3:82:d1:3d:39:79:
9e:ef:64:e2:f5:61:9b:ea:29:94:fb:00:8f:b8:08:7c:f0:ee:
68:b6
```

```
-----BEGIN CERTIFICATE-----
```

```
MIICVDCCAb2gAwIBAgIBAjANBgkqhkiG9w0BAQQFADAYMRYwFAYDVoQDEw1G3Vu
ZHN0b251IENBMB4XDTAzMDkxMjIzMzY1NFoXDTA4MTAyMDIzMzY1NFowKDEmMCQG
A1UEAxMdrM91bmRzdG9uZSBFbnRlcnByaXNlIE1hbmFnZXIwZGZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBALkM6dC0y0NcAe2H/gz+Uj2BWXXhyH0Ri8KICxma07Yk
xOMQOx6YfQNCTFIq/SC+wKopcfHqc16DLKIIzUa4Q08Vg8IjkWuSvMTC2d1MgsZd
PlqwNe5Js9MysEpHml8wmg8n9KNzS9/odjw2fwWJgsOLIEsqG6fMzTcRnbZWtnEH
AgMBAAGjgZ0wgZowCQYDVR0TBAlwADAsBg1ghkgBhvhCAQ0EHydT3BlblNTTCBH
ZW51cmF0ZWQgQ2VydG1maWNhdGUwHQYDVR0OBBYEFA1SVO+gs5GdPUes2J5iKjQP
Cf+NMEAGA1UdIwQ5MDeAFGQ8UJTPbqSP202Mygs2sqzU2h7LoRykgJAYMRYwFAYD
VQDEw1G3VuZHN0b251IENBggEAMA0GCSqGSIb3DQEBAUAA4GBAEqIP1E0WzA7
W3xXMYyiOwAWYax7t67NaBEBolK3WR7GW68q7fnu72QRsrkUIX0sNdPLCQihqyaT
D6qX68xlq5WjDXcLIyBKDQQYRy1Yp95hn6o82qUANbXrUvviW1ZFAgJ53w+HvPOC
0T05eZ7vZOL1YZvqKZT7AI+4CHzw7mi2
```

```
-----END CERTIFICATE-----
```


8

MANAGING JUNIPER NETWORKS NSM PROFILER SCANNERS

The Juniper Networks NetScreen Security Manager (NSM) console passively collects valuable asset information from your network through deployed Juniper intrusion detection and prevention (IDP) sensors. STRM connects to the Profiler database stored on the NSM server to retrieve these records. The STRM server must have access to the Profiler database. STRM supports NSM versions 2007.1r2 to 2007.2r2. For more information, see your vendor documentation.

STRM collects data from the PostgreSQL database on the NSM using Java Database Connectivity (JDBC). To collect data, STRM must have access to the Postgres database port (TCP port 5432). This access is provided in the `pg_hba.conf` file, which is typically located in `/var/netscreen/DevSvr/pgsql/data/pg_hba.conf` on the NSM host.

Once you configure the Juniper Networks NSM Profiler device and the Juniper Networks NSM Profiler scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency; however, the Juniper NSM Profiler scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring a Juniper scanner including:

- [Configuring a Juniper NSM Profile Scanner](#)
- [Adding a Juniper NSM Profiler Scanner](#)
- [Editing a Profiler Scanner](#)
- [Deleting a Profiler Scanner](#)

Configuring a Juniper NSM Profile Scanner

To configure a Juniper NSM Profiler scanner:

- Step 1** Log in to your Juniper Networks NSM device.
- Step 2** Enable UAC Correlation.

To enable the ability to associate a username and a role to profiler log data, a simple edit in the following file is required.

Change the default configuration `listen_address = '127.0.0.1'` to `listen_address = '*'` so that PostgreSQL will listen on all interfaces for incoming connections.

Edit the following file: `/usr/netscreen/DevSvr/var/pgsql/data/postgresql.conf`.

Note: *Placing an IP address between the single quotes is also a valid option, but for simplicity sake, we recommend using `*`.*

Step 3 Edit `pg_hba.conf`.

In addition to having PostgreSQL listen on addresses other than the local host address, an entry must be made in the `pg_hba.conf` file to authenticate incoming connection requests.

Open the following file:

`/var/netscreen/DevSvr/pgsql/data/pg_hba.conf` file

Add the following line to the end of the file:

`host all all <IP address>/32 trust`

Where `<IP address>` is the IP address of the Event Collector you want to connect to the database.

Step 4 Create a Custom View in the profilerDb.

STRM Series appliances require the data to be extracted in a particular format, so a custom view needs to be created in the profilerDb for this purpose. You must log into the profilerDb using the `psql` tool and create the view with the following command:

`psql profilerDb nsm`

This command assumes that you have chosen “nsm” as the username for your profilerDb during installation. Substitute the username for whatever you used if it is different, but “nsm” is the default option presented during installation.

You will now be logged into the `psql` command-line tool for the profilerDb.

Step 5 Copy and paste the following command into the database command-line interface (CLI) to create the STRM Series view:

```
create view strm_avt_view as SELECT a.name, a.category,
v.srcip,v.dstip,v.dstport, v."last", u.name as userinfo,
v.id, v.device, v.vlan,v.sessionid, v.bytecnt,v.pktcnt,
v."first" FROM avt_part v JOIN app a ON v.app =a.id JOIN
userinfo u ON v.userinfo = u.id;
```

This will create a view named `VA_scanner_view` and will join information from other AVT tables into this view.

Step 6 Reload the Postgres service. Enter the following command:

```
su - nsm -c "pg_ctl reload -D
/var/netscreen/DevSvr/pgsql/data"
```

You are now ready to configure the log source within the STRM interface.

Adding a Juniper NSM Profiler Scanner

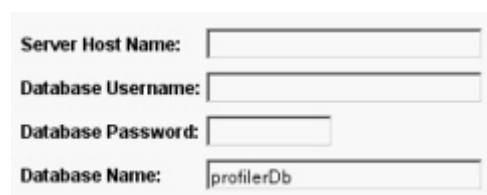
To add a Juniper NSM Profiler scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 8-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select Juniper NSM Profiler Scanner .

The list of parameters for the selected scanner type appears.



Server Host Name:

Database Username:

Database Password:

Database Name:

- Step 6** Enter values for the parameters:

Table 8-2 Juniper NSM Profiler Parameters

Parameter	Description
Server Host Name	Specify the hostname or IP address of the NetScreen Security Manager (NSM) server.
Database Username	Specify the Postgres username to log in to the Profiler database stored on the NSM server.
Database Password	Specify the password associated with the Database Username to log in to the server.

Table 8-2 Juniper NSM Profiler Parameters (continued)

Parameter	Description
Database Name	Specify the name of the Profiler database. The default is profilerDB.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, click **Deploy Changes**.

Editing a Profiler Scanner

To edit a Juniper NSM Profiler scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window appears.
- Step 6** Update parameters, as necessary. See [Table 8-2](#).
- Step 7** Click **Save**.
- Step 8** From the Admin tab menu, click **Deploy Changes**.

Deleting a Profiler Scanner

To delete a Juniper NSM Profiler scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window appears.

Step 6 Click **Ok**.

Step 7 From the Admin tab menu, click **Deploy Changes**.

9

MANAGING RAPID7 NeXPOSE SCANNERS

The Rapid7 NeXpose scanner uses a Perl-based API to obtain scan results for a site. STRM supports Rapid7 NeXpose version 4.5 and above.

Once you configure the Rapid7 NeXpose device and the Rapid7 NeXpose scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the Rapid7 NeXpose scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring a Rapid7 NeXpose scanner including:

- [Adding a Rapid7 NeXpose Scanner](#)
- [Editing a Rapid7 NeXpose Scanner](#)
- [Deleting a Rapid7 NeXpose Scanner](#)

For more information, see your Rapid7 NeXpose documentation.

Adding a Rapid7 NeXpose Scanner

To add a Rapid7 NeXpose scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 9-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select Rapid7 Nexpose Scanner .

The list of parameters for the selected scanner type appears.

A screenshot of a configuration form with four input fields. The fields are labeled as follows: 'Remote Hostname:', 'Login Username:', 'Login Password:', and 'Nexpose Site Id:'. Each label is followed by a text input box. The 'Login Password' field is shorter than the others.

Step 6 Enter values for the parameters:

Table 9-2 Rapid7 NeXpose Parameters

Parameter	Description
Remote Hostname	Specify the hostname or IP address of the Rapid7 NeXpose server.
Login Username	Specify the username to log in to the Rapid7 NeXpose server. The login must be obtained from the Rapid7 NeXpose server interface. For more information, see your Rapid7 NeXpose server administrator.
Login Password	Specify the password to log in to the Rapid7 NeXpose server.
Nexpose Site Id	Specify the site ID you want the scan to use. The site ID must be obtained from the Rapid7 NeXpose server interface. To obtain the site ID: <ol style="list-style-type: none"> 1 Log in to the Rapid7 NeXpose user interface. 2 Click the Assets tab. 3 From the list, select the option that allows you to view assets by the sites to which they belong. The list of sites appears. 4 Click the link for the asset you want STRM to use. 5 The URL in your browser address bar displays the numeric ID of the site. This is the ID value that you must enter in the Rapid7 NeXpose scanner Nexpose Site Id parameter. For more information, see your Rapid7 NeXpose server administrator.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, click **Deploy Changes**.

Editing a Rapid7 NeXpose Scanner

To edit a Rapid7 NeXpose scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window appears.
- Step 6** Update parameters, as necessary. See [Table 9-2](#).
- Step 7** Click **Save**.
- Step 8** From the Admin tab menu, click **Deploy Changes**.

Deleting a Rapid7 NeXpose Scanner

To delete a Rapid7 NeXpose scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window appears.
- Step 6** Click **Ok**.
- Step 7** From the Admin tab menu, click **Deploy Changes**.

10

MANAGING netVigilance SecureScout SCANNERS

Both the SecureScout NX and SecureScout SP devices store all scan results to an SQL database (Microsoft MSDE or SQL Server). STRM connects to the database, locates the latest scanning results for a given IP address, and returns the discovered services and vulnerabilities to STRM's asset profile. STRM supports SecureScout scanner version 2.6.

To connect STRM to the SecureScout database and query for results, you must have appropriate administrative access to STRM and your SecureScout device. For more information, see your SecureScout documentation. Ensure that all firewalls, including the firewall on the SecureScout host, will allow a connection with the Event Collector. STRM connects to an SQL server using a TCP connection on port 1433.

We recommend that you create a user in your SecureScout configuration specifically for STRM. The STRM database user must have select permissions to the following tables:

- HOST
- JOB
- JOB_HOST
- SERVICE
- TCRESULT
- TESTCASE
- PROPERTY
- PROP_VALUE
- WKS

Also, a STRM user must have execute permissions on the stored procedure IPSORT.

Once you configure the SecureScout device and the SecureScout scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the SecureScout scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring SecureScout scanner including:

- [Adding a SecureScout Scanner](#)
- [Editing a SecureScout Scanner](#)
- [Deleting a SecureScout Scanner](#)

Adding a SecureScout Scanner

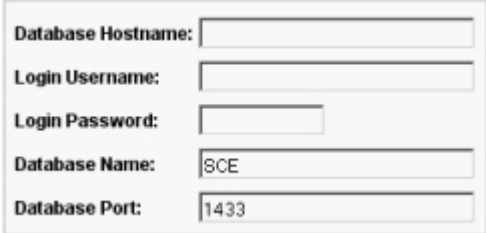
To add a SecureScout scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 10-1 SecureScout Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select SecureScout Scanner .

The list of parameters for the selected scanner type appears.



The screenshot shows a form with the following fields and values:

- Database Hostname:
- Login Username:
- Login Password:
- Database Name: SCE
- Database Port: 1433

- Step 6** Enter values for the parameters:

Table 10-2 SecureScout Parameters

Parameter	Description
Database Hostname	Specify the IP address or hostname of the SecureScout database server that runs the SQL server.
Login Username	Specify the SQL database username that you want STRM to use to log in to the SecureScout database.
Login Password	Specify the corresponding password for the Login Username.
Database Name	Specify the name of the database within the SQL server that contains the SecureScout data. The default is SCE.
Database Port	Specify the TCP port you want the SQL server to monitor for connections. The default is 1433.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, click **Deploy Changes**.

Editing a SecureScout Scanner

To edit a scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window appears.
- Step 6** Update parameters, as necessary. See [Table 10-2](#).
- Step 7** Click **Save**.
- Step 8** From the Admin tab menu, click **Deploy Changes**.

Deleting a SecureScout Scanner

To delete a scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window appears.
- Step 6** Click **Ok**.
- Step 7** From the Admin tab menu, click **Deploy Changes**.

11

MANAGING eEye REM SCANNERS

The eEye REM Security Management Console and the Network Security Scanner uses SNMP versions 1, 2, or 3 to send SNMP traps to STRM. Before you configure your eEye scanner in STRM, you must configure your eEye device to send SNMP traps to STRM. STRM supports eEye version 3.5.6.

Once your eEye REM scanner and STRM have been configured, STRM constantly monitors the listening port to obtain scanner information. Once a scan is completed, the results are sent to STRM and the scanner records all the information. To ensure the host and port profile information is persisted, you must configure a scheduled scan for the eEye REM scanner. This scan determines which of the port and host profiles are persisted to the profile database.

To connect STRM to the eEye REM scanner, you must have appropriate administrative access to STRM and your eEye device. For more information, see your product documentation. Ensure that all firewalls will allow a connection with your STRM system.

Once you configure the eEye REM device and the eEye REM scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the eEye REM scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring eEye scanner including:

- [Adding an eEye REM Scanner](#)
- [Editing an eEye REM Scanner](#)
- [Deleting an eEye REM Scanner](#)



Note: *If you want to use this scanner with a STRM release prior to 2008.2R2, you must add a firewall access rule for UDP and the associated listening port. For information on configuring your firewall access, see the [Configuring Access Settings, Configuring Firewall Access](#) section in the *STRM Administration Guide*. Make sure you select UDP and configure the same port that you want to configure in the scanner configuration.*

Adding an eEye REM Scanner

To add an eEye REM scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 11-1 eEye REM Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select eEye REM Scanner .

The list of parameters for the selected scanner type appears.

The screenshot shows the configuration window for an eEye REM scanner. The parameters and their values are as follows:

- Base Directory:** /store/wis/eEye/
- Cache Size:** 40
- Retention Period:** 432000000
- Listen Port:** 1162
- Source Host:** (empty)
- Version:** v2
- Community String:** public
- Authentication Protocol:** SHA
- Authentication Password:** (empty)
- Encryption Protocol:** DES
- Encryption Password:** (empty)

- Step 6** Enter values for the parameters:

Table 11-2 eEye Parameters

Parameter	Description
Base Directory	Specify the location you want to store the temporary files that result from the scan. The default is /store/vis/eEye/.
Cache Size	Specify the number of incomplete, concurrent data transactions you want to store before saving the information to disk. The default is 40.
Retention Period	Specify the time period, in milliseconds, the system stores scan information. If you do not have a scan scheduled by the end of the retention period, the information is deleted. The default is 432,000,000 milliseconds.
Listen Port	Specify the port that you want STRM to monitor for incoming scan information. The default is 1162.
Source Host	Specify the source IP address for the eEye REM server.
Version	Specify the version of SNMP you want to support for this scanner. The options are v1, v2, or v3.
Community String	Specify the SNMP community, such as public for incoming traffic. This parameter only applies if you are using SNMPv2.
Authentication Protocol	Specify the algorithm you want to use to authenticate SNMP traps. This parameter only applies to SNMPv3.
Authentication Password	Specify the password you want to use to authenticate SNMP. The password must be at least 8 characters in length. This parameter only applies to SNMPv3.
Encryption Protocol	Specify the protocol you want to use to decrypt SNMP traps. This parameter only applies to SNMPv3.
Encryption Password	Specify the password used to decrypt SNMP traps. The password must be at least 8 characters in length. This parameter only applies to SNMPv3.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, click **Deploy Changes**.

Editing an eEye REM Scanner

To edit a scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window appears.

Step 6 Update parameters, as necessary. See [Table 11-2](#).

Step 7 Click **Save**.

Step 8 From the Admin tab menu, click **Deploy Changes**.

Deleting an eEye REM Scanner

To delete a scanner:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window appears.

Step 6 Click **Ok**.

Step 7 From the Admin tab menu, click **Deploy Changes**.

12

MANAGING PatchLink SCANNERS

You can integrate a PatchLink scanner (version 6.4.4. and above) with STRM 2008.2R2 and above. The PatchLink scanner queries the PatchLink Scanner Engine using the PatchLink API. STRM collects vulnerability data from existing scan results with PatchLink. Therefore, your PatchLink system must include configuration that is appropriate for STRM to use and a scan that runs regularly to ensure results are current. Since the API provides access to the PatchLink application, make sure the PatchLink application runs continuously on the PatchLink server.



Note: *The PatchLink scanner is now known as the Lumension Security Management Console and is also formally known as the Harris Stat Guardian.*

To connect STRM to the PatchLink scanner, you must have appropriate administrative access to STRM and your PatchLink device. For more information, see your product documentation. Ensure that all firewalls are configured to allow a connection with your STRM system.

Once you configure the PatchLink device and the PatchLink scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the PatchLink scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring the PatchLink scanner including:

- [Adding a PatchLink Scanner](#)
- [Editing a PatchLink Scanner](#)
- [Deleting a PatchLink Scanner](#)

Adding a PatchLink Scanner

To add a PatchLink scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.

The VA Scanners window appears.

Step 4 Click **Add**.

The Add Scanner window appears.

Step 5 Enter values for the following parameters:

Table 12-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select PatchLink Scanner .

The list of parameters for the selected scanner type appears.



The screenshot shows a form with the following fields and values:

- Engine Address: [Empty text box]
- Port: 205
- Username: sa
- Password: [Empty text box]
- Job Name: [Empty text box]
- Result Refresh Rate (mins.): 15

Step 6 Enter values for the parameters:

Table 12-2 PatchLink Parameters

Parameter	Description
Engine Address	Specify the address where the PatchLink scanner is installed.
Port	The API transmits Simple Object Access Protocol (SOAP) requests over HTTPS to the engine's default port (205). If the default is changed by modifying the <code>HKLM\Software\Harris\reportcenter_listenport</code> registry key, specify the new port number.
Username	Specify the user name you want STRM to use for authenticating the PatchLink engine. The user must have access to the scan configuration (default sa).
Password	Specify the password corresponding to the Username.
Job Name	Specify the job name that exists in the PatchLink scanner and to which the user has access. Make sure this job is completed before you run the scan in STRM.

Table 12-2 PatchLink Parameters (continued)

Parameter	Description
Result Refresh Rate (mins)	Specify how often you want the scanner to retrieve results from the PatchLink server. This retrieval process is a resource intensive process that is only done after the interval defined in this field. Valid values are entered in minutes and the default is 15 minutes.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, click **Deploy Changes**.

Editing a PatchLink Scanner

To edit a scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window appears.
- Step 6** Update parameters, as necessary. See [Table 12-2](#).
- Step 7** From the Admin tab menu, click **Deploy Changes**.

Deleting a PatchLink Scanner

To delete a scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.

A confirmation window appears.

Step 6 Click **Ok**.

Step 7 From the Admin tab menu, click **Deploy Changes**.

13

MANAGING MCAFEE VULNERABILITY MANAGER SCANNERS

Once you install the STRM McAfee Vulnerability Manager, the scanner queries the McAfee Foundstone Enterprise engine using the FoundScan OpenAPI. The McAfee Vulnerability Manager scanner does not directly execute scans but gathers current scan results as displayed in the scanning application. STRM supports McAfee Vulnerability Manager versions 6.8 and above.



Note: *Foundstone and their scanner products have been acquired by McAfee and are sold as the McAfee Vulnerability Manager. If you are using a previous Foundstone Foundscan scanner version, see [Managing FoundScan Scanners](#).*

Your McAfee Foundstone Enterprise system must include a configuration appropriate for STRM and a scan that runs regularly to keep the results current. To ensure that your McAfee Vulnerability Manager scanner is able to retrieve scan information, make sure your McAfee Foundstone Enterprise system meets the following requirements:

- Since the Foundstone Open API provides access to the McAfee Foundstone Enterprise Manager server, make sure the McAfee Foundstone Enterprise application runs continuously on the McAfee Foundstone Enterprise Manager server.
- The scan that includes the necessary configuration to connect with STRM must be complete and visible in the McAfee Foundstone Enterprise interface for STRM to retrieve the scan results. If the scan does not appear in the McAfee Foundstone Enterprise interface or is scheduled to be removed after completion, STRM needs to retrieve the results before the scan is removed or the scan will fail.
- The appropriate user privileges must be configured in the McAfee Foundstone Configuration Manager application, which will allow STRM to communicate with McAfee Foundstone Enterprise.

Since the FoundScan OpenAPI only provides host and vulnerability information to STRM, your STRM Asset Profile information will display all vulnerabilities for a host assigned to port 0.

SSL connects the McAfee Foundstone Enterprise Manager server to the Foundstone Open API. STRM authenticates to the McAfee Foundstone Enterprise Manager server using client-side certificates. You must create and process the

appropriate certificates on the McAfee Foundstone Enterprise Manager server, then import the keys to STRM. For more information, see [Using Certificates](#).

Once you configure the McAfee Foundstone Enterprise system and the McAfee Vulnerability Manager scanner in the STRM interface, you can schedule a scan. The scan schedule configuration allows you to configure potency, however, the McAfee Vulnerability Manager scanner does not consider the potency parameter when performing the scan. For more information, see [Chapter 14 Managing Scan Schedules](#).

This chapter includes information on configuring a FoundScan scanner including:

- [Adding a McAfee Vulnerability Manager Scanner](#)
- [Editing a McAfee Vulnerability Manager Scanner](#)
- [Deleting a McAfee Vulnerability Manager Scanner](#)
- [Using Certificates](#)

Adding a McAfee Vulnerability Manager Scanner

To add a McAfee Vulnerability Manager scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Click **Add**.
The Add Scanner window appears.
- Step 5** Enter values for the following parameters:

Table 13-1 Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you want to assign to this scanner. The name may be up to 255 characters in length.
Description	Specify a description for this scanner. The description may be up to 50 characters in length.
Managed Host	Using the drop-down list box, select the managed host you want to configure this scanner.
Type	Using the drop-down list box, select McAfee Vulnerability Manager .

The list of parameters for the selected scanner type appears.

SOAP API URL:

Customer Name:

User Name:

Password:

Client IP Address:

Portal Name:

Configuration Name :

CA Truststore :

Client Keystore :

Step 6 Enter values for the parameters:

Table 13-2 McAfee Vulnerability Manager Parameters

Parameter	Description
SOAP API URL	Specify the web address for the Foundscan Open API in the following format: https://<IP address>:<SOAP port> Where: <IP address> is the IP address or hostname of the McAfee Foundstone Enterprise Manager Server. <SOAP port> is the port number for the Open API server's incoming connection. The default is https://localhost:3800 .
Customer Name	Specify a name to identify which customer or organization owns the user name. The customer name must match the Organization ID required for McAfee Foundstone Enterprise Manager log in.
User Name	Specify the user name you want STRM to use for authenticating the McAfee Foundstone Enterprise Manager server in the Open API. This user must have access to the scan configuration.
Password	Specify the password corresponding to the Login User Name for access to the Open API.
Client IP Address	Specify the IP address of the STRM server that you want to perform the scans. By default, this value is not used, however, is necessary for validating some environments.
Portal Name	Optional. Specify the portal name. This field may be left blank for STRM purposes. See your McAfee Vulnerability Manager administrator for more information.
Configuration Name	Specify the scan configuration name that exists in McAfee Foundstone Enterprise and to which the user has access.
CA Truststore	Specifies the directory path and filename for the CA truststore file. The default is /opt/qradar/conf/foundscan68.keystore.
Client Keystore	Specifies the directory path and filename for the client keystore. The default is /opt/qradar/conf/foundscan68.truststore.

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a In the text field, enter the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list.
 - b Click **Add**.
- Step 8** Click **Save**.
- Step 9** From the Admin tab menu, select **Deploy Changes**.

Editing a McAfee Vulnerability Manager Scanner

To edit an McAfee Vulnerability Manager scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window appears.
- Step 6** Update parameters, as necessary. See [Table 13-2](#).
- Step 7** Click **Save**.
- Step 8** From the Admin tab menu, select **Deploy Changes**.

Deleting a McAfee Vulnerability Manager Scanner

To delete a McAfee Vulnerability Manager scanner:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window appears.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window appears.
- Step 6** Click **Ok**.
- Step 7** From the Admin tab menu, select **Deploy Changes**.

Using Certificates

Creating third-party certificates and connecting through the Foundstone Open API requires the McAfee Certificate Manager Tool. If the certificate manager tool is not already installed on the McAfee Foundstone Enterprise Manager server, contact McAfee Technical Support.

You must process client-side certificates into valid keystore and truststore files for STRM on the McAfee Foundstone Enterprise Manager server. The McAfee Foundstone Enterprise Manager server must be compatible with the version of the FIPS-Capable OpenSSL used by the Foundstone Certificate Manager to correctly create the certificates. A Java Software Development Kit (Java SDK) must be present on this server for this processing. To obtain the latest Java SDK go to <http://java.sun.com>.

This section provides information on obtaining and importing the necessary certificates including:

- [Obtaining Certificates](#)
- [Processing Certificates](#)
- [Importing Certificates into STRM](#)

Obtaining Certificates

To obtain the necessary certificates:

- Step 1** Run the Foundstone Certificate Manager.
- Step 2** Click the **Create SSL Certificates** tab.
- Step 3** Enter the host address for STRM.
- Step 4** Click **Resolve** (optional).
If you choose not to resolve the host name, see [Step 6](#).
- Step 5** Click **Create Certificate Using Common Name**.
- Step 6** Click **Create Certificate Using Host Address**.
- Step 7** Save the ZIP file containing the certificate files to an accessible location.
- Step 8** Copy the pass phrase provided to a text file in the same known and accessible location.



Note: We recommend that you save this pass phrase for future use. If you misplace your pass phrase from [Step 8](#), you will be required to create new certificates.

You are now ready to process the certificates for STRM. See [Processing Certificates](#).

Processing Certificates To process the certificates:

- Step 1** Extract the ZIP file containing the certificates to any directory.
- Step 2** From the Qmmunity web site, download the following files into the same directory containing the extracted files from [Step 1](#).

`vulnerabilityManager-Cert.bat`
`qllabs_vis_foundscan.jar`



Note: You may be required to modify the following line found in the `vulnerabilityManager-Cert.bat` script to point to the location of the Java SDK:

```
set JAVA_HOME="C:\Program Files\Java\jdk1.6.0_20"
```

- Step 3** Execute `vulnerabilityManager-Cert.bat`.
- Step 4** Enter the pass phrase when prompted.

`Enter pass phrase for FoundstoneClientCertificate.pem:`

When the pass phrase is entered, the following message is displayed to inform you the files have been created.

`Created foundstone68.keystore and foundstone68.truststore files.`
 You are now ready to import the certificates into STRM. See [Importing Certificates into STRM](#).

Importing Certificates into STRM

The keystore and truststore files must be imported to STRM. We highly recommend that you use a secure method for copying certificate files such as SCP.



Note: Before importing files, we recommend that you remove or rename keystore and truststore files from previously configurations.

To import the certificates, secure copy the `foundstone68.keystore` and `foundstone68.truststore` files to STRM in the `/opt/qradar/conf` directory.

14

MANAGING SCAN SCHEDULES

This chapter provides information on managing the vulnerability assessment scan schedule including:

- [Viewing Scheduled Scans](#)
- [Scheduling a Scan](#)
- [Editing a Scan Schedule](#)
- [Deleting a Scheduled Scan](#)




Note: The below procedure describes how to manage scan schedules using the *Admin* tab. You can also manage scan schedules using the *VA Scan* option in the *Asset* tab.

Viewing Scheduled Scans

To view scheduled scans:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **Schedule VA Scanners** icon.
The Scan Scheduling appears.



VA Scanner	CIDR	Ports	Priority	Potency	Status	Concurrent Scans	Next Run Time
No results were returned.							

The following information is provided for each scheduled scan:

Table 14-1 Scheduled Scan Parameters

Parameter	Description
VA Scanner	Specifies the name of the schedule scan.
CIDR	Specifies the IP address(es) to be included in this scan. The VA scanner scans each IP address in the range individually.
Ports	<p>Specifies the ports included in the scan.</p> <p>If the scanner performing the scan directly executes the scan (NMap, Nessus, or Nessus Scan Results Importer), the specified ports restricts the number of ports scanned.</p> <p>However, for all other scanners, the port range is not considered when requesting asset information from a scanner. For example, ip360 and Qualys scanners report all ports.</p>
Priority	Specifies the priority of the scan: High or Low. When processing all scheduled scans, the scans with a high priority are executed before the low priority scans.
Potency	<p>Specifies the aggressiveness of the scan. The precise interpretation of the levels depends on the scanner, however, typically, the levels indicate:</p> <ul style="list-style-type: none"> • Very safe - Specifies a safe, non-intrusive assessment. They may generate false results. • Safe - Specifies an intermediate assessment and produces safe, banner-based results. • Medium - Specifies a safe intermediate assessment with accurate results. • Somewhat safe - Specifies an intermediate assessment but may leave service unresponsive. • Somewhat unsafe - Specifies an intermediate assessment, however, may result in your host or server cease functioning. • Unsafe - Specifies an intermediate assessment, however, this may cause your service to become unresponsive. • Very unsafe - Specifies an unsafe, aggressive assessment that may result in your host or server becoming unresponsive. <p>Note: Potency levels only apply to the Nessus and NMap scanners.</p>

Table 14-1 Scheduled Scan Parameters (continued)

Parameter	Description
Status	<p>Specifies the status of the scan:</p> <ul style="list-style-type: none"> • New - Specifies the schedule scan entry is newly created. When the status is New, you can edit the scan entry. Once the initial start time for the scan has been reached, the status changes to Pending and you can no longer edit the scan entry. • Pending - Specifies the scan has begun. The status remains Pending until the first results are received. The VA scanner submits a scan result for each IP address scanned. • Percentage complete - Each time an IP address is scanned, the VA scanner calculates the completion of the scan. Specifies the percentage complete status for the scan. • Complete - Once the calculated percentage complete reaches 100%, the scan is complete and the status changes to Complete. • Failed - Specifies an error has occurred in the scan process.
Concurrent Scans	<p>Specifies the number of simultaneous Vulnerability Assessment (VA) scan requests that the scanner sends to a device. The higher the value, the higher the processing load required for STRM to process concurrent scan requests.</p> <p><i>Note: STRM supports a maximum of 32 concurrent Vulnerability Assessment scans. The concurrent scan number is calculated by summing the values for all concurrent scans scheduled in a configuration. One-time complete scans, deleted or failed scans do not count toward the maximum concurrent scans limit.</i></p>
Next Run Time	<p>Specifies the next time that a scan will be run. Only a scan with a status of New, Failed, or Complete will be run when the Next Run Time arrives.</p> <p>If the scan is only scheduled to run once, the Next Run Time is zero.</p> <p>The Next Run Time value only updates when the scan is running.</p>

Scheduling a Scan

To schedule a Vulnerability Assessment scan:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **Schedule VA Scanners** icon.

The Scan Scheduling window appears.

Step 4 Click **Add**.

The Add Schedule window appears.



Note: If you do not have any scanners configured, an error message appears. You must configure the scanners before you can schedule a scan. For more information on configuring scanners, see [Chapter 1 Overview](#).

Step 5 Enter values for the parameters:

Table 14-2 Scan Schedule Parameters

Parameter	Description
VA Scanner	Using the drop-down list box, select the scanner for which you want to create a schedule.
Network CIDR	Choose one of the following options: <ul style="list-style-type: none"> • Network CIDR - Select the option and specify the network CIDR range to which you want this scan to apply. • Subnet/CIDR - Select the option and specify the subnet or CIDR range to which you want this scan to apply. The entered subnet/CIDR must be within the selected Network CIDR. The entered values must reflect the values configured in your VIS configuration.

Table 14-2 Scan Schedule Parameters (continued)

Parameter	Description
Potency	<p>Specify the level of scan you want to perform. The precise interpretation of the levels depends on the scanner, however, typically, the levels indicate:</p> <ul style="list-style-type: none"> • Very safe - Specifies a safe, non-intrusive assessment. They may generate false results. • Safe - Specifies an intermediate assessment and produces safe, banner-based results. • Medium - Specifies a safe intermediate assessment with accurate results. • Somewhat safe - Specifies an intermediate assessment but may leave service unresponsive. • Somewhat unsafe - Specifies an intermediate assessment, however, may result in your host or server cease functioning. • Unsafe - Specifies an intermediate assessment, however, this may cause your service to become unresponsive. • Very unsafe - Specifies an unsafe, aggressive assessment that may result in your host or server becoming unresponsive. <p>Note: Potency levels only apply to the Nessus and NMap scanners.</p>
Priority	Specify the priority you want to assign to this scan. The options are: High or Low.
Ports	Specify the ports you want this scan to apply.
Start Time	Specify the start date and time for the scan. The default is the local time of your STRM system.
Interval	Specify how often you want this scan to run. An interval of 0 indicates that the scan will run once.
Concurrent Scans	Specify the number of vulnerability scans you want to occur at the same time.

Step 6 Click **Save**.

Editing a Scan Schedule

To edit a Vulnerability Assessment scan schedule:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **Schedule VA Scanners** icon.
The Scan Scheduling window appears.
- Step 4** Select the schedule you want to edit.
- Step 5** Click **Edit**.

The Edit Schedule window appears.

Step 6 Update values, as necessary. See [Table 14-2](#).

Step 7 Click **Save**.

Deleting a Scheduled Scan

To delete a schedule Vulnerability Assessment scan:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **Schedule VA Scanner** icon.

The VA Scanners appears.

Step 4 Select the scan you want to delete.

Step 5 Click **Delete**.

A confirmation window appears.

Step 6 Click **OK**.

INDEX

C

conventions 5

E

eEye REM scanner
adding 62
deleting 64
editing 63

F

FoundScan
about 37
adding 38
custom certificates 41
deleting 40
editing 40

I

ip360
about 11
adding 12
deleting 15
editing 14
exporting reports 15

J

Juniper NSM Profiler
adding 49
editing 50

M

McAfee
about 69
adding 70
certificates 73
deleting 72
editing 72

N

Nessus
adding 18
deleting 21
editing 20
Nessus scan result importer
adding 23

deleting 26
editing 25

Nmap

adding 27
deleting 30
editing 29

P

PatchLink
adding 65
deleting 67
editing 67

Q

Qualys
adding 31
deleting 35
editing 35

R

Rapid7 NeXpose
adding 53
deleting 55
editing 55

S

scan
deleting schedule 50, 80
editing schedule 50, 79
scheduling 77
SecureScout
adding 58
deleting 60
editing 59

V

VA 7
vulnerability assessment 7
configuring 7

