



**Security Threat Response Manager**

# **Managing Vulnerability Assessment**

***Release\_2008.1***

**Juniper Networks, Inc.**

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

## Copyright Notice

Copyright © 2008 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 2008.1

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

31 January 2008—Revision 1

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

# CONTENTS

---

## ABOUT THIS GUIDE

- Documentation Feedback 3
- Requesting Support 3

---

## 1 OVERVIEW

- Configuring Vulnerability Assessment 5
- Viewing Scanners 6

---

## 2 MANAGING IP360 SCANNERS

- Adding a ip360 Scanner 7
- Editing an ip360 Scanner 9
- Deleting a ip360 Scanner 9

---

## 3 MANAGING NESSUS SCANNERS

- Adding a Nessus Scanner 11
- Editing an Nessus Scanner 13
- Deleting a Nessus Scanner 14

---

## 4 MANAGING NESSUS SCAN RESULT IMPORTERS

- Adding a Nessus Scan Result Importer 15
- Editing a Nessus Scan Result Importer 17
- Deleting a Nessus Scan Result Importer 17

---

## 5 MANAGING NMAP SCANNERS

- Adding a Nmap Scanner 19
- Editing an Nmap Scanner 21
- Deleting an Nmap Scanner 21

---

## 6 MANAGING QUALYS SCANNERS

- Adding a Qualys Scanner 23
- Editing a Qualys Scanner 24
- Deleting a Qualys Scanner 25

---

## **7 MANAGING FOUNDSCAN SCANNERS**

- Adding a FoundScan Scanner 28
- Editing a FoundScan Scanner 30
- Deleting a FoundScan Scanner 31
- Importing Custom Certificates 31
  - Example Of TrustedCA.pem File 33
  - Example of Portal.pem File 33

---

## **8 MANAGING JUNIPER NETWORKS NSM PROFILER SCANNERS**

- Adding a Juniper NSM Profiler Scanner 37
- Editing a Profiler Scanner 39
- Deleting a Profiler Scanner 39

---

## **9 MANAGING RAPID7 NEXPOSE SCANNERS**

- Adding a Rapid7 NeXpose Scanner 41
- Editing a Rapid7 NeXpose Scanner 42
- Deleting a Rapid7 NeXpose Scanner 43

---

## **10 MANAGING SCAN SCHEDULES**

- Scheduling a Scan 45
- Editing a Scan Schedule 47
- Deleting a Scheduled Scan 48

---

## **11 VIEWING ASSET PROFILE INFORMATION**

---

## **INDEX**

# ABOUT THIS GUIDE

This preface provides the following guidelines for using the *Managing Vulnerability Assessment Guide*:

- [Documentation Feedback](#)
- [Requesting Support](#)

---

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

---

## Requesting Support

Open a support case using the Case Management link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).



# 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 wish to scan.

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

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

---

### Configuring Vulnerability Assessment

To configure vulnerability assessment, you must:

**Step 1** Configure your scanner using one of the following supported scanners:

- [Chapter 2 Managing 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 Networks NSM Profiler Scanners](#)
- [Chapter 9 Managing Rapid7 NeXpose 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.

You must configure scanners using the Administration Console. For information on accessing the Administration Console, see the *STRM Administration Guide*.

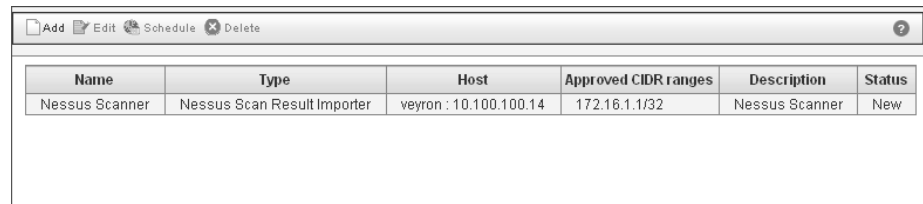
- Step 2** Schedule vulnerability assessment. See [Chapter 10 Managing Scan Schedules](#).
- Step 3** View the results of the asset profile. See [Chapter 11 Viewing Asset Profile Information](#).

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.

## Viewing Scanners

To view currently configured scanners:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** 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 wish 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 ip360 SCANNERS

nCircle ip360 can export scan results in XML to a remote server using SSH. STRM uses SSH to access the remote server (SSH expert server) then retrieves and interprets the scanned data. STRM supports VnE Manager version IP360-6.5.2.9. To configure the automated ip360 scan results, refer your vendor documentation.

This chapter includes information on configuring an ip360 scanner including:

- [Adding a ip360 Scanner](#)
- [Editing an ip360 Scanner](#)
- [Deleting a ip360 Scanner](#)



**Note:** For STRM compatibility, the scan data must be exported in the XML2 format.

---

### Adding a ip360 Scanner

To add an ip360 scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Click **Add**.  
The Add Scanner window appears.
- Step 4** Enter values for the following parameters:

**Table 2-1** Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you wish 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 255 characters in length.
Managed Host	Using the drop-down list box, select the managed host you wish to configure this scanner.
Type	Using the drop-down list box, select <b>nCircle IP360 Scanner</b> .

The list of parameters for the selected scanner type appears.

**Step 5** Enter values for the parameters:

**Table 2-2** ip360 Parameters

Parameter	Description
Path	Specify the location on the remote server where the scan results are stored. The default is /var/ncircle/.
SSH Server Host Name	Specify the IP address or host name to the remote server.
SSH Username	Specify the SSH remote server username.
Password	Specify the password to the remote server.
Private Key Authorization	Enable (Yes) or disable (No) private key authorization for the server. The default value is No.
Private Key Path	Specify the private key path. The default is /opt/qradar/conf/vis.ssh.key. This parameter is not used if the Private Key Authorization parameter is set to false.
File Pattern	The VIS retrieves reports, at the configured polling interval, from the nCircle device. Specify the file pattern you wish to retrieve. The default is XML2_ip360.d_1.a_[0-9]*.xml
Polling Interval	Specify the frequency that you wish the VIS to retrieve reports from the nCircle device. The default value is 900.

**Step 6** To configure the CIDR ranges you wish this scanner to consider:

- a In the text field, enter the CIDR range you wish this scanner to consider or click Browse to select the CIDR range from the network list.

- b Click **Add**.
- Step 7** Click **Save**.

---

### Editing an ip360 Scanner

To edit a scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to edit.
- Step 4** Click **Edit**.  
The Edit Scanner window appears.
- Step 5** Update parameters, as necessary. See [Table 2-2](#).
- Step 6** Click **Save**.

---

### Deleting a ip360 Scanner

To delete a scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to delete.
- Step 4** Click **Delete**.  
A confirmation window appears.
- Step 5** Click **Ok**.



# 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.*

STRM supports Nessus version 2.2.x to 3.0.4. 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** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **VA Scanners** icon.

The VA Scanners window appears.

**Step 3** Click **Add**.

The Add Scanner window appears.

**Step 4** Enter values for the following parameters:

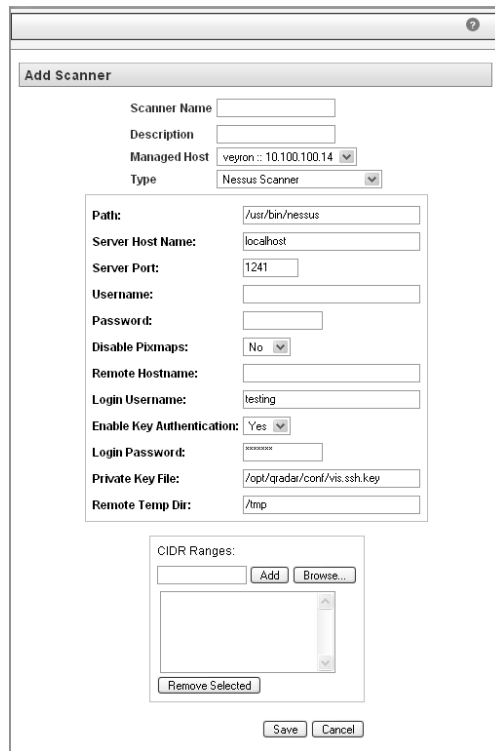
**Table 3-1** Scanner Parameters

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

**Table 3-1** Scanner Parameters (continued)

Parameter	Description
Description	Specify a description for this scanner. The description may be up to 255 characters in length.
Managed Host	Using the drop-down list box, select the managed host you wish to configure this scanner.
Type	Using the drop-down list box, select <b>Nessus Scanner</b> .

The list of parameters for the selected scanner type appears.



**Step 5** Enter values for the parameters:

**Table 3-2** Nessus Parameters

Parameter	Description
Path	Specify the location 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 DNS name of the Nessus server as seen by the Nessus client. 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.

**Table 3-2** Nessus Parameters (continued)

Parameter	Description
Disable Pixmaps	Enables (Yes) or Disables (No) pixmaps. 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 to the system that is hosting the Nessus client and execute the client with no parameters. An error message appears if no graphical client is installed.
Remote Hostname	Specify the DNS name or IP address of the system hosting the Nessus client.
Login Username	Specifies 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. The default is Yes. For more information, see your SSH documentation for configuring public key authentication.
Login Password	If Enable Key Authentication is disabled, specify the password that STRM uses to authenticate the SSH connection.  If key authentication is disabled, you must set a login password.
Private Key File	Specify the directory path to 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 <code>/opt/qradar/conf/vis.ssh.key</code> .  This parameter is mandatory if key authentication is enabled.
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. Default setting is <code>/tmp</code> .

**Step 6** To configure the CIDR ranges you wish this scanner to consider:

- a In the text field, enter the CIDR range you wish this scanner to consider or click **Browse** to select the CIDR range from the network list.
- b Click **Add**.

**Step 7** Click **Save**.

---

## Editing an Nessus Scanner

To edit a scanner:

**Step 1** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **VA Scanners** icon.

The VA Scanners window appears.

- Step 3** Select the scanner you wish to edit.
- Step 4** Click **Edit**.  
The Edit Scanner window appears.
- Step 5** Update parameters, as necessary. See [Table 3-2](#).
- Step 6** Click **Save**.

---

### Deleting a Nessus Scanner

To delete a scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to delete.
- Step 4** Click **Delete**.  
A confirmation window appears.
- Step 5** Click **Ok**.

# 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 scan results from Nessus version 2.2.x to 3.0.4. For more information on installing and configuring Nessus, see your Nessus documentation.



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

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** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Click **Add**.  
The Add Scanner window appears.
- Step 4** Enter values for the following parameters:

**Table 4-1** Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you wish 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 255 characters in length.

**Table 4-1** Scanner Parameters (continued)

Parameter	Description
Managed Host	Using the drop-down list box, select the managed host you wish to configure this scanner.
Type	Using the drop-down list box, select <b>Nessus Scan Result Importer</b> .

The list of parameters for the selected scanner type appears.

**Step 5** Enter values for the parameters:

**Table 4-2** Nessus Scan Result Importer Parameters

Parameter	Description
Remote Hostname	Specify the DNS name or IP address of the system hosting the Nessus scan results file.
Login Username	Specifies 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. The default is Yes. For more information, see your SSH documentation for configuring public key authentication.
Login Password	If Enable Key Authentication is disabled, specify the password that STRM uses to authenticate the SSH connection. If key authentication is disabled, you must set a login password.

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

Parameter	Description
Private Key File	Specify the directory path to 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.  This parameter is mandatory if key authentication is enabled.
Remote Results File	Specify the directory and filename on the Nessus server from which STRM retrieves the scan results.

- Step 6** To configure the CIDR ranges you wish this scanner to consider:
- a In the text field, enter the CIDR range you wish this scanner to consider or click Browse to select the CIDR range from the network list.
  - b Click **Add**.
- Step 7** Click **Save**.

---

### Editing a Nessus Scan Result Importer

To edit a Nessus Scan Result Importer:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to edit.
- Step 4** Click **Edit**.  
The Edit Scanner window appears.
- Step 5** Update parameters, as necessary. See [Table 4-2](#).
- Step 6** Click **Save**.

---

### Deleting a Nessus Scan Result Importer

To delete a Nessus Scan Result Importer:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **Scanner Configuration Management** icon.  
The Scanner Configurations window appears.
- Step 3** Using the Existing Configurations drop-down list box, select the scanner you wish to delete.

## 18 MANAGING NESSUS SCAN RESULT IMPORTERS

**Step 4** Click **Delete**.

The confirmation window appears.

**Step 5** Click **Ok**.

# 5

## MANAGING NMAP SCANNERS

You can integrate Network Mapper (Nmap) scanners (version 4.2) 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.

Before you configure your scanners, you must configure the server that hosts your scanner. You can install a scanner locally on the system hosting the STRM Console (not recommended) or on a remote system. To set up a scanner on a remote system, the remote system must be designated as the scanner server and have the latest STRM supported versions of scanner software and SSH installed. For future assistance, see your scanner and SSH documentation.

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** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Click **Add**.  
The Add Scanner window appears.
- Step 4** Enter values for the following parameters:

**Table 5-1** Scanner Parameters

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

**Table 5-1** Scanner Parameters (continued)

Parameter	Description
Description	Specify a description for this scanner. The description may be up to 255 characters in length.
Managed Host	Using the drop-down list box, select the managed host you wish to configure this scanner.
Type	Using the drop-down list box, select <b>NMap Scanner</b> .

The list of parameters for the selected scanner type appears.

**Step 5** Enter values for the parameters:

**Table 5-2** Nmap Parameters

Parameter	Description
Path	Specify the location of the executable file for the Nmap application. The default is /usr/bin/nmap.
Disable Ping	Enables or disables ICMP pings. The default is False.
Remote Hostname	Specify the hostname or IP address of the system hosting the Nmap client.
Login Username	Specify the username necessary to access the system hosting the Nmap client.

**Table 5-2** Nmap Parameters (continued)

Parameter	Description
Enable Key Authentication	Enables (Yes) or disables (No) public/private key authentication. The default is Yes.
Login Password	If Enable Key Authentication is disabled, specify the password necessary to log in to the Nessus client system. If key authentication is disabled, you must set a login password.
Private Key File	Specify the directory path to the file that contains the private key information. The default is /opt/qradar/conf/vis.ssh.key. This parameter is mandatory if key authentication is enabled.

- Step 6** To configure the CIDR ranges you wish this scanner to consider:
- a In the text field, enter the CIDR range you wish this scanner to consider or click Browse to select the CIDR range from the network list.
  - b Click **Add**.
- Step 7** Click **Save**.

---

### Editing an Nmap Scanner

To edit an Nmap scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to edit.
- Step 4** Click **Edit**.  
The Edit Scanner window appears.
- Step 5** Update parameters, as necessary. See [Table 5-2](#).
- Step 6** Click **Save**.

---

### Deleting an Nmap Scanner

To delete an Nmap scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to delete.
- Step 4** Click **Delete**.

A confirmation window appears.

**Step 5** Click **Ok**.

# 6

## MANAGING QUALYS SCANNERS

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

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

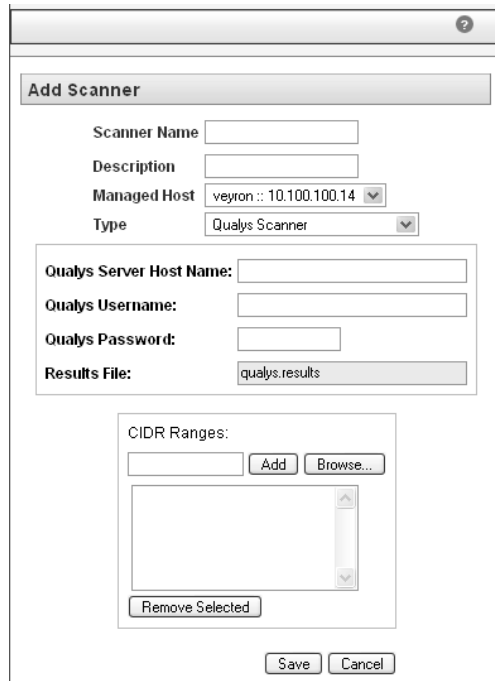
To add a Qualys scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Click **Add**.  
The Add Scanner window appears.
- Step 4** Enter values for the following parameters:

**Table 6-1** Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you wish 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 255 characters in length.
Managed Host	Using the drop-down list box, select the managed host you wish to configure this scanner.
Type	Using the drop-down list box, select <b>Qualys Scanner</b> .

The list of parameters for the selected scanner type appears.



**Step 5** Enter values for the parameters:

**Table 6-2** Qualys Parameters

Parameter	Description
Qualys Server Host Name	Specify the hostname or IP address of the QualysGuard server.
Qualys Username	Specify the username to log in to the Qualys server.
Qualys Password	Specify the password to log in to the Qualys server.
Results File	Specify the temporary file name you wish to store the Qualys scan results. The default is qualys.results.

**Step 6** To configure the CIDR ranges you wish this scanner to consider:

- a In the text field, enter the CIDR range you wish this scanner to consider or click **Browse** to select the CIDR range from the network list.
- b Click **Add**.

**Step 7** Click **Save**.

### Editing a Qualys Scanner

To edit a Qualys scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab. The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.

The VA Scanners window appears.

**Step 3** Select the scanner you wish to edit.

**Step 4** Click **Edit**.

The Edit Scanner window appears.

**Step 5** Update parameters, as necessary. See [Table 6-2](#).

**Step 6** Click **Save**.

---

### Deleting a Qualys Scanner

To delete an Qualys scanner:

**Step 1** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **VA Scanners** icon.

The VA Scanners window appears.

**Step 3** Select the scanner you wish to delete.

**Step 4** Click **Delete**.

A confirmation window appears.

**Step 5** Click **Ok**.



# 7

## MANAGING FOUNDSCAN SCANNERS

Once you install the STRM Foundstone FoundScan scanner, the scanner queries the FoundScan Engine using the FoundScan OpenAPI. STRM collects vulnerability data from existing scan results with FoundScan. Therefore, your FoundScan system must include a configuration appropriate for STRM to use and a scan that runs regularly to keep the results current. Since the API provides access to the FoundScan application, it is also important that the FoundScan application runs continuously on the FoundScan server.



**Note:** *We recommend that you install the FoundScan scanner alone and deploy all changes through the STRM Administration Console to ensure that all files are properly distributed to all STRM managed hosts.*

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 earlier than 5.1, you must import the appropriate certificates and keys on the STRM host(s). For more information, see [Importing Custom Certificates](#).

This chapter includes information on configuring a FoundScan scanner including:

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

## Adding a FoundScan Scanner

To add a FoundScan scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Click **Add**.  
The Add Scanner window appears.
- Step 4** Enter values for the following parameters:

**Table 7-1** Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you wish 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 255 characters in length.
Managed Host	Using the drop-down list box, select the managed host you wish to configure this scanner.
Type	Using the drop-down list box, select <b>FoundScan Scanner</b> .

The list of parameters for the selected scanner type appears.

**Step 5** Enter values for the parameters:

**Table 7-2** FoundScan Parameters

Parameter	Description
SOAP API URL	Specify the web address for the SOAP API in the following format:  <b>https://&lt;foundstone IP address&gt;:&lt;SOAP port&gt;</b> 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 <b>https://localhost:3800</b>
Customer Name	Specify the name of the customer under which the Login User Name belongs.
User Name	Specify the user name you wish STRM to use for authenticating the FoundScan engine. This user must have access to the scan configuration.
Password	Specify the password corresponding to the Login User Name.
Client IP Address	Specify the IP address of the STRM server. By default, this value is not used, however, is necessary for validating some environments.

**Table 7-2** FoundScan Parameters (continued)

Parameter	Description
Portal Name	Specify the IP address or hostname of the FoundScan server. This field is optional, however, may be necessary for authentication. 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 /opt/qradar/conf/foundscan.keystore.
Client Keystore	Specifies the directory path and filename for the client keystore. The default is /opt/qradar/conf/foundscan.truststore.
CA Truststore	Specifies the directory path and filename for the CA truststore file. The default is /opt/qradar/conf/foundscan.keystore.
Client Keystore	Specifies the directory path and filename for the client keystore. The default is /opt/qradar/conf/foundscan.truststore.

**Step 6** To configure the CIDR ranges you wish this scanner to consider:

- a In the text field, enter the CIDR range you wish this scanner to consider or click **Browse** to select the CIDR range from the network list.
- b Click **Add**.

**Step 7** Click **Save**.

---

## Editing a FoundScan Scanner

To edit an FoundScan scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to edit.
- Step 4** Click **Edit**.  
The Edit Scanner window appears.
- Step 5** Update parameters, as necessary. See [Table 7-2](#).
- Step 6** Click **Save**.

---

## Deleting a FoundScan Scanner

To delete a FoundScan scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to delete.
- Step 4** Click **Delete**.  
A confirmation window appears.
- Step 5** Click **Ok**.

---

## Importing Custom Certificates

If the FoundScan Engine includes custom certificates, you must import the certificates on each STRM managed host that will host the VIS component. Before you perform the below procedure, make sure the FoundScan scanner is installed.

To import custom certificates:

- Step 1** Obtain two certificate files 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. Make sure the filename allows you to easily distinguish the CA certificate file from the private key chain file.
- Step 3** On the STRM host, change the directory to where the two PEM files are copied.
- Step 4** 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 5** Repeat for all managed hosts in your deployment, which will host the VIS.

**Example Of TrustedCA.pem File**

```
-----BEGIN CERTIFICATE-----
MIICFzCCAYCgAwIBAgIBADANBgkqhkiG9w0BAQQFADAYMRYwFAYDVQQDEw1Gb3Vu
ZHN0b251IENBMB4XDTAzMDkxMjIzMjkxMVoXDTA4MTAyMDIzMjkxMVowGDEWMBQG
A1UEAxMNRM91bmRzdG9uZSBDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
sWN8ZqqREmZ7qByvuIqr2q4XaP5TfP3hRC08mjvqWsQjk2B8WMRAGzjHqvPN/qfG
5uZw5gm1M6IyoVbLkaQwDF34McRpqlTLVjeDadjPuRazGVu4zVknC8s83EPqKU9+
fdqmhtCwwqVYq+sQFp1S3kKUvXIBEGV0r9mnFAD3InUCAwEAAANxMG8wHQYDVR0O
BBYEFGQ8UJTPbqSP202Mygs2sqzU2h7LMEAGA1UdIwQ5MDeAFGQ8UJTPbqSP202M
ygs2sqzU2h7LoRykGjAYMRYwFAYDVQQDEw1Gb3VuZHN0b251IENBggEAMAwGA1Ud
EwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAQ7F9nq4X/RemMag+0ORM+mnEp/0i
j0ynMtEM2mtuf95uxeGFe581k31w9d3IGt19uahtyqG860kr4/ys3r7LjA0f9rjf
J9PUXhzRqqh8yzh795R9Dloj7hsyZtq4My6gKu8RuHVBscYvJVvPMUkPmDHMnpj1
4p7dh7GKk7ymFYs=
-----END CERTIFICATE-----
```

**Example of Portal.pem File**

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQC5DOnQtMtDXAHth/4M/1I9gVlyoch9EYvCiAsZmtO2JMTjedse
mh0DQkxSKv0gvsCqKXh6nNegyyiCM1GuEDvFYPCI5FrkrzEwtndTILGXT5asDXu
SbPTMrBKR5pFMJoPJ/Sjc0vf6A48Nn8FiYLDiyBLKhunzMO3EZ22VrZxBwIDAQAB
AoGARZfkqzgdJZ8JnpJBahOPTFBEGodbhIW+IPfW7Nc8fcjQPvDQuw3wHfSmDVTh
g6AZhyU1FBzvLIE6nOmggdMzn9KIN8WMD+XDAAR4AaWOGkn18Ib4h1VVnsa90hYS
ncnAl/9am4jAhADDPfb9ZRMoE6aFE13XD21o49gJG4sH+VkcQQDrf6OGfnR6YaYz
4QFLQzPOQz4bN+vIFLWBZX2r6gCD1PkLfZEYijnycbtJdmATccSf9qLOt9VP28y+
BPIWVsfbAkeAySj6iwtolLVsXC5cIP4YzNzNs j2QBqeEhEfUmLtZl8vD1sj+EM2L
JggOcRpYmXIj64ob/hevavXew1CFermpRQJBAKaq6OKQsILEhUoGHLJTt2BtOpEs
3JP4BBUV7QE0VTTKxA8byQqjGSu6zh/JxWk9hTjo5oSCmlcwahC5k104Cy0CQQCt
vnwv7mncFtsB/3TJdk67Wxc7FRs59CRsEJKaXG80weVjtXRj1PSto6+9ltCJQ+jm
fxxQaeq0SqqEWlb+UuC1AkeAr6Z503v5p1rVUWT0+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-----

MIICVDCCAb2gAwIBAgIBAjanBgkqhkiG9w0BAQQFADAYMRYwFAYDVQQDEw1Gb3Vu  
ZHN0b251IENBMB4XDTAzMDkxMjIzMzY1NFoXDTA4MTAyMDIzMzY1NFowKDEmMCQG  
A1UEAxMdrM91bmRzdG9uZSBFbnRlcnByaXNlIE1hbmFnZXIwZ8wDQYJKoZIhvcN  
AQEBBQADgY0AMIGJAoGBAlkM6dC0y0NcAe2H/gz+Uj2BWxKhyH0Ri8KICxma07Yk  
xOMQox6YfQNCTFIq/SC+wKopcFHqc16DLKIIzUa4QO8Vg8IjkWuSvMTC2d1MgsZd  
PlqwNe5Js9MysEpHml8wmg8n9KNzS9/oDjw2fwWJgsOLIEsqG6fMzTcRnbZWtnEH  
AgMBAAGjgZ0wgZowCQYDVR0TBAlwADAsBglghkgBhvhCAQ0EHzYdT3BlblNTTCBH  
ZW51cmF0ZWQgQ2VydG1maWNhdGUwHQYDVR0OBByEFA1SVO+gs5GdPUs2J5iKjQP  
Cf+NMEAGA1UdIwQ5MDeAFGQ8UJTPbqSP202Mygs2sqzU2h7LoRykGjAYMRYwFAYD  
VQQDEw1Gb3VuZHN0b251IENBggEAMA0GCSqGSIsb3DQEBAUAA4GBAEqIP1E0WzA7  
W3xXMYyiOwAWYax7t67NaBEBolK3WR7GW68q7fnu72QRsrkUIX0sNdPLCQihqyaT  
D6qX68xlq5WjDXcLIyBKDQYRy1Yp95hn6o82qUANbXrUvviWlZFAgJ53w+HvPOC  
0T05eZ7vZOL1YZvqKZT7AI+4CHzw7mi2

-----END CERTIFICATE-----



# 8

## MANAGING JUNIPER NETWORKS NSM PROFILER SCANNERS

The Juniper Networks NSM console passively collects valuable asset information from your network through deployed Juniper Networks 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 version 2006.2. For more information, see your vendor documentation.

This chapter includes information on configuring a Juniper Networks scanner including:

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

---

### Adding a Juniper NSM Profiler Scanner

To add a Juniper NSM Profiler scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Click **Add**.  
The Add Scanner window appears.
- Step 4** Enter values for the following parameters:

**Table 8-1** Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you wish 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 255 characters in length.

**Table 8-1** Scanner Parameters (continued)

Parameter	Description
Managed Host	Using the drop-down list box, select the managed host you wish to configure this scanner.
Type	Using the drop-down list box, select <b>Juniper NSM Profiler Scanner</b> .

The list of parameters for the selected scanner type appears.

**Step 5** 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 username to log in to the Profiler database stored on the NSM server.
Database Password	Specify the password to log in to the server.
Database Name	Specify the name of the Profiler database. The default is profilerDB.

- Step 6** To configure the CIDR ranges you wish this scanner to consider:
- a In the text field, enter the CIDR range you wish this scanner to consider or click Browse to select the CIDR range from the network list.
  - b Click **Add**.
- Step 7** Click **Save**.

---

### Editing a Profiler Scanner

To edit an Juniper NSM Profiler scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to edit.
- Step 4** Click **Edit**.  
The Edit Scanner window appears.
- Step 5** Update parameters, as necessary. See [Table 8-2](#).
- Step 6** Click **Save**.

---

### Deleting a Profiler Scanner

To delete an Juniper NSM Profiler scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to delete.
- Step 4** Click **Delete**.  
A confirmation window appears.
- Step 5** Click **Ok**.



# 9

## MANAGING RAPID7 NEXPOSE SCANNERS

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](#)

STRM supports Rapid7 NeXpose version 4.5 and above. For more information, see your Rapid7 NeXpose documentation.

---

### Adding a Rapid7 NeXpose Scanner

To add a Rapid7 NeXpose scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Click **Add**.  
The Add Scanner window appears.
- Step 4** Enter values for the following parameters:

**Table 9-1** Scanner Parameters

Parameter	Description
Scanner Name	Specify the name you wish 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 255 characters in length.
Managed Host	Using the drop-down list box, select the managed host you wish to configure this scanner.
Type	Using the drop-down list box, select <b>Rapid7 Nexpose Scanner</b> .

The list of parameters for the selected scanner type appears.

**Step 5** 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.
Login Password	Specify the password to log in to the Rapid7 NeXpose server.
Nexpose Site Id	Specify the site identifier you wish the scan to use.

**Step 6** To configure the CIDR ranges you wish this scanner to consider:

- a In the text field, enter the CIDR range you wish this scanner to consider or click Browse to select the CIDR range from the network list.
- b Click **Add**.

**Step 7** Click **Save**.

### Editing a Rapid7 NeXpose Scanner

To edit a Rapid7 NeXpose scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab. The SIM Configuration panel appears.

- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to edit.
- Step 4** Click **Edit**.  
The Edit Scanner window appears.
- Step 5** Update parameters, as necessary. See [Table 9-2](#).
- Step 6** Click **Save**.

---

**Deleting a Rapid7 NeXpose Scanner**

To delete a Rapid7 NeXpose scanner:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **VA Scanners** icon.  
The VA Scanners window appears.
- Step 3** Select the scanner you wish to delete.
- Step 4** Click **Delete**.  
A confirmation window appears.
- Step 5** Click **Ok**.



# 10

## MANAGING SCAN SCHEDULES

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

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



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

---

**Scheduling a Scan** To schedule a Vulnerability Assessment scan:

**Step 1** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **Schedule VA Scanner** icon.

The VA Scanners appears.

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

**Step 3** 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 4** Enter values for the parameters:

**Table 10-1** Scan Schedule Parameters

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

**Table 10-1** Scan Schedule Parameters (continued)

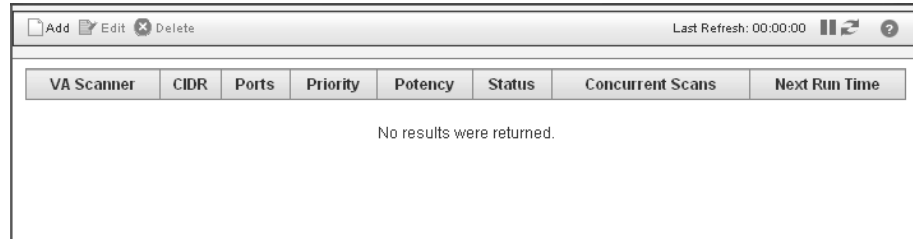
Parameter	Description
Potency	Specify the level of scan you wish to perform. The precise interpretation of the levels depends on the scanner, however, typically, the levels indicate: <ul style="list-style-type: none"> <li>• <b>Very safe</b> - Specifies a safe, non-intrusive assessment. They may generate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

**Step 5** Click **Save**.

## Editing a Scan Schedule

To edit a Vulnerability Assessment scan schedule:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.  
The SIM Configuration panel appears.
- Step 2** Click the **Schedule VA Scanner** icon.  
The VA Scanners appears.



**Step 3** Select the schedule you wish to edit.



**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 4** Click **Edit**.

The Edit Schedule window appears.

**Step 5** Update values, as necessary. See [Table 10-1](#).

**Step 6** Click **Save**.

---

## Deleting a Scheduled Scan

To delete a schedule Vulnerability Assessment scan:

**Step 1** In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

**Step 2** Click the **Schedule VA Scanner** icon.

The VA Scanners appears.

**Step 3** Select the scan you wish to delete.

**Step 4** Click **Delete**.

A confirmation window appears.

**Step 5** Click **Ok**.

# 11

## VIEWING ASSET PROFILE INFORMATION

You can access asset profile data for any IP address that appears in the asset profile.



**Note:** For more information on Assets, see the *Managing Assets Chapter* in the *STRM Users Guide*

To view asset profile data:

**Step 1** On any IP address in the STRM interface, use the right mouse button (right-click) to access the menu.

The menu appears.

**Step 2** Select **Information > Asset Profile**.

The Asset Profile window appears. If the Asset Profile menu option is not available, no data is available for the selected IP address.

Asset Profile Ports History

Name			
Description			
IP Address	10.105.2.3	VA Risk Level	1
Operating System		How Threatening	10
Host Name (DNS Name)	10.105.2.3	How Threatened	0
Asset Weight	0 - Not Important		
MAC		Host Name	
Machine Name			
User		User Group	
Extra Data			

Save Changes Cancel Close Window

Port	OSVDB ID	Name	Description	Risk / Severity	Last Seen	First Seen
25				1	2007-02-05 23:15:00 (Passive)	2007-02-05 23:15:00 (Passive)
53				1	2007-02-05 23:15:00 (Passive)	2007-02-05 23:15:00 (Passive)

The Asset Profile window provides the following:

**Table 11-2** Asset Profile Window

Parameter	Description
Name	Specify a name you wish to associate with this asset profile.
Description	Specify a description that you wish to associate with this asset profile.
IP Address	Specifies the IP address of the asset.
Operating System	Specifies the operating system running on the asset.
Host Name (DNS Name)	Specifies the IP address or DNS name of the asset.
Asset Weight	Using the drop-down list box, specify the level of importance you wish to associate with this asset. The range is 0 (not valuable) to 10 (very valuable).
VA Risk Level	Specifies the vulnerability assessment risk level (0 to 10) for the asset where 0 is the lowest and 10 is the highest. This is a weighted value against all other hosts in your deployment.
How Threatening	Specifies the threat level (0 to 10) posed by the asset where 0 is the lowest and 10 is the highest. This is a weighted value against all other hosts in your deployment.
How Threatened	Specifies the threat level (0 to 10) to the asset where 0 is the lowest and 10 is the highest. This is a weighted value against all other hosts in your deployment.
MAC	Specifies the MAC address of the asset.
Machine Name	Specifies the name of the asset system.
User	Specifies the last user associated with this asset.
Extra Data	Specifies any additional information associated with this asset.
Host Name	Specifies the host name of this asset.
User Group	Specifies the user group associated with this asset.

**Step 3** To view port information, click **Ports**. This is the default display for assets.

**Table 11-3** Ports Information

Parameter	Description
Port	Specifies the port number for the services discovered running on the asset.
OSVDB ID	Specifies the vulnerability identifier for the asset. Click the ID to obtain more information.
Name	Specifies the name of the detected vulnerability. This value is only available when integrating with VA tools.
Description	Specifies a description of the detected vulnerability. This value is only available when integrating with VA tools.
Risk/Severity	Specifies the risk level for the vulnerability.

**Table 11-3** Ports Information (continued)

Parameter	Description
Last Seen	Specifies the date and time that the service was last detected running on the asset both either passively or actively.
First Seen	Specifies the date and time when the service was first detected running on the asset both either passively or actively.

**Step 4** To view History information, click **History**.

**Table 11-4** History Information

Parameter	Description
MAC	Specifies the MAC address for this asset. If unknown, this field is blank.
Host Name	Specifies the host name of this asset. If unknown, this field is blank.
Machine Name	Specifies the machine name of this asset. If unknown, this field is blank.
User	Specifies the user for this asset. If unknown, this field is blank.
User Group	Specifies the user group for this asset. If unknown, this field is blank.
Extra Data	Specifies any extra information for this asset. If the text for this field is greater than 50 characters, click the text to view the full text in a separate window.
Last Observed	Specifies the last time data was recorded for this asset.

**Step 5** Click **Save Changes**.

**Step 6** Click **Close Window**.



# INDEX

---

## F

FoundScan  
about 27  
adding 28  
custom certificates 31  
deleting 31  
editing 30

---

## I

ip360  
about 7  
adding 7  
deleting 9  
editing 9

---

## J

Juniper NSM Profiler  
adding 37  
deleting 39  
editing 39

---

## N

Nessus  
adding 11  
deleting 14  
editing 13  
nessus scan result importer  
adding 15  
deleting 17  
editing 17  
Nmap  
adding 19  
deleting 21  
editing 21

---

## Q

Qualys  
adding 23  
deleting 25  
editing 24

---

## R

Rapid7 NeXpose  
adding 41  
deleting 43  
editing 42

---

## S

scan  
deleting schedule 48  
editing schedule 47  
scheduling 45

---

## V

VA 5  
vulnerability assessment 5  
configuring 5

