



Security Threat Response Manager

Managing Vulnerability Assessment

Release 2013.2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Published: 2013-07-19

Copyright Notice

Copyright © 2013 Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc.

The following terms are trademarks or registered trademarks of other companies:

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.



All other trademarks, service marks, registered trademarks, or registered service marks are the property of 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 Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

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

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT, SUBJECT TO THE MODIFICATIONS SET FORTH BELOW ON THIS PAGE, 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 2013.2

Copyright © 2013, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

July 2013—Managing Vulnerability Assessment

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>, as modified by the following text, which shall be treated under the EULA as an Entitlement Document taking precedence over any conflicting provisions of such EULA as regards such software:

As regards software accompanying the STRM products (the "Program"), such software contains software licensed by Q1 Labs and is further accompanied by third-party software that is described in the applicable documentation or materials provided by Juniper Networks.

For the convenience of Licensee, the Program may be accompanied by a third party operating system. The operating system is not part of the Program, and is licensed directly by the operating system provider (e.g., Red Hat Inc., Novell Inc., etc.) to Licensee. Neither Juniper Networks nor Q1 Labs is a party to the license between Licensee and the third party operating system provider, and the Program includes the third party operating system "AS IS", without representation or warranty, express or implied, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement. For an installed Red Hat operating system, see the license file: /usr/share/doc/redhat-release-server-6Server/EULA.

By downloading, installing or using such software, you agree to the terms and conditions of that EULA as so modified.

CONTENTS

ABOUT THIS GUIDE

| | |
|------------------------------------|----|
| Audience | 9 |
| Documentation Conventions | 9 |
| Technical Documentation | 9 |
| Requesting Technical Support | 10 |

1 OVERVIEW

| | |
|--|----|
| Configure Vulnerability Assessment | 13 |
| Manually Install a Scanner | 14 |
| View Configured Scanners | 15 |

2 MANAGE BEYOND SECURITY AVDS SCANNERS

| | |
|---|----|
| Add a Beyond Security AVDS Scanner | 17 |
| Edit a Beyond Security AVDS Scanner | 19 |
| Delete a Beyond Security AVDS Scanner | 20 |

3 MANAGE IBM SECURITY APPSCAN ENTERPRISE SCANNERS

| | |
|--|----|
| Configure AppScan Enterprise | 21 |
| Create a Custom User Type | 22 |
| Enable STRM Integration | 22 |
| Create an Application Deployment Map | 22 |
| Publish Reports to STRM | 23 |
| Configure a Scanner in STRM | 24 |
| Add an AppScan Enterprise Scanner | 24 |
| Edit an AppScan Enterprise Scanner | 26 |
| Delete an AppScan Enterprise Scanner | 26 |

4 MANAGE IBM GUARDIUM SCANNERS

| | |
|--------------------------------------|----|
| Add an IBM Guardium Scanner | 27 |
| Edit an IBM Guardium Scanner | 29 |
| Delete an IBM Guardium Scanner | 30 |

5 MANAGE IBM SITEPROTECTOR SCANNERS

| | |
|---|----|
| Add an IBM SiteProtector Scanner | 31 |
| Edit an IBM SiteProtector Scanner | 33 |

| | |
|--|----|
| Delete an IBM SiteProtector Scanner. | 34 |
|--|----|

6 IBM TIVOLI ENDPOINT MANAGER SCANNER

| | |
|--|----|
| Add an IBM Tivoli Endpoint Manager Scanner. | 35 |
| Edit an IBM Tivoli Endpoint Manager Scanner. | 37 |
| Delete an IBM Tivoli Endpoint Manager Scanner. | 37 |

7 MANAGE nCIRCLE IP360 SCANNERS

| | |
|--|----|
| Add an nCircle IP360 Scanner. | 39 |
| Edit an nCircle IP360 Scanner. | 41 |
| Delete an nCircle IP360 Scanner. | 42 |
| Export nCircle Scan Reports. | 42 |

8 MANAGE NESSUS SCANNERS

| | |
|--|----|
| Add a Nessus Scanner. | 44 |
| Add a Nessus Scheduled Live Scan. | 44 |
| Add a Nessus Scheduled Results Import. | 46 |
| Add a Nessus Scheduled Live Scan Using the XMLRPC API. | 48 |
| Add a Nessus Completed Report Import Using the XMLRPC API. | 50 |
| Edit a Nessus Scanner. | 52 |
| Delete a Nessus Scanner. | 52 |

9 MANAGE NMAP SCANNERS

| | |
|---|----|
| Add an Nmap Remote Live Scan. | 56 |
| Add an Nmap Remote Results Import Scan. | 58 |
| Edit an Nmap Scanner. | 60 |
| Delete an Nmap Scanner. | 60 |

10 MANAGE QUALYS SCANNERS

| | |
|--|----|
| Configure a Qualys Detection Scanner. | 64 |
| Add a Qualys Detection Scanner. | 64 |
| Edit a Qualys Detection Scanner. | 66 |
| Delete a Qualys Detection Scanner. | 67 |
| Configure a Qualys Scanner. | 68 |
| Add a Qualys Scheduled Live Scan Report. | 68 |
| Add a Qualys Scheduled Import Asset Data Report. | 70 |
| Add a Qualys Scheduled Import Scan Report. | 72 |
| Edit a Qualys Scanner. | 75 |
| Delete a Qualys Scanner. | 76 |

11 MANAGE FOUNDSCAN SCANNERS

| | |
|-------------------------------------|----|
| Add a FoundScan Scanner. | 78 |
| Edit a FoundScan Scanner. | 79 |
| Delete a FoundScan Scanner. | 80 |
| Configure Certificates. | 80 |

| | | |
|-----------|---|-----|
| | Obtain a Certificate | 80 |
| | Import Certificates | 81 |
| | Example Of TrustedCA.pem File | 82 |
| | Example of Portal.pem File | 83 |
| 12 | MANAGE JUNIPER NETWORKS NSM PROFILER SCANNERS | |
| | Add a Juniper Networks NSM Profiler Scanner | 85 |
| | Edit a Juniper Networks NSM Profiler Scanner | 86 |
| | Delete a Juniper Networks NSM Profiler Scanner | 87 |
| 13 | MANAGE RAPID7 NEXPOSE SCANNERS | |
| | Import Rapid7 NeXpose Vulnerability Data Using the API | 89 |
| | Configure a Rapid7 NeXpose Scanner | 90 |
| | Troubleshoot a Rapid7 NeXpose API Scan Import | 91 |
| | Import Rapid7 NeXpose Vulnerabilities from a Local File | 92 |
| | Edit a Rapid7 NeXpose Scanner | 93 |
| | Delete a Rapid7 NeXpose Scanner | 94 |
| 14 | MANAGE NETVIGILANCE SECURESCOUT SCANNERS | |
| | Add a SecureScout Scanner | 96 |
| | Edit a SecureScout Scanner | 97 |
| | Delete a SecureScout Scanner | 97 |
| 15 | MANAGE EYE SCANNERS | |
| | Add an eEye Scanner | 99 |
| | Install the Java Cryptography Extension | 103 |
| | Edit an eEye Scanner | 103 |
| | Delete an eEye Scanner | 104 |
| 16 | MANAGE PATCHLINK SCANNERS | |
| | Add a PatchLink Scanner | 105 |
| | Edit a PatchLink Scanner | 107 |
| | Delete a PatchLink Scanner | 107 |
| 17 | MANAGE MCAFEE VULNERABILITY MANAGER SCANNERS | |
| | Add a McAfee Vulnerability Manager Scanner | 110 |
| | Configure a Remote XML Import | 110 |
| | Configure a OpenAPI Scan | 112 |
| | Edit a McAfee Vulnerability Manager Scanner | 114 |
| | Delete a McAfee Vulnerability Manager Scanner | 115 |
| | Configure Certificates | 115 |
| | Generate Certificates | 115 |
| | Process Certificates | 116 |
| | Import Certificates | 117 |

| | | |
|-----------|---|-----|
| 18 | MANAGE SAINT SCANNERS | |
| | Configure a SAINTwriter Report Template | 119 |
| | Add a SAINT Scanner | 120 |
| | Edit a SAINT Scanner | 122 |
| | Delete a SAINT Scanner | 123 |
| 19 | MANAGE AXIS SCANNERS | |
| | Add an AXIS Scanner | 125 |
| | Edit an AXIS Scanner | 127 |
| | Delete an AXIS Scanner | 128 |
| 20 | MANAGE TENABLE SECURITYCENTER SCANNERS | |
| | Add a Tenable SecurityCenter Scanner | 129 |
| | Edit a Tenable SecurityCenter Scanner | 130 |
| | Delete a Tenable SecurityCenter Scanner | 131 |
| | Install the Java Cryptography Extension | 131 |
| 21 | MANAGE SCAN SCHEDULES | |
| | View Scheduled Scans | 133 |
| | Schedule a Scan | 136 |
| | Edit a Scan Schedule | 138 |
| | Delete a Scan Schedule | 138 |
| 22 | SUPPORTED SCANNERS | |

INDEX

ABOUT THIS GUIDE

The Managing Vulnerability Assessment guide provides you with information on managing vulnerability scanners and configuring scan schedules to work with STRM.




Audience

This guide is intended for the system administrator responsible for setting up STRM Installation in your network. This guide assumes that you have STRM administrative access and a knowledge of your corporate network and networking technologies.

Documentation 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. |

Technical Documentation

You can access technical documentation, technical notes, and release notes directly from the Juniper Customer Support website at <https://www.juniper.net/support/>. Once you access the Juniper Customer Support website, locate the product and software release for which you require documentation.

Your comments are important to us. Please send your e-mail comments about this guide or any of the Juniper Networks documentation to:

techpubs-comments@juniper.net.

Include the following information with your comments:

- Document title
- Page number

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 STRM to build vulnerability assessment profiles.

Vulnerability assessment profiles use correlated event data, network activity, and behavioral changes to determine the threat level and vulnerabilities present on critical business assets in your network.

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

You must have the proper permissions to access networks containing CIDR addresses you schedule for vulnerability assessment scans.

Information found in this documentation about configuring scanners is based on the latest RPM files located at www.juniper.net/support/.

Configure Vulnerability Assessment

To configure vulnerability assessment scans in STRM, you must:

- 1 Install the scanner RPM, if necessary.
For more information, see [Manually Install a Scanner](#).
- 2 Configure your scanner using the following list of supported scanners:
 - [Manage IBM Security AppScan Enterprise Scanners](#)
 - [Manage nCircle IP360 Scanners](#)
 - [Manage Nessus Scanners](#)
 - [Manage Nmap Scanners](#)
 - [Manage Qualys Scanners](#)
 - [Manage FoundScan Scanners](#)
 - [Manage Juniper Networks NSM Profiler Scanners](#)
 - [Manage Rapid7 NeXpose Scanners](#)

- [Manage netVigilance SecureScout Scanners](#)
- [Manage eEye Scanners](#)
- [Manage PatchLink Scanners](#)
- [Manage McAfee Vulnerability Manager Scanners](#)
- [Manage SAINT Scanners](#)
- [Manage AXIS Scanners](#)
- [Manage Tenable SecurityCenter 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.

If you add, edit, or delete a scanner, you must click **Deploy Changes** on the **Admin** tab for the changes to be updated. Configuration changes do not interrupt scanners with scans in progress, as changes are applied when the scan completes.

- 3 Schedule a vulnerability scan to import the data in to STRM. For more information, see [Manage Scan Schedules](#).

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.

Manually Install a Scanner

To update or install a new scanner, you must either configure STRM to automatically download and install scanner rpm files using the Auto Updates icon on the **Admin** tab or install the scanner rpm manually.

If you choose to install a scanner update manually, the latest rpm installation file for your scanner is available on the Juniper customer support website or from www.juniper.net/support/.

To manually install a scanner:

- Step 1** Download the scanner rpm file from the following website:
www.juniper.net/support/
- Step 2** Copy the file to your STRM.
- Step 3** Using SSH, log in to your STRM as a root user.
Username: `root`
Password: `<password>`
- Step 4** Navigate to the directory that includes the downloaded file.

Step 5 Type the following command:

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

Where <filename> is the name of the downloaded file.

For example: `rpm -Uvh VIS-nCircleIP360 -7.0-148178.rpm`

Step 6 Log in to STRM.

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

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

Step 7 Click the **Admin** tab.

The Administration tab is displayed.

Step 8 On the **Admin** tab, click **Deploy Changes**.

View Configured Scanners

To view currently configured scanners:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

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

Table 1-1 Scanner Parameters

| Parameter | Description |
|----------------------|---|
| Name | Displays the name of the scanner. |
| Type | Displays the type of scanner, for example, Nessus Scan Results Importer. |
| Host | Displays the IP address or host name of the host on which the scanner operates. |
| Approved CIDR ranges | Displays the CIDR range you want this scanner to consider. Multiple CIDR ranges are displayed using a comma separated list. |
| Description | Displays a description for this scanner. |
| Status | Displays the status of the scanner schedule. Note: When the status of a scheduled scan changes, the status field in the list of installed scanners updates, see Table 21-1 for more information on scan status. |

2

MANAGE BEYOND SECURITY AVDS SCANNERS

The Beyond Security Automated Vulnerability Detection System (AVDS) appliance uses the Asset Export Information Source (AXIS) XML file format to collect vulnerabilities for STRM.

To successfully integrate a Beyond Security AVDS vulnerabilities with STRM, you must configure your Beyond Security ADVS appliance to publish vulnerability data to an AXIS formatted XML results file. The XML vulnerability data must be published to a remote server that is accessible to STRM using SFTP. The term remote server refers to a system or 3rd party appliance or network storage location, reachable using SFTP that can host the published XML scan results.

The most recent XML results containing Beyond Security AVDS vulnerabilities are imported to STRM when a scan schedule is launched by STRM. Scan schedules allow you to determine the frequency with which STRM requests data from an AXIS-compatible scanner, such as Beyond Security AVDS. After you add your Beyond Security AVDS appliance to STRM, you can then add a scan schedule to retrieve your vulnerability information. Vulnerabilities for assets in your network are displayed on the **Assets** tab of STRM.

Add a Beyond Security AVDS Scanner

To add an Beyond Security AVDS scanner to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:**Table 2-1** Beyond Security AVDS Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Beyond Security AVDS Scanner . |

Step 6 Configure values for the following parameters:**Table 2-2** Beyond Security AVDS Scanner Parameters

| Parameter | Description |
|--------------------------|---|
| Remote Hostname | Type the hostname or IP address of the remote server. |
| Login Username | Type the username used by STRM to authenticate the connection. |
| Enable Key Authorization | <p>Select this check box to enable private key authorization for the server.</p> <p>If the check box is selected, the authentication is completed using a private key and the password is ignored. The default value is disabled. Selecting this option enables the Private Key File field in the scanner configuration.</p> |
| Login Password | <p>If Enable Key Authentication is disabled, you must type the password corresponding to the Login Username parameter that STRM uses to authenticate the connection.</p> <p>If Enable Key Authentication is enabled, the Login Password parameter is ignored.</p> |
| Remote Directory | Type the directory location of the scan result files. |
| File Name Pattern | <p>Type a regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing.</p> <p>For example, if you want to list all files ending with XML, use the following entry:</p> <p><code>. * \ . xml</code></p> <p>Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/</p> |

Table 2-2 Beyond Security AVDS Scanner Parameters (continued)

| Parameter | Description |
|-----------------------|---|
| Private Key File | <p>Type the directory path to the file that contains the private key information. If you are using key-based authentication, STRM uses the private key to authenticate the 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 type another file name.</p> <p>This parameter is mandatory if the Enable Key Authentication check box is selected. If the Enable Key Authentication check box is clear, this parameter is ignored.</p> |
| Max Report Age (Days) | <p>Type the maximum file age to include when importing your XML vulnerabilities file during a scheduled scan. By default, the value is 7 days.</p> <p>Files that are older than the specified days and timestamp on the report file are excluded from the scheduled import.</p> |
| Ignore Duplicates | <p>Select this check box to track files that have already been processed and you do not want the files to be processed a second time.</p> <p>Note: If a result file is not seen for 10 days, it is removed from the tracking list and is processed the next time the file is discovered.</p> |

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- a** In the text field, type 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** On the **Admin** tab, click **Deploy Changes**.

Edit a Beyond Security AVDS Scanner

To edit the configuration of your Beyond Security ADVS scanner:

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

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete a Beyond Security AVDS Scanner

To delete a Beyond Security ADVS scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

3

MANAGE IBM SECURITY APPSCAN ENTERPRISE SCANNERS

STRM can import scan results from IBM Security AppScan® Enterprise report data, providing you a centralized security environment for advanced application scanning and security compliance reporting.

Importing IBM Security AppScan Enterprise scan results allows you to collect asset vulnerability information for malware, web applications, and web services in your deployment. STRM retrieves AppScan Enterprise reports using the Representational State Transfer (REST) web service to import vulnerability data and generate offenses in STRM for your security team.

To integrate AppScan Enterprise with STRM, you must:

- 1 Generate scan reports in AppScan Enterprise. For more information on generating scan reports, see your AppScan Enterprise vendor documentation.
- 2 Configure AppScan Enterprise to grant STRM access to report data.
- 3 Configure your AppScan Enterprise scanner in STRM.
- 4 Create a schedule in STRM to import AppScan Enterprise results.

Configure AppScan Enterprise

A member of the security team or your AppScan Enterprise administrator must determine which AppScan Enterprise users have permissions to publish reports to STRM.

After AppScan Enterprise users have been configured, the reports generated by AppScan Enterprise can be published to STRM, making them available for download.

To configure AppScan Enterprise to grant STRM access to scan reports:

- 1 Create a custom user type.
- 2 Enable AppScan Enterprise and STRM integration.
- 3 Create an Application Deployment Map.
- 4 Publish your scan results to STRM.

Create a Custom User Type Custom user types allow administrators to perform limited and specific administrative tasks and must be created before you can assign permissions.

To create a custom user type:

- Step 1** Log in to IBM Security AppScan Enterprise.
- Step 2** Click the **Administration** tab.
- Step 3** On the User Types page, click **Create**.
- Step 4** Create the user type, and select any the following custom user permissions for the user type:
 - **Configure STRM Integration** - Select this check box to allow users to access the STRM integration options for AppScan Enterprise.
 - **Publish to STRM** - Select this check box to allow STRM access to published scan report data.
 - **STRM Service Account** - Select this check box to configure permission on the account to use the REST API. It does not access the user interface.
- Step 5** Save the user type.

You are now ready to enable STRM integration with AppScan Enterprise.

Enable STRM Integration To complete these steps, you must be logged in as a user with the Configuration STRM Integration user type enabled.

To enable AppScan Enterprise with STRM:

- Step 1** Click the **Administration** tab.
- Step 2** On the navigation menu, select **Network Security Systems**.
- Step 3** From the STRM Integration Settings pane, click **Edit**.
The STRM Integration Settings configuration is displayed.
- Step 4** Select the **Enable STRM Integration** check box.

Any reports previously published to STRM are displayed. If any of the reports displayed are no longer required, you can remove them from the list. As you publish additional reports to STRM, the reports are displayed in this list.

You are now ready to configure the Application Deployment Mapping in AppScan Enterprise.

Create an Application Deployment Map The Application Deployment Map allows AppScan Enterprise to determine the locations hosting the application in your production environment.

As vulnerabilities are discovered, AppScan Enterprise knows the locations of the hosts and the IP addresses affected by the vulnerability. If an application is deployed to several hosts, then AppScan Enterprise generates a vulnerability for each host in the scan results.

To create an Application Deployment Map:

- Step 1** Click the **Administration** tab.
- Step 2** On the navigation menu, click **Network Security Systems**.
- Step 3** On the Application Deployment Mapping pane, click **Edit**.
The Application Deployment Mapping configuration is displayed.
- Step 4** In the **Application test location (host or pattern)** field, type the test location for your application.
- Step 5** In the **Application production location (host)** field, type the IP address for your production environment.

To add vulnerability information to STRM, your Application Deployment Mapping must include an IP address. Any vulnerability data without an IP address is excluded from STRM if the IP address is not available in the AppScan Enterprise scan results.

- Step 6** Click **Add**.
- Step 7** Repeat [Step 3](#) to [Step 6](#) to map all of your production environments in AppScan Enterprise.
- Step 8** Click **Done** to save your configuration changes.

You are now ready to publish completed reports to STRM.

Publish Reports to STRM Completed vulnerability reports generated by AppScan Enterprise must be made accessible to STRM by publishing the report.

To complete these steps, you must be logged in as a user with the Publish to STRM user type enabled.

To publish a vulnerability report in AppScan Enterprise:

- Step 1** Click the **Jobs & Reports** tab.
- Step 2** Navigate to the security report you want to make available to STRM.
- Step 3** On the menu bar of any security report, select **Publish > Grant report access to STRM**.

You are now ready to add your AppScan Enterprise scanner to STRM.

Configure a Scanner in STRM

After you have configured AppScan Enterprise and published reports, you can add the AppScan Enterprise scanner in STRM.

Adding a scanner allows STRM to know which scan reports to collect. You can add multiple AppScan Enterprise scanners in STRM, each with a different configuration. Adding multiple configurations for a single AppScan Enterprise scanner allows you to create individual scanners for specific result data. The scan schedule you configure in STRM allows you to determine the frequency with which STRM imports the scan result data from AppScan Enterprise using the REST web service.

Your scan result data must include the IP address of the host from the Application Deployment Mapping. Any vulnerability data without an IP address is excluded from STRM if the IP address is not available in the AppScan Enterprise scan results.

This section includes the following topics:

- [Add an AppScan Enterprise Scanner](#)
- [Edit an AppScan Enterprise Scanner](#)
- [Delete an AppScan Enterprise Scanner](#)

Add an AppScan Enterprise Scanner

To add an AppScan Enterprise scanner to :

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 3-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |

Table 3-1 Scanner Parameters (continued)

| Parameter | Description |
|-----------|--|
| Type | From the list box, select IBM AppScan Scanner . |

The list of fields for the selected scanner type is displayed.

Step 6 Configure values for the following parameters:

Table 3-2 IBM AppScan Enterprise Parameters

| Parameter | Description |
|-----------------------|---|
| ASE Instance Base URL | Type the full base URL of the AppScan Enterprise instance. This field supports URLs for HTTP and HTTPS addresses. For example, <code>http://myasehostname/ase/</code> . |
| Authentication Type | Select an Authentication Type: <ul style="list-style-type: none"> • Windows Authentication - Select this option to use Windows Authentication when using the REST web service to retrieve scan report data from AppScan Enterprise. • Jazz™ Authentication - Select this option to use Jazz Authentication when using the REST web service to retrieve scan report data for AppScan Enterprise. |
| Username | Type the username required to retrieve scan results from AppScan Enterprise. |
| Password | Type the password required to retrieve scan results from AppScan Enterprise. |
| Report Name Pattern | Type a regular expression (regex) required to filter the list vulnerability reports available from AppScan Enterprise. All matching files are included and processed by STRM. You can specify a group of vulnerability reports or an individual report using a regex pattern. By default, the Report Name Pattern field contains <code>. *</code> as the regex pattern. The <code>. *</code> pattern imports all scan reports that are published to STRM. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/ . |

Step 7 To configure the CIDR ranges you want this scanner to consider:

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

The CIDR range allows you to filter the list of IP addresses the scanner considers when retrieving scan results from AppScan Enterprise devices. Since you can configure and schedule multiple AppScan Enterprise scanners in STRM, the CIDR range acts as a filter when searching the network for scan result data. To collect all results within AppScan Enterprise published reports, you can use a CIDR range of 0.0.0.0/0.

- b Click **Add**.

Step 8 Click **Save**.

Step 9 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule in STRM. For more information, see [Manage Scan Schedules](#).

Edit an AppScan Enterprise Scanner

To edit an AppScan Enterprise scanner:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary. See [Table 3-2](#).

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete an AppScan Enterprise Scanner

To delete an AppScan Enterprise scanner:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

4

MANAGE IBM GUARDIUM SCANNERS

IBM InfoSphere™ Guardium® appliances are capable of exporting database vulnerability information that can be critical to protecting customer data.

IBM Guardium audit processes export the results of tests that fail the Common Vulnerability and Exposures (CVE) tests generated when running security assessment tests on your IBM Guardium appliance. The vulnerability data from IBM Guardium must be exported to a remote server or staging server in Security Content Automation Protocol (SCAP) format. STRM can then retrieve the scan results from the remote server storing the vulnerability using SFTP.

IBM Guardium only exports vulnerability from databases containing failed CVE test results. If there are no failed CVE tests, IBM Guardium may not export a file at the end of the security assessment.

For information on configuring security assessment tests and creating an audit process to export vulnerability data in SCAP format, see your IBM InfoSphere Guardium documentation.

After you have configured your IBM Guardium appliance, you are ready to configure STRM to import the results from the remote server hosting the vulnerability data. You must add an IBM Guardium scanner to STRM and configure the scanner to retrieve data from your remote server. The most recent vulnerabilities are imported by STRM when you create a scan schedule. Scan schedules allow you to determine the frequency with which STRM requests data from the remote server host your IBM Guardium vulnerability data. For more information, see [Manage Scan Schedules](#).

Add an IBM Guardium Scanner

To add an IBM Guardium scanner to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.

Step 4 Click **Add**.

The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:**Table 4-1** IBM Guardium SCAP Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select IBM Guardium SCAP Scanner . |

Step 6 Configure values for the following parameters:**Table 4-2** IBM Guardium SCAP Scanner Parameters

| Parameter | Description |
|--------------------------|---|
| Remote Hostname | Type the hostname or IP address of the remote server hosting your SCAP XML files. |
| Remote Port | Type the number of the port on the remote server to retrieve scan result files using SFTP. The default is port 22. |
| Login Username | Type the username used by STRM to authenticate the SFTP connection. |
| Login Password | <p>If Enable Key Authentication is disabled, you must type the password corresponding to the Login Username parameter that STRM uses to authenticate the SFTP connection.</p> <p>If Enable Key Authentication is enabled, the Login Password parameter is ignored.</p> |
| Enable Key Authorization | <p>Select this check box to enable private key authorization for the server.</p> <p>If the check box is selected, the authentication is completed using a private key and the password is ignored. The default value is disabled.</p> |
| Private Key File | <p>Type the directory path to the file that contains the private key information. If you are using key-based authentication, STRM uses the private key to authenticate the connection.</p> <p>This parameter is mandatory if the Enable Key Authentication check box is selected. If the Enable Key Authentication check box is clear, this parameter is ignored.</p> |
| Remote Directory | Type the directory location of the scan result files on the remote server hosting your IBM Guardium vulnerabilities. |

Table 4-2 IBM Guardium SCAP Scanner Parameters (continued)

| Parameter | Description |
|-----------------------|---|
| File Name Pattern | <p>Type a regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing.</p> <p>For example, if you want to list all files ending with XML, use the following entry:</p> <p><code>. * \ . xml</code></p> <p>Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/</p> |
| Max Report Age (Days) | <p>Type the maximum file age to include when importing your XML result file during a scheduled scan.</p> <p>Files that are older than the specified days and timestamp on the report file are excluded from the scheduled import.</p> |

Step 7 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 On the **Admin** tab, click **Deploy Changes**.

Edit an IBM Guardium Scanner

To edit an IBM Guardium scanner:

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

Delete an IBM Guardium Scanner

To delete an IBM Guardium scanner from STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window is displayed.
- Step 6** Click **OK**.
- Step 7** On the **Admin tab**, click **Deploy Changes**.

5

MANAGE IBM SITEPROTECTOR SCANNERS

The IBM SiteProtector® scanner module for STRM accesses vulnerability data from IBM SiteProtector scanners using the JDBC.

The IBM SiteProtector scanner retrieves data from the RealSecureDB table and polls for available vulnerability information. The compare field allows STRM to retrieve only the latest information from the RealSecureDB table and import any new vulnerabilities to STRM.

When you configure your IBM SiteProtector, we recommend that you create a SiteProtector user account specifically for STRM. Creating a user account ensures that STRM has the credentials required to poll the IBM SiteProtector database to retrieve vulnerability data. After you create a user account for STRM, you should verify communication between STRM and your IBM SiteProtector system to ensure there are no firewalls blocking communication on the port you are using to poll the RealSecureDB.

Add an IBM SiteProtector Scanner

You can add multiple IBM SiteProtector scanners in STRM, each with a different configuration to determine which CIDR ranges you want the scanner to consider.

Adding multiple configurations for a single IBM SiteProtector scanner allows you to create individual scanners for collecting specific result data from specific locations. After you add and configure the IBM SiteProtector scanner in STRM, you can create a scan schedule to determine the frequency with which STRM polls the IBM SiteProtector database.

To add an IBM SiteProtector scanner in STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:**Table 5-1** Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select IBM SiteProtector Scanner . |

The list of fields for the selected scanner type is displayed.

Step 6 Configure values for the following parameters:**Table 5-2** IBM SiteProtector Scanner Parameters

| Parameter | Description |
|---------------|--|
| Hostname | Type the IP address or hostname of the IBM SiteProtector containing the vulnerabilities you want to add to STRM. |
| Port | <p>Type the port number used by the database server. The default that is displayed depends on the selected Database Type. The valid range is 0 to 65536. The default for MSDE is port 1433.</p> <p>The JDBC configuration port must match the listener port of the database. The database must have incoming TCP connections enabled to communicate with STRM.</p> <p>The default port number for all options include:</p> <ul style="list-style-type: none"> • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Oracle - 1521 • Sybase - 1521 |
| Username | Type the username required to access IBM SiteProtector. |
| Password | Type the password required to access IBM SiteProtector. |
| Domain | <p>Type the domain required, if required, to connect to your IBM SiteProtector database.</p> <p>If you select MSDE as the database type and the database is configured for Windows, you must define a Windows domain. Otherwise, leave this field blank.</p> <p>The domain can be up to 255 alphanumeric characters in length. The domain can include the following special characters: underscore (_), en dash (-), and period(.).</p> |
| Database Name | Type the name of the database to which you want to connect. The default database name is RealSecureDB . |

Table 5-2 IBM SiteProtector Scanner Parameters (continued)

| Parameter | Description |
|------------------------------|---|
| Database Instance | Type the database instance for your IBM SiteProtector database. If you are not using a database instance, you can leave this field blank. If you select MSDE as the Database Type and you have multiple SQL server instances on one server, define the instance to which you want to connect. |
| Use Named Pipe Communication | Select this check box to use named pipes when communicating to the IBM SiteProtector database. By default, this check box is clear. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Selecting this check box uses the default Named Pipe for your system. |
| Use NTLMv2 | Select this check box if your IBM SiteProtector uses NTLMv2 as an authentication protocol. By default, this check box is clear. The Use NTLMv2 check box forces MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. If the Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication. |

Step 7 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select the CIDR range from the network list. To collect all available IBM SiteProtector vulnerabilities, you can type 0.0.0.0/0 as the CIDR address.
- b Click **Add**.

Step 8 Click **Save**.

Step 9 On the **Admin** tab, click **Deploy Changes**.

Edit an IBM SiteProtector Scanner

To edit a scanner configured in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

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

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete an IBM SiteProtector Scanner

To delete a scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

6

IBM TIVOLI ENDPOINT MANAGER SCANNER

The IBM Tivoli® Endpoint Manager scanner module accesses vulnerability data from IBM Tivoli Endpoint Manager using the SOAP API installed with the Web Reports application.

The Web Reports application for Tivoli Endpoint Manager is required to retrieve vulnerability data from Tivoli Endpoint Manager for STRM. We recommend that you create a user in IBM Tivoli Endpoint Manager for STRM.

STRM is compatible with IBM Tivoli Endpoint Manager versions 8.2.x. However, we recommend that you update and use the latest version of IBM Tivoli Endpoint Manager that is available.

Add an IBM Tivoli Endpoint Manager Scanner

You can add multiple IBM Tivoli Endpoint Manager scanners in STRM, each with a different configuration to determine which CIDR ranges you want the scanner to consider.

Adding multiple configurations for a single IBM Tivoli Endpoint Manager scanner allows you to create individual scanners for collecting specific result data from specific locations. After you add and configure the IBM Tivoli Endpoint Manager in STRM, you can create a scan schedule to determine the frequency with which STRM accesses IBM Tivoli Access Manager. This allows you to schedule how often STRM requests data from IBM Tivoli Endpoint Manager using the SOAP API.

To add an IBM Tivoli Endpoint Manager scanner in STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 6-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select IBM Tivoli Endpoint Manager . |

The list of fields for the selected scanner type is displayed.

Step 6 Configure values for the following parameters:

Table 6-2 IP360 Parameters

| Parameter | Description |
|-----------|---|
| Hostname | Type the IP address or hostname of the IBM Tivoli Endpoint Manager containing the vulnerabilities you want to add to STRM. |
| Port | Type the port number used to connect to the IBM Tivoli Endpoint Manager using the SOAP API. By default, port 80 is the port number for communicating with IBM Tivoli Endpoint Manager. If you are use HTTPS, you must update this field to the HTTPS port number for your network. Most configurations use port 443 for HTTPS communications. |
| Use HTTPS | Select this check box to connect using HTTPS. If you select this check box, the hostname or IP address you specify uses HTTPS to connect to your IBM Tivoli Endpoint Manager. If a certificate is required to connect using HTTPS, you must copy any certificates required by the STRM Console or managed host to the following directory: <code>/opt/qradar/conf/trusted_certificates</code> Note: STRM support certificates with the following file extensions: .crt, .cert, or .der. Any required certificates should be copied to the trusted certificates directory before you save and deploy your changes. |
| Username | Type the username required to access IBM Tivoli Endpoint Manager. |
| Password | Type the password required to access IBM Tivoli Endpoint Manager. |

Step 7 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 On the **Admin** tab, click **Deploy Changes**.

Edit an IBM Tivoli Endpoint Manager Scanner

To edit a scanner configured in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

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

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete an IBM Tivoli Endpoint Manager Scanner

To delete a scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

7

MANAGE NCIRCLE IP360 SCANNERS

STRM uses SSH to access the remote server (SSH export server) to retrieve and interpret the scanned data.

STRM supports VnE Manager version IP360-6.5.2 to 6.8.2.8.

You can configure an nCircle IP360 scanner device to export scan results to a remote server. These scan results are exported, in XML2 format, to an SSH server. To successfully integrate an IP360 device with STRM, these XML2 format files must be read from the remote server (using SSH). STRM can be configured to schedule a scan or poll the SSH server for updates to the scan results and import the latest results for processing. 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 about exporting scan results, see [Export nCircle Scan Reports](#).

The scan results contain identification information about the scan configuration from which it was produced. The most recent scan results are used when a scan is imported by STRM. STRM only supports exported scan results from the IP360 scanner in XML2 format.

Add an nCircle IP360 Scanner

To add an nCircle IP360 scanner to :

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 7-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select nCircle IP360 Scanner . |

The list of fields for the selected scanner type is displayed.

Step 6 Configure values for the following parameters:

Table 7-2 IP360 Parameters

| Parameter | Description |
|--------------------------|---|
| SSH Server Host Name | Type the IP address or host name to the remote server hosting the scan result files. We recommend a UNIX-based system with SSH enabled. |
| SSH Username | Type the SSH remote server username. |
| SSH Password | Type the password to the remote server corresponding to the SSH Username. If the Enable Key Authentication check box is selected, the password is ignored. |
| SSH Port | Type the port number used to connect to the remote server. |
| Remote Directory | Type the directory location of the scan result files. |
| File Max Age (days) | Type the maximum file age to include when performing a scheduled scan. Files that are older than a specified time are excluded from the import of the result data in STRM. |
| File Pattern | Type a regular expression (regex) required to filter the list of files specified in the Remote Directory field. All matching files are included and processed. For example, if you want to list all XML2 format files ending with XML, use the following entry: XML2.*\.*.xml Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/ |
| Enable Key Authorization | Select this check box to enable key authorization for the server. If the Enable Key Authentication check box is selected, the SSH authentication is completed using a private key and the password is ignored. The default value is disabled. |

Table 7-2 IP360 Parameters (continued)

| Parameter | Description |
|------------------|---|
| Private Key Path | <p>Type the private key path.</p> <p>The private key path is the full directory path on your STRM where the private key to be used for SSH key-based authentication is stored. The default path is <code>/opt/qradar/conf/vis.ssh.key</code>, but this file does not exist. You must create a <code>vis.ssh.key</code> file for your remote host or type another file name.</p> <p>If the Enable Key Authentication check box is clear, the Private Key Path is ignored.</p> |

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 fails. Make sure the following line is displayed 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 can differ. For more information, see the vendor documentation for your scanner.

Step 7 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 On the **Admin** tab, click **Deploy Changes**.

Edit an nCircle IP360 Scanner

To edit a scanner configured in STRM:

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

Delete an nCircle IP360 Scanner

To delete a scanner from STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window is displayed.
- Step 6** Click **OK**.
- Step 7** On the **Admin** tab, click **Deploy Changes**.

Export nCircle 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- hand navigation, select **Administer > System > VNE Manager > Automated Export**.
The Automated Export menu is displayed.
- 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 XML format.
- Step 5** Record the Target settings displayed in the user interface. These settings are necessary to configure STRM to integrate with your nCircle device.

8

MANAGE NESSUS SCANNERS

STRM can retrieve vulnerability scan reports about your network assets by leveraging the Nessus client and server relationship or by using the Nessus XMLRPC API to access scan data directly.

When you configure your Nessus client, we recommend that you create a Nessus user account for STRM. Creating a user account ensures that STRM has the credentials required to log in using SSH and communicate with the Nessus server to retrieve scan report data using either the client server relationship or using the XMLRPC API. After you create a user account for STRM, you should attempt to SSH from STRM to your Nessus client to verify STRM's credentials. This ensures that STRM and the Nessus client can communicate before you attempt to collect scan data or start a live scan.

The following data collection options are available for Nessus:

- **Scheduled Live Scan** - Allows STRM to connect to a Nessus client and launch a pre-configured scan. STRM uses SSH to retrieve the scan report data from the client's temporary results directory after the live scan completes.
- **Scheduled Results Import** - Allows STRM to connect to the location hosting your Nessus scan reports. STRM connects to the repository using SSH and imports completed scan report files from the remote directory. STRM supports importing Nessus scan reports or scan reports in a Nessus supported output format.
- **Scheduled Live Scan - XMLRPC API** - Allows STRM to use the XMLRPC API to start a pre-configured scan. To start a live scan from STRM, you must specify the policy name for the live scan data you want to retrieve. As the live scan runs, STRM updates the percentage complete in the scan status. After the live scan completes, STRM retrieves the data and updates the vulnerability assessment information for your assets.
- **Scheduled Completed Report Import - XMLRPC API** - Allows STRM to connect to your Nessus server and download data from any completed reports that match the report name and report age filters.

Nessus vulnerability data can be integrated into STRM by adding a Nessus scanner using the VA Scanners icon in the **Admin** tab. After you add your Nessus client, you can add a scan schedule to retrieve Nessus vulnerability data on a one-time or repeating interval. For more information on scheduling a scan, see [Schedule a Scan](#).

We recommend that you do not install your Nessus software on a critical system due to the high CPU requirements.

Add a Nessus Scanner

The Nessus scanner module for STRM provides several collection types for retrieving vulnerability data from your Nessus server.

This section includes the following topics:

- [Add a Nessus Scheduled Live Scan](#)
- [Add a Nessus Scheduled Results Import](#)
- [Add a Nessus Scheduled Live Scan Using the XMLRPC API](#)
- [Add a Nessus Completed Report Import Using the XMLRPC API](#)

The Nessus XMLRPC API is only available on Nessus servers and clients using software v4.2 and above.

Add a Nessus Scheduled Live Scan

A live scan allows you to start a live scan on your Nessus server and import the result data from a temporary directory containing the live scan report data.

After the scan is complete, STRM downloads the scan data from the temporary directory and updates the vulnerability information for your assets.

To add a Nessus live scan in STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 8-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |

Table 8-1 Scanner Parameters (continued)

| Parameter | Description |
|--------------|---|
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Nessus Scanner . |

The list of parameters for the selected scanner type is displayed.

Step 6 From the **Collection Type** list box, select **Scheduled Live Scan**.

Step 7 Configure values for the following parameters:

Table 8-2 Nessus Scheduled Live Scan Parameters

| Parameter | Description |
|---------------------------|--|
| Server Hostname | Type the IP address or hostname of the Nessus server as seen by the Nessus client. If the server process and the client are located on the same host, you can use localhost as the server hostname. |
| Server Port | Type the port for the Nessus server. The default is port 1241. |
| Server Username | Type the Nessus username that the Nessus client uses to authenticate with the Nessus server. |
| Server Password | Type the Nessus password that corresponds to the username. Note: Your Nessus server password must not contain the ! character. This character could cause authentication failures over SSH. |
| Client Temp Dir | Type the directory path of the Nessus client that STRM can use to store temporary files. STRM uses the temporary directory of the Nessus client as a read and write location to upload scan targets and read scan results. Temporary files are removed when STRM completes the scan and retrieves the scan reports from the Nessus client. The default directory path on the Nessus client is /tmp. |
| Nessus Executable | Type the directory path to the Nessus executable file on the server hosting the Nessus client. By default, the directory path for the executable file is /usr/bin/nessus . |
| Nessus Configuration File | Type the directory path to the Nessus configuration file on the Nessus client. |
| Client Hostname | Type the hostname or IP address of the system hosting the Nessus client. |
| Client SSH Port | Type the number of the SSH port on the Nessus server that can be used to retrieve scan result files. The default is port 22. |
| Client Username | Type the username used by STRM to authenticate the SSH connection. |

Table 8-2 Nessus Scheduled Live Scan Parameters (continued)

| Parameter | Description |
|---------------------------|---|
| Client Password | <p>Type the password that corresponds to the Client Username field. This field is required if the Enable Key Authentication check box is clear.</p> <p>If Enable Key Authentication is enabled, the Login Password parameter is ignored.</p> <p>Note: <i>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 fails. Ensure the following line is displayed in your sshd_config file, which is typically found in the /etc/ssh directory on the SSH server: <code>PasswordAuthentication yes</code>. If your scanner server does not use OpenSSH, the configuration can differ. For more information, see the vendor documentation for your scanner.</i></p> |
| Enable Key Authentication | <p>Select this check box to enable public or private key authentication.</p> <p>If the check box is selected, STRM attempts to authenticate the SSH connection using the private key that is provided and the SSH Password field is ignored.</p> |

Step 8 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

Step 11 After the changes are deployed, you must create a scan schedule for the live scan.

Scan reports can be created as a one-time event or as a reoccurring scheduled import. For more information on scheduling a scan, see [Schedule a Scan](#).

Add a Nessus Scheduled Results Import

A scheduled results import retrieves completed Nessus scan reports from an external location.

The external location can be a Nessus server or a file repository that contains a completed scan report. STRM connects to the location of your scan reports using SSH and imports completed scan report files from the remote directory using a regular expression or maximum report age to filter for your scan reports. STRM supports importing Nessus scan reports (.Nessus) or scan reports exported to a Nessus supported output format, such as XML.

To add a Nessus scheduled result import in STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 8-3 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Nessus Scanner . |

The list of parameters for the selected scanner type is displayed.

- Step 6** From the **Collection Type** list box, select **Scheduled Results Import**.
- Step 7** Configure values for the following parameters:

Table 8-4 Nessus Scheduled Results Import Parameters

| Parameter | Description |
|---------------------------|--|
| Remote Results Hostname | Type the IP address or hostname of the Nessus client or server hosting your Nessus or XML scan result files. |
| Remote Results SSH Port | Type the number of the SSH port on the Nessus server that can be used to retrieve scan result files. The default port is 22. |
| SSH Username | Type a username that STRM can use to authenticate the SSH session with the Nessus server. |
| SSH Password | Type the password that corresponds to the SSH username. Note: Your Nessus server password must not contain the ! character. This character could cause authentication failures over SSH. |
| Enable Key Authentication | Select this check box to enable public or private key authentication. If the check box is selected, STRM attempts to authenticate the SSH connection using the private key provided and the SSH Password field is ignored. |

Table 8-4 Nessus Scheduled Results Import Parameters (continued)

| Parameter | Description |
|-----------------------------|--|
| Remote Results Directory | Type the full path for the directory containing the Nessus scan report files on the Nessus client. The directory path uses <code>./</code> as the default value. |
| Remote Results File Pattern | Type a file pattern, using a regular expression (regex), for the scan result files you are attempting to import. By default, the following file pattern is included for Nessus files: <code>**.nessus</code> . If you use an output mask to export your scan report in another supported Nessus format, such as XML, you must update the regex for the file pattern accordingly. Note: If you update the regex in the Remote Results File Pattern field, you must deploy the change to update your scanner configuration. |
| Results File Max Age (Days) | Type the maximum file age to include when importing Nessus scan result files during a scheduled scan. By default, the results file maximum age is 7 days. Files that are older than the specified days and the timestamp on the results file are excluded from the result file import. |

Step 8 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

Step 11 After the changes are deployed, you must create a scan schedule to import the vulnerability data.

Scan reports can be created as a one-time event or as a reoccurring scheduled import. For more information on scheduling a scan, see [Schedule a Scan](#).

Add a Nessus Scheduled Live Scan Using the XMLRPC API

The XMLRPC API allows STRM to start a pre-configured live scan on your Nessus server.

To start a live scan from STRM, you must specify the scan name and the policy name for the live scan data you want to retrieve. As the live scan progresses, you can place your mouse over your Nessus scanner in the Scan Scheduling window to view the percentage of the live scan that is complete. After the live scan reaches completion, STRM uses the XMLRPC API to retrieve the scan data and update the vulnerability information for your assets.

The Nessus XMLRPC API is only available on Nessus servers and clients using software v4.2 and above.

To add a Nessus XMLRPC API live scan in STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 8-5 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Nessus Scanner . |

The list of parameters for the selected scanner type is displayed.

- Step 6** From the **Collection Type** list box, select **Scheduled Live Scan - XMLRPC API**.
- Step 7** Configure values for the following parameters:

Table 8-6 Scheduled Live Scan XMLRPC API Parameters

| Parameter | Description |
|-----------|---|
| Hostname | Type the IP address or hostname of the Nessus server. |
| Port | Type the port number for STRM to access your Nessus server using the XMLRPC API. The default is port 8834. |
| Username | Type the username required to log in to the Nessus server. |
| Password | Type the password that corresponds to the username. |
| Scan Name | Optional. Type the name of the scan you want displayed when the live scan runs on the Nessus server. If this field is clear, the API attempts to start a live scan for "STRM Scan". Note: STRM does not support using the ampersand (&) character in this field. |

Table 8-6 Scheduled Live Scan XMLRPC API Parameters (continued)

| Parameter | Description |
|-------------|--|
| Policy Name | <p>Type the name of a policy on your Nessus server to start a live scan.</p> <p>The policy you define must exist on the Nessus server when STRM attempts to launch the scan. If the policy does not exist, then an error is displayed in the status when STRM attempts to start the live scan.</p> <p>In most cases the policy name is customized to your Nessus server, but several default policies are included with Nessus.</p> <p>For example,</p> <ul style="list-style-type: none"> • External Network Scan • Internal Network Scan • Web App Tests • Prepare for PCI DSS audits <p>For more information on policies, see your Nessus vendor documentation.</p> |

Step 8 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

Step 11 After the changes are deployed, you must create a scan schedule for your live scan.

Scan reports can be created as a one-time event or as a reoccurring scheduled import. For more information on scheduling a scan, see [Schedule a Scan](#).

Add a Nessus Completed Report Import Using the XMLRPC API

A scheduled results import using the XMLRPC API allows STRM to retrieve completed Nessus scan reports from the Nessus server.

STRM connects to your Nessus server and downloads data from any completed reports matching the report name and maximum report age filter.

The Nessus XMLRPC API is only available on Nessus servers and clients using software v4.2 and above.

To add a Nessus completed scan import in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Click **Add**.

The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 8-7 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Nessus Scanner . |

The list of parameters for the selected scanner type is displayed.

Step 6 From the **Collection Type** list box, select **Scheduled Completed Report Import - XMLRPC API**.

Step 7 Configure values for the following parameters:

Table 8-8 Scheduled Completed Report Import XMLRPC API Parameters

| Parameter | Description |
|-----------------------------|--|
| Hostname | Type the IP address or hostname of the Nessus client or server hosting your Nessus or XML scan result files. |
| Port | Type the port number for STRM to access your Nessus server using the XMLRPC API. The default is port 8834. |
| Username | Type the username required to log in to the Nessus server. |
| Password | Type the password that corresponds to the username. |
| Report Name Filter | Type the file pattern, using a regular expression (regex), for the scan result files you are attempting to import. By default, the following file pattern is included to collect all available completed scan reports: *.* Note: If you update the regex in the Report Name Filter field, you must deploy the change to update your scanner configuration. |
| Results File Max Age (Days) | Type the maximum file age to include when importing Nessus scan result files during a scheduled scan. By default, the results file maximum age is 7 days. Files that are older than the specified days and the timestamp on the results file are excluded from the result file import. |

Step 8 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

Step 11 After the changes are deployed, you must create a scan schedule to import the scan report data.

Scan reports can be created as a one-time event or as a reoccurring scheduled import. For more information on scheduling a scan, see [Schedule a Scan](#).

Edit an Nessus Scanner

To edit a Nessus scanner configuration in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary.

- For scheduled live scan configurations, see [Table 8-2](#).
- For scheduled results import configurations, see [Table 8-4](#).
- For scheduled live scan XMLRPC API configurations, see [Table 8-6](#).
- For scheduled completed report import XMLRPC API configurations, see [Table 8-8](#).

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete a Nessus Scanner

To delete a Nessus scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

9

MANAGE NMAP SCANNERS

You can integrate Network Mapper (Nmap) scanners with STRM.

STRM uses SSH to communicate with the scanner server, start remote Nmap scans, and download the scan results. STRM supports two methods for importing Nmap vulnerability data:

- **Remote Live Scan** - Allows STRM to connect to a Nmap scanner and launch a scan using the Nmap binary file. STRM monitors the status of the live scan in progress and waits for the Nmap server to complete the scan. After the scan completes, STRM downloads the vulnerability results using SSH.

Several types of Nmap port scans require Nmap to run as root. Therefore, STRM must have access as root or you must clear the **OS Detection** check box. To run Nmap scans with **OS Detection** enabled, you must provide STRM with root access or configure the Nmap binary with setuid root. For assistance, contact your Nmap administrator.

- **Remote Results Import** - Allows STRM to connect to a Nmap scanner using SSH and download completed scan result files that are stored in a remote folder on the Nmap scanner. STRM can only import remote results stored in XML format. When configuring your Nmap scanner to generate a file for STRM import, you must generate the results file using the `-oX <file>` option.

Where `<file>` is the path to create and store the XML formatted scan results on your Nmap scanner.

After you add and configure either a Remote Live Scan or a Remote Results Import in STRM, you can schedule the frequency with which STRM imports vulnerability data. For more information, see [Manage Scan Schedules](#).

Add an Nmap Remote Live Scan

Adding a Remote Live Scan allows STRM to launch a Nmap scan, wait for the scan to complete, and then import the results.

After you added a live scan, you must assign a scan schedule in STRM. The scan schedule determines how often STRM launches a live scans on your Nmap scanner and retrieves vulnerability data for your assets.

To add an Nmap Remote Live Scan:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 9-1 Scanner Parameters

| Parameter | Description |
|--------------|--|
| Scanner Name | Type the name that you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host that you want to use to configure the scanner. |
| Type | From the list box, select Nmap Scanner . |

The list of parameters for the selected scanner type is displayed.

- Step 6** From the **Scan Type** list box, select **Remote Live Scan**.
- Step 7** Configure values for the following parameters:

Table 9-2 Nmap Live Scan Parameters

| Parameter | Description |
|---------------------------|---|
| Server Hostname | Type the hostname or IP address of the remote system hosting the Nmap client. We recommend using a UNIX-based system running SSH. |
| Server Username | Type the username required to access the remote system hosting the Nmap client using SSH. |
| Enable Key Authentication | Select this check box to enable STRM to use public or private key authentication. Selecting this check box requires you to specify the directory path to your key file on STRM using the Private Key File field. By default, the check box is clear. |

Table 9-2 Nmap Live Scan Parameters (continued)

| Parameter | Description |
|------------------|--|
| Login Password | Type the password associated with the username in the Server Username field. |
| Private Key File | <p>Type the directory path for the file that contains the private key information. This field is only displayed if the Enable Key Authentication check box is selected.</p> <p>If you are using SSH key based authentication, STRM uses the private key to authenticate the SSH connection. The default directory path is /opt/gradar/conf/vis.ssh.key. However, by default, this file does not exist. You must create the vis.ssh.key file or type another file name.</p> <p>This parameter is mandatory if the Enable Key Authentication check box is selected, otherwise this parameter is ignored.</p> |
| Nmap Executable | <p>Type the full directory path and filename of the executable file for the Nmap binary file.</p> <p>The default directory path to the executable file is /usr/bin/Nmap.</p> |
| Disable Ping | In some networks, the ICMP protocol is partially or completely disabled. In situations where ICMP is not enabled, you can select this check box to enable ICMP pings to enhance the accuracy of the scan. By default, the check box is clear. |
| OS Detection | <p>OS Detection allows Nmap to identify the operating system of a device or appliance in the target network. By default, the OS Detection check box is selected.</p> <p>The options include:</p> <p>Selected - If you select the OS Detection check box, you must provide a username and password with root privileges in the Server Username and Login Password fields.</p> <p>Cleared - If the OS Detection check box is clear and the returned results do not contain operating system information. The Server Username and Login Password fields do not require root privileges.</p> |
| Max RTT Timeout | <p>Select the Maximum Round-Trip Timeout (RTT) from the list box. The timeout value determines if a scan should be stopped or reissued due to latency between the scanner and the scan target. The default value is 300 milliseconds (ms).</p> <p>Note: If you type 50 milliseconds as the Maximum Round-Trip Timeout, we recommend the devices you are scanning be located on a local network. If you are scanning devices that are located on remote networks, we recommend selecting the 1 second Max RTT Timeout value.</p> |

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 fails. Make sure the following line is displayed 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 can differ. For more information, see the vendor documentation for your scanner.

Step 8 To configure the CIDR ranges that you want this scanner to consider:

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

Step 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

You are now ready to add a scan schedule to specify how often you want STRM to launch a live scan on your Nmap scanner. STRM can only import the vulnerability data after the live scan is complete. For more information on scheduling a scan, see [Manage Scan Schedules](#).

Add an Nmap Remote Results Import Scan

Adding an Nmap Remote Results Import scanner allows you to generate and store scans on your Nmap scanner.

Scans must be generated in XML format using the `-oX <file>` on your Nmap scanner. After you have added and configured your Nmap scanner, you must assign a scan schedule to specify how often you want STRM to import Nmap scans.

To add an Nmap Remote Result Import:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 9-3 Scanner Parameters

| Parameter | Description |
|--------------|--|
| Scanner Name | Type the name that you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host that you want to use to configure the scanner. |
| Type | From the list box, select Nmap Scanner . |

The list of parameters for the selected scanner type is displayed.

Step 6 From the **Scan Type** list box, select **Remote Results Import**.

Step 7 Configure values for the following parameters:

Table 9-4 Nmap Remote Results Import Parameters

| Parameter | Description |
|---------------------------|--|
| Server Hostname | Type the hostname or IP address of the remote system hosting the Nmap client. We recommend using a UNIX-based system running SSH. |
| Server Username | Type the username required to access the remote system hosting the Nmap client. |
| Enable Key Authentication | Select this check box to enable STRM to use public or private key authentication. Selecting this check box requires you to specify the directory path to your key file on STRM using the Private Key File field. By default, the check box is clear. |
| Login Password | Type the password associated with the username in the Server Username field. |
| Private Key File | <p>Type the directory path for the file that contains the private key information. This field is only displayed if the Enable Key Authentication check box is selected.</p> <p>If you are using SSH key based authentication, STRM uses the private key to authenticate the SSH connection. The default directory path 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 type another file name.</p> <p>This parameter is mandatory if the Enable Key Authentication check box is selected, otherwise this parameter is ignored.</p> |
| Remote Folder | Type the directory path on the Nmap scanner containing the XML vulnerability data. |
| Remote File Pattern | <p>Type a regular expression (regex) pattern to determine which Nmap XML result files to include in the scan report.</p> <p>All file names matching the regex pattern are included when importing the vulnerability scan report. You must use a valid regex pattern in this field. For example, the following pattern imports all XML files located in the remote folder:</p> <pre>. *\ .xml</pre> <p>Note: Scan reports imported and processed by STRM are not deleted from the remote folder. We recommend you schedule a cron job to delete previously processed scan reports on a scheduled basis.</p> |

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 fails. Make sure the following line is displayed 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 can differ. For more information, see the vendor documentation for your scanner.

Step 8 To configure the CIDR ranges that you want this scanner to consider:

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

Step 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

You are now ready to add a scan schedule to specify how often you want STRM to import the XML formatted scan reports from your NMap scanner. For more information on scheduling a scan, see [Manage Scan Schedules](#).

Edit an Nmap Scanner

To edit an Nmap scanner configuration in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary.

- For Nmap Live Scan configurations, see [Table 9-2](#).
- For Nmap Remote Results Import configurations, see [Table 9-4](#).

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete an Nmap Scanner

To delete an Nmap scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

10

MANAGE QUALYS SCANNERS

STRM retrieves vulnerability information from Qualys scanners in two ways; the Qualys Application Programming Interface (API) and by downloading scan reports generated by QualysGuard appliances.

QualysGuard vulnerability and asset information is supported on QualysGuard appliances using software version 4.7 to 7.2.

STRM offers two scanner modules for retrieving Qualys data:

- **Qualys Detection Scanner** - The Qualys Detection Scanner module accesses vulnerability data using the Qualys Host List Detection API of the QualysGuard appliance. The Qualys Detection Scanner allows you to retrieve results across multiple scan reports to collect vulnerability data. The Qualys Detection Scanner module for STRM requires that you specify a Qualys user that has the ability to download the Qualys KnowledgeBase.

For more information on Qualys Detection Scanner, see [Configure a Qualys Detection Scanner](#).

- **Qualys Scanner** - The Qualys Scanner module accesses vulnerability and asset scan reports through the remote web server of the QualysGuard appliance using an HTTPS connection.

For more information on Qualys Detection Scanner, see [Configure a Qualys Scanner](#)

After you configure the Qualys Detection Scanner or Qualys Scanner module in STRM, you can schedule a scan in STRM to collect vulnerabilities using the API or by downloading the scan report. Scan schedules allow you schedule how frequently STRM is updated with vulnerability data from external vulnerability appliances, such as Qualys Vulnerability Manager. For more information, see [Manage Scan Schedules](#).

Configure a Qualys Detection Scanner

The Qualys Detection Scanner uses the QualysGuard Host Detection List API to query across multiple scan reports to collect vulnerability data for assets.

The returned data contains the vulnerability as an identification number, which STRM compares against the latest Qualys Vulnerability Knowledge Base. The Qualys Detection Scanner does not support live scans, but allows the Qualys Detection Scanner to retrieve vulnerability information aggregated across multiple scan reports. STRM supports the key search parameters, such as the **Operating System Filter** field and **Asset Group Name** field.

The Qualys Detection Scanner also provides an option to configure how frequently the Qualys Vulnerability Knowledge Base is retrieved and cached by STRM. This is the **Qualys Vulnerability Retention Period** field. To force STRM to update the Qualys Vulnerability Knowledge Base for every scheduled scan, the Qualys Detection Scanner includes a **Force Qualys Vulnerability Update** check box. The Qualys user account you specify for STRM must have permissions enabled to download the Qualys KnowledgeBase. For more information, see your Qualys documentation.

Add a Qualys Detection Scanner

To add a Qualys Detection Scanner to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 10-1 Qualys Detection Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Qualys Detection Scanner . |

Step 6 Configure values for the following parameters:**Table 10-2** Qualys Detection Scanner Parameters

| Parameter | Description |
|-------------------------|---|
| Qualys Server Host Name | <p>Type the Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console based on your location. When specifying the FQDN, you must type the host name and not the URL.</p> <p>For example:</p> <ul style="list-style-type: none"> Type qualysapi.qualys.com for a QualysGuard server located in the United States. Type qualysapi.qualys.eu for a QualysGuard server host server located in Europe. Type qualysapi.<management_console> if you are using the full scanning infrastructure including an internal management console, where <management_console> is the host name of your internal management appliance. |
| Qualys Username | <p>Type the username necessary for requesting scans. This is the same username used to log in to the Qualys server.</p> <p>Note: The user you specify must have access to download the Qualys KnowledgeBase or you must enable the user account with the option to download the Qualys KnowledgeBase. For more information, see your Qualys documentation.</p> |
| Qualys Password | Type the password that corresponds to the Qualys Username. |
| Operating System Filter | <p>Type the regular expression (regex) required to filter the returned data by operating system. The Operating System Filter field contains .* as the default regex expression, which matches all operating systems.</p> <p>If you type an invalid regular expression in the Operating System Filter field, the scan fails when STRM initializes the scanner. To view the error message from a failed scan, move your mouse over the text in the Status column.</p> |
| Asset Group Names | <p>Type a comma-separated list, without spaces, to query IP addresses by their Asset Group Name. An asset group is a name provided by a user in the Qualys management interface to identify a list or range of IP addresses.</p> <p>For example, an Asset Group named Building1 can contain the IP address 192.168.0.1. An Asset Group named Webserver can contain 192.168.255.255. In STRM, to retrieve vulnerability information for both of these assets, type Building1,Webserver without spaces in the Asset Group Names field.</p> <p>When the scan completes, the Asset tab in STRM displays vulnerabilities by their IP address. For the example above, STRM would display all vulnerabilities for assets 192.168.0.1 and 191.168.255.255.</p> |

Table 10-2 Qualys Detection Scanner Parameters (continued)

| Parameter | Description |
|--|---|
| Host Scan Time Filter (days) | Type a numeric value (in days) to create a filter for the last time the host was scanned. Host Scan Times that are older than the specified number of days are excluded from the results returned by Qualys. |
| Qualys Vulnerability Retention Period (days) | Type the number of days you want to store the Qualys Vulnerability Knowledge Base locally in STRM. The default is 7 days. If a scan is scheduled and the retention period has expired, STRM downloads an updated Qualys Vulnerability Knowledge Base. |
| Force Qualys Vulnerability Update | Select this check box to force STRM to retrieve and cache the latest Qualys Vulnerability Knowledge Base. If this check box is selected, the retention period is set to zero retention and each scheduled scan retrieves the Qualys Vulnerability Knowledge Base. |
| Use Proxy | Select this check box if your scanner requires a proxy for communication or authentication. |
| Proxy Host Name | Type the host name or IP address of your proxy server if your scanner requires a proxy. |
| Proxy Port | Type the port number of your proxy server if your scanner requires a proxy. |
| Proxy Username | Type the username of your proxy server if your scanner requires a proxy. |
| Proxy Password | Type 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:

- a In the text field, type 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 On the **Admin** tab, click **Deploy Changes**.

You are now ready to configure a scan schedule to determine the frequency with which STRM collects Qualys Detection scanner information. For more information, see [Manage Scan Schedules](#).

Edit a Qualys Detection Scanner

To edit a Qualys Detection Scanner configuration in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the name of the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary. See [Table 10-2](#).

Step 7 Click **Save**.

Step 8 Choose one of the following deployment options:

- If you are reconfiguring Qualys Detection Scanner and did not update the Qualys Detection Scanner proxy credentials, click **Deploy Changes** on the **Admin** tab navigation menu.
- If you are reconfiguring your Qualys Detection Scanner and update the credentials in the **Proxy Username** field or the **Proxy Password** field, select **Advanced > Deploy Full Configuration** from the **Admin** tab navigation menu.

*Selecting **Deploy Full Configuration** restarts STRM services, resulting in a gap in data collection for events and flows until the deployment completes.*

Your Qualys scanner changes are complete.

Delete a Qualys Detection Scanner

To delete an Qualys scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

The Qualys Detection scanner is deleted from the scanner list.

Configure a Qualys Scanner

The Qualys Scanner module downloads and analyzes scan reports from the Qualys appliance.

If you select the Qualys Scanner, STRM must access the remote web server through an HTTPS connection to retrieve scan reports. The Qualys Scanner module supports three methods of scan data collection from Qualys.

The scan options for a Qualys scanner include:

- Starting a live scan on Qualys and collecting of the completed scan data.
- Scheduling imports of completed asset data reports.
- Scheduling imports of completed scan reports.

*If you are upgrading your Qualys Scanner from a version less than VIS-QualysQualysGuard-7.0-259655, you must verify the **Collection Type** parameter in the Add Scanner window for all existing Qualys Scanner configurations in STRM.*

Add a Qualys Scheduled Live Scan Report

Live scans allow STRM to launch preconfigured scans on the Qualys Scanner and collect the scan results when the live scan completes.

To add a Qualys live scan in STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 10-3 Qualys Scanner Parameters

| Parameter | Description |
|--------------|--|
| Scanner Name | Type the name that you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Qualys Scanner . |

Step 6 From the **Collection Type** list box, select **Scheduled Live - Scan Report**.

The configuration options for launching a live scan on your Qualys server are displayed.

Step 7 Configure values for the following parameters:**Table 10-4** Qualys Live Scan Parameters

| Parameter | Description |
|-------------------------|---|
| Qualys Server Host Name | Type the Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console based on your location. When specifying the FQDN, you must type the host name and not the URL. For example: <ul style="list-style-type: none"> Type qualysapi.qualys.com for a QualysGuard server located in the United States. Type qualysapi.qualys.eu for a QualysGuard server located in Europe. Type qualysapi.<management_console> if you are using the full scanning infrastructure including an internal management console, where <management_console> is the host name of your internal management appliance. |
| Qualys Username | Type the username necessary for requesting scans. This is the same username used to log in to the Qualys server. |
| Qualys Password | Type the password that corresponds to the Qualys Username. |
| Use Proxy | Select this check box if STRM requires a proxy server to communicate with your Qualys scanner. By default, this check box is clear. This check box displays additional proxy configuration settings. |
| Proxy Host Name | Type the host name or IP address of your proxy server. |
| Proxy Port | Type the port number of your proxy server. |
| Proxy Username | Type a username that allows STRM to authenticate with your proxy server. |
| Proxy Password | Type the password associated with the Proxy Username field. |
| Scanner Name | Type the name of the scanner that you want to perform the scan, as it is displayed on the QualysGuard server. To obtain the scanner name, contact your network administrator. Note: If you are using a public scanning appliance, you must clear the name from the Scanner Name field. |

Table 10-4 Qualys Live Scan Parameters (continued)

| Parameter | Description |
|-------------------|--|
| Option Profile(s) | Type the name of the option profile to determine which existing scan report is started as a live scan on the Qualys scanner. STRM retrieves the completed live scan data after the live scan completes. <i>Note: Live scans only support one option profile name per scanner configuration.</i> |

Step 8 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

You are now ready to configure a scan schedule to determine the frequency with which STRM launches the live scan on your Qualys scanner. For more information, see [Manage Scan Schedules](#).

Add a Qualys Scheduled Import Asset Data Report

An asset report data import allows you to schedule STRM to retrieve an asset report from your Qualys scanner. STRM determines which asset report to import from the file specified in the **Import File** field. If an import file is not specified, then STRM attempts to import the asset report based on the **Report Template Title** field.

To add a Qualys scheduled asset data report import to STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Click **Add**.

The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 10-5 Qualys Scanner Parameters

| Parameter | Description |
|--------------|--|
| Scanner Name | Type the name that you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |

Table 10-5 Qualys Scanner Parameters (continued)

| Parameter | Description |
|--------------|--|
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Qualys Scanner . |

Step 6 From the **Collection Type** list box, select **Scheduled Import - Asset Data Report**.

The configuration options for importing a Qualys asset report are displayed.

Step 7 Configure values for the following parameters:

Table 10-6 Qualys Asset Data Import Parameters

| Parameter | Description |
|-------------------------|---|
| Qualys Server Host Name | Type the Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console based on your location. When specifying the FQDN, you must type the host name and not the URL. For example: <ul style="list-style-type: none"> Type qualysapi.qualys.com for a QualysGuard server host name located in the United States. Type qualysapi.qualys.eu for a QualysGuard server host name located in Europe. Type qualysapi.<management_console> if you are using the full scanning infrastructure including an internal management console, where <management_console> is the host name of your internal management appliance. |
| Qualys Username | Type the username necessary for requesting scans. This is the same username used to log in to the Qualys server. |
| Qualys Password | Type the password that corresponds to the Qualys Username. |
| Use Proxy | Select this check box if STRM requires a proxy server to communicate with your Qualys scanner. By default, this check box is clear. This check box displays additional proxy configuration settings. |
| Proxy Host Name | Type the host name or IP address of your proxy server. |
| Proxy Port | Type the port number of your proxy server. |
| Proxy Username | Type a username that allows STRM to authenticate with your proxy server. |
| Proxy Password | Type the password associated with the Proxy Username field. |
| Collection Type | From the list box, select Scheduled Import - Asset Data Report . This option allows the scanner to retrieve the latest asset report from the file specified in the Import File field. |

Table 10-6 Qualys Asset Data Import Parameters (continued)

| Parameter | Description |
|------------------------|---|
| Report Template Title | Type a report template title to replace the default title when retrieving asset data reports. |
| Max Report Age (Days) | Type the maximum file age to include when importing Qualys Asset Data during a scheduled scan. By default, the results file maximum age is 7 days. Files that are older than the specified days and the timestamp on the report file are excluded from the scheduled import. |
| Import File (Optional) | Optional. Type a directory path to download and import a single asset report from Qualys to your STRM Console or managed host. For example, to download an asset report named STRM_scan.xml from a logs directory on your managed host, type the following: <code>/qualys_logs/STRM_scan.xml</code> If you specify an import file location, STRM downloads the contents of the asset report from Qualys to the local directory. After the download of the asset report is complete to your Console, then STRM imports the asset information using the local file. If the Import File field does not contain a value or if the file or directory cannot be found, then the Qualys scanner attempts to retrieve the latest asset report using the Qualys API based on the information in the Report Template Title field. |

Step 8 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

You are now ready to configure a scan schedule to determine the frequency with which STRM imports the asset report from your Qualys scanner. For more information, see [Manage Scan Schedules](#).

Add a Qualys Scheduled Import Scan Report

A scheduled import of Qualys scan reports allows STRM to retrieve completed scans from your Qualys scanner.

To add a Qualys scan report data import to STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Click **Add**.

The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 10-7 Qualys Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Qualys Scanner . |

Step 6 From the **Collection Type** list box, select **Scheduled Import - Scan Report**.

The configuration options for importing completed Qualys scan reports are displayed.

Step 7 Configure values for the following parameters:

Table 10-8 Qualys Schedule Scan Import Parameters

| Parameter | Description |
|-------------------------|---|
| Qualys Server Host Name | Type the Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console based on your location. When specifying the FQDN, you must type the host name and not the URL. For example: <ul style="list-style-type: none"> Type qualysapi.qualys.com for a QualysGuard server host name located in the United States. Type qualysapi.qualys.eu for a QualysGuard server host name located in Europe. Type qualysapi.<management_console> if you are using the full scanning infrastructure including an internal management console, where <management_console> is the host name of your internal management appliance. |
| Qualys Username | Type the username necessary for requesting scans. This is the same username used to log in to the Qualys server. |
| Qualys Password | Type the password that corresponds to the Qualys Username. |

Table 10-8 Qualys Schedule Scan Import Parameters (continued) (continued)

| Parameter | Description |
|--------------------------|--|
| Use Proxy | Select this check box if STRM requires a proxy server to communicate with your Qualys scanner. By default, this check box is clear. This check box displays additional proxy configuration settings. |
| Proxy Host Name | Type the host name or IP address of your proxy server. |
| Proxy Port | Type the port number of your proxy server. |
| Proxy Username | Type a username that allows STRM to authenticate with your proxy server. |
| Proxy Password | Type the password associated with the Proxy Username field. |
| Collection Type | From the list box, select Scheduled Import - Scan Report . |
| Option Profile(s) | Type a single option profile name or use a comma-separated list of option profile names to filter the list of scan reports downloaded from your Qualys scanner. Any scan reports matching the option profile name are imported. If the Option Profile(s) field does not contain an Option Profile name, then the list is not filtered based on any Option Profiles and all scan reports for all Option Profiles are retrieved. For more information, see your QualysGuard documentation. Note: <i>If data is not retrieved from an Option Profile in your comma-separated list, the scan report might not be available for download. Ensure Qualys has completed the scan report associated with the Option Profile.</i> |
| Scan Report Name Pattern | Type a file pattern, using a regular expression (regex), for the scan reports you are attempting to import. By default, STRM attempts to download all available scan reports using the following file pattern: <code>.*</code> . |
| Max Report Age (Days) | Type the maximum file age to include when importing Qualys scan reports during a scheduled scan. By default, the results file maximum age is 7 days. Files that are older than the specified days and the timestamp on the report file are excluded from the scheduled import. |

Table 10-8 Qualys Schedule Scan Import Parameters (continued) (continued)

| Parameter | Description |
|---------------------------|---|
| Import File (Optional) | <p>Optional. Type a directory path to download and import a single scan report from Qualys to your STRM Console or managed host.</p> <p>For example, to download a scan report named STRM_scan.xml from a logs directory on your managed host, type the following:</p> <pre>/qualys_logs/STRM_scan.xml</pre> <p>If you specify an import file location, STRM downloads the contents of the asset scan report from Qualys to the local directory. After the download of the asset scan report is complete, then STRM imports the asset information using the local file.</p> <p>If the Import File field does not contain a value or if the file or directory cannot be found, then the Qualys scanner attempts to retrieve the latest asset data report using the Qualys API based on the information in the Report Template Title field.</p> |

Step 8 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

You are now ready to configure a scan schedule to determine the frequency with which STRM imports the asset data report from your Qualys scanner. For more information, see [Manage Scan Schedules](#).

Edit a Qualys Scanner To edit a Qualys Scanner configuration in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary.

- For Qualys Live Scan parameters, see [Table 10-4](#).
- For Qualys Asset Report Data Import parameters, see [Table 10-6](#).
- For Qualys Scheduled Import Scan Report parameters, see [Table 10-8](#).

Step 7 Click **Save**.

Step 8 Choose one of the following deployment methods:

- If you are reconfiguring the Qualys Scanner and did not update the Qualys Scanner proxy credentials, click **Deploy Changes** on the **Admin** tab navigation menu to complete your configuration edit.
- If you are reconfiguring your Qualys Scanner and updating the credentials in the **Proxy Username** field or the **Proxy Password** field, select **Advanced > Deploy Full Configuration** on the **Admin** tab navigation menu to complete your configuration edit.

*Selecting **Deploy Full Configuration** restarts STRM services, resulting in a gap in data collection for events and flows until the deployment completes.*

Your Qualys scanner changes are complete.

Delete a Qualys Scanner To delete a Qualys scanner from STRM:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.

Step 3 Click the **VA Scanners** icon.
The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.
A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.
The Qualys scanner is deleted from the scanner list.

11

MANAGE FOUNDSCAN SCANNERS

The Foundstone FoundScan scanner for STRM allows STRM to query the FoundScan Engine using the FoundScan OpenAPI for host and vulnerability information.

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 user interface for STRM to retrieve the scan results. If the scan is not displayed in the FoundScan user interface or is scheduled to be removed after completion, STRM needs to retrieve the results before the scan is removed or the scan fails.
- The appropriate user privileges must be configured in the FoundScan application, which allows STRM to communicate with FoundScan.

Since the FoundScan OpenAPI only provides host and vulnerability information to STRM, your Asset Profile information displays 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 plug-in 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. For more information, see [Import Certificates](#).

After you configure the FoundScan system and the FoundScan scanner in STRM, 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 [Manage Scan Schedules](#).

Add a FoundScan Scanner

To add a FoundScan scanner to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 11-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. <i>Note: Certificates for your FoundScan scanner must reside on the managed host selected in the Managed Host list box.</i> |
| Type | From the list box, select FoundScan Scanner . |

- Step 6** Configure values for the following parameters:

Table 11-2 FoundScan Parameters

| Parameter | Description |
|--------------|---|
| SOAP API URL | Type the web address for the Foundscan OpenAPI in the following format: https://<foundstone IP address>:<SOAP port> 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 https://localhost:3800 . |

Table 11-2 FoundScan Parameters (continued)

| Parameter | Description |
|--------------------|---|
| Customer Name | Type the name of the customer under which the Login User Name belongs. |
| User Name | Type 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 | Type the IP address of the STRM server that you want to perform the scan. By default, this value is not used; however, is necessary for validating some environments. |
| Password | Type the password corresponding to the Login User Name for access to the API. |
| Portal Name | Optional. Type the portal name. This field can be left blank for STRM purposes. See your FoundScan administrator for more information. |
| Configuration Name | Type 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 | Displays the directory path and filename for the CA truststore file. The default is /opt/qradar/conf/foundscan.keystore. |
| Client Keystore | Displays the directory path and filename for the client keystore. The default is /opt/qradar/conf/foundscan.truststore. |

Step 7 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 On the **Admin** tab, select **Deploy Changes**.

Edit a FoundScan Scanner

To edit a FoundScan scanner configuration in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

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

Step 7 Click **Save**.

Step 8 On the **Admin** tab, select **Deploy Changes**.

Delete a FoundScan Scanner

To delete a FoundScan scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, select **Deploy Changes**.

Configure 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 the following:

- [Obtain a Certificate](#)
- [Import Certificates](#)

Obtain 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 type 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 hosts the scanner component. See [Import Certificates](#).

Import 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 to the STRM managed host you selected in [Table 11-1](#).

Before you attempt to import certificates using the procedure below, make sure the FoundScan scanner is added to STRM, see [Add a FoundScan Scanner](#).

To import certificates to STRM:

- 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** Type 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 can 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 host the scanner.

Example Of TrustedCA.pem File

```
-----BEGIN CERTIFICATE-----
MIICFzCCAYCgAwIBAgIBADANBgkqhkiG9w0BAQQFADAYMRYwFAYDVQQDEw1Gb3Vu
ZHN0b251IENBMB4XDTAzMDEkxMjIzMjZkxMV0XDTA4MTAyMDIzMjZkxMVowGDEWMBQ
J9PUXhzRqqh8yZh795R9D1oj7hsyZtq4My6gKu8RuHVBscYvJVwPMUkPmDHMnpj1
A1UEAxMNRm91bmRzdG9uZSBDQTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
sWN8ZzqqREMZ7qByvuIqr2q4XaP5Tfp3hRC08mjvqWsQjK2B8WMRagZjHqvPN/qfG
5uZw5gm1M6IyoVbLkaQwDF34McRpqlTLVjeDadjPuRaZGVu4zVknC8s83EPqKU9+
fdqmhtCwwqVYq+sQFp1S3kKUvXIBEGV0r9mnFAD3InUCAwEAAaNxMG8wHQYDVR0O
BBYEFG08UJTPbqSP202Mqys2sqzU2h7LMEAGA1UdIwQ5MDeAFG08UJTPbqSP202M
```

```
ygs2sqzU2h7LoRykGjAYMRYwFAYDVQQDEw1Gb3VuZHN0b251IENBggEAMAwGA1Ud
j0ynMtEM2mtuf95uxeGFe581k31w9d3IGt19uahtyqG860kr4/ys3r7LjA0f9rjf
J9PUXhzRqgh8yzh795R9D1oj7hsyZtq4My6gKu8RuHVBscYvJVwPMUKPmDHMnpj1
4p7dh7GKk7ymFYs=
-----END CERTIFICATE-----
```

Example of Portal.pem File

The following is an example of the Portal.pem file:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQC5DOnQtMtDXAHth/4M/1I9gVlyoch9EYvCiAsZmtO2JMTjEDse
mH0DQkxSKv0gvsCqKXhX6nNegyyiCM1GuEDvFYPCI5FrkrzEwtndTILGXT5asDXu
ncnAl/9am4jAhADDPFfb9ZRMoe6aFE13XD21o49gJG4sH+VkcQQDrf6OGfnR6YaYz
SbPTMrBKR5pfMJOPJ/Sjc0vf6A48Nn8FiYLDiyBLKhunzM03EZ22VrZxBwIDAQAB
AoGARZfkqzgDJZ8JnpJBahOPTFBEGodbhiW+IPfW7Nc8fcjQPvDQuw3wHfSmDVTb
g6AZhyU1FBzvLIE6nOmggdMzn9KIN8WMD+XDAAR4AaWOGkN18Ib4h1VVnsa90hYS
BPIWVsfbAkEAySj6iwtolLVsXC5cIP4YzNzNsJ2QBqeEhEfUmLtZl8vDlsj+EM2L
JggOcRpYMxIj64ob/hevavXewlCFermpRQJBAKaq60KQsILEhUoGHLJTt2BtOpEs
3JP4BBUV7QE0VTTKxA8byQqjGSu6zh/JxWk9hTjo5oSCmlcwahC5k104Cy0CQQCt
vnwv7mncFtsB/3TJdk67Wxc7FRs59CRsEJKaXG80weVjtXRj1PSTo6+91tCJQ+jM
fxxQaeq0SqqEWlb+UuC1AkEA6Z503v5plrVUWTo+L8JaygumdzZRuBZi/EVuxqG
j79b6Xa+UvXtXquU2qlolweanry/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
ZHN0b251IENBMB4XDTAzMzY1NFoXDTA4MTAyMDIzMzY1NFowKDEmMCQG
A1UEAxMdBm91bmRzdG9uZSBFbnRlcnByaXNlIE1hbmFnZXIwZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBALkM6dC0y0NcAe2H/gz+Uj2BWKKhyH0Ri8KICxma07Yk
xOMQOx6YfQNCtFIq/SC+wKopcfHqc16DLKIIzUa4QO8Vg8IjkWuSvMTC2d1MgsZd
PlqwNe5Js9MysEpHm18wmg8n9KNzS9/oDjw2fwWJgsOLIEsqG6fMzTcRnbZWtnEH
AgMBAAGjgZ0wgZowCQYDVR0TBAlwADAsBgIghkgBhvCAQ0EHxYdT3B1b1NTTCBH
ZW51cmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFA1SVO+gs5GdPUes2J5iKjQP
Cf+NMEAGA1UdIwQ5MDeAFGQ8UJTPbqSP202Mygs2sqzU2h7LoRykGjAYMRYwFAYD
VQQDEw1Gb3VuZHN0b251IENBggEAMA0GCSqGSIb3DQEBAUAA4GBAEqIP1E0WzA7
W3xXMYyiOwAWYax7t67NaBEBolK3WR7GW68q7fnu72QRsrkUIX0sNdPLCQihqyaT
D6qX68x1q5WjDXcLIyBKDQQYRy1Yp95hn6o82qUAnbXrUvviW1ZFAGj53w+HvPOC
0T05eZ7vZOL1YzvqKZT7AI+4CHzw7mi2
-----END CERTIFICATE-----

```

12

MANAGE JUNIPER NETWORKS NSM PROFILER SCANNERS

The Juniper Networks Netscreen Security Manager (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 versions 2007.1r2, 2007.2r2, 2008.1r2, 2009.1r1, and 2010.x. For more information, see your vendor documentation.

STRM collects data from the PostgreSQL database on the NSM using 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.

After you add the Juniper Networks NSM Profiler scanner in STRM, you can schedule a scan. Scan schedules allow you to configure the frequency with which STRM attempts to retrieve vulnerabilities. For more information, see [Manage Scan Schedules](#).

Add a Juniper Networks NSM Profiler Scanner

To add a Juniper Networks NSM Profiler scanner:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 12-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Juniper NSM Profiler Scanner . |

Step 6 Configure values for the following parameters:

Table 12-2 Juniper Networks NSM Profiler Parameters

| Parameter | Description |
|-------------------|---|
| Server Host Name | Type the hostname or IP address of the NetScreen Security Manager (NSM) server. |
| Database Username | Type the Postgres username to log in to the Profiler database stored on the NSM server. |
| Database Password | Type the password associated with the Database Username to log in to the server. |
| Database Name | Type 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, type 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 On the **Admin** tab, click **Deploy Changes**.

Edit a Juniper Networks NSM Profiler Scanner

To edit a Juniper Networks NSM Profiler scanner configuration in STRM:

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

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary. See [Table 12-2](#).

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete a Juniper Networks NSM Profiler Scanner

To delete a Juniper Networks NSM Profiler scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

13

MANAGE RAPID7 NeXPOSE SCANNERS

The Rapid7 NeXpose scanner uses a web-based API to obtain scan results for STRM from all sites connected to your NeXpose Security Console.

STRM supports two methods for importing Rapid7 NeXpose vulnerability data:

- Import Site Data - Adhoc Report via API
Site data importing allows STRM to log in to the Rapid7 NeXpose scanner and download an adhoc report from the scanner based on the vulnerabilities discovered from the IP addresses configured for your site. For more information, see [Import Rapid7 NeXpose Vulnerability Data Using the API](#).
- Import Site Data - Local File
Local file site importing allows STRM to import scan reports for a site based from a local file downloaded to your STRM Console. The Rapid7 NeXpose XML file containing the vulnerability data must be copied from your Rapid7 NeXpose appliance to the STRM Console or managed host that is performing the local import. You must create a directory on the STRM Console or managed host before copying scan report XML files. Files can be copied using Secure Copy (SCP) or Secure File Transfer Protocol (SFTP). For more information, see [Import Rapid7 NeXpose Vulnerabilities from a Local File](#).

After you configure the Rapid7 NeXpose device and the Rapid7 NeXpose scanner in STRM, you can schedule a scan. Scheduling a scan allows you to schedule when STRM imports vulnerability data from Rapid7 NeXpose using the API or when STRM imports the local XML file containing vulnerability data. For more information, see [Manage Scan Schedules](#).

For more information, see your Rapid7 NeXpose documentation.

Import Rapid7 NeXpose Vulnerability Data Using the API

Importing site vulnerability data using the API allows STRM to import completed vulnerability scans based on the site names configured on your Rapid7 NeXpose scanner.

Configure a Rapid7 NeXpose Scanner

To configure a Rapid7 NeXpose scanner to import ad-hoc site report data:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 13-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Rapid7 Nexpose Scanner . |

- Step 6** From the **Import Type** list box, select **Import Site Data - Adhoc Report via API**.
- Step 7** Configure values for the following parameters:

Table 13-2 Rapid7 NeXpose Parameters

| Parameter | Description |
|-----------------|---|
| Remote Hostname | Type the host name or IP address of the Rapid7 NeXpose Security Console configured with the site vulnerability data you want to import. |
| Login Username | Type the username to log in to the Rapid7 NeXpose Security Console. <i>Note: The login must be a valid user and obtained from the Rapid7 NeXpose Security Console user interface. For more information, contact your Rapid7 NeXpose administrator.</i> |
| Login Password | Type the password to log in to the Rapid7 NeXpose Security Console. |
| Port | Type the port used to connect to the Rapid7 NeXpose Security Console. <i>Note: The port number is the same port used to connect to the Rapid7 NeXpose Security Console user interface. This is typically port 3780. For more information, contact your Rapid7 NeXpose server administrator.</i> |

Table 13-2 Rapid7 NeXpose Parameters (continued)

| Parameter | Description |
|-------------------------|---|
| Site Name Pattern | Type a regular expression (regex) pattern to determine which Rapid7 NeXpose sites to include in the scan report. The default Site Name Pattern <code>.*</code> selects all available site name reports. All site names matching the regex pattern are included in the scan report. You must use a valid regex pattern in this field. |
| Cache Timeout (Minutes) | Type the length of time the data from the last generated scan report is stored in the cache. Note: If the specified time limit expires, new vulnerability data is requested from the Rapid7 NeXpose Security Console using the API. |

Step 8 To configure the CIDR ranges you want this scanner to consider:

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

Since STRM imports scan reports from Rapid7 NeXpose, we recommend you configure a CIDR range of 0.0.0.0/0 to import scan reports. This ensures scan reports are not missed during a scheduled scan when STRM attempts to import scan reports from your Rapid7 NeXpose appliance.

Step 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

You are now ready to add a scan schedule to determine the frequency with which STRM imports adhoc vulnerability data reports from the Rapid7 NeXpose using the API. For more information on scheduling a scan, see [Manage Scan Schedules](#).

Troubleshoot a Rapid7 NeXpose API Scan Import

The Rapid7 NeXpose scanners that are using the API to collect adhoc reports of asset vulnerabilities are based on your site configuration.

Depending on the number of IP addresses configured for each site can impact the size of the adhoc report. Large site configurations can cause the site reports to be extremely large and take several hours to complete. Rapid7 NeXpose must successfully generate a site scan report before the session timeout value expires. If you cannot retrieve the scan results from your largest Rapid7 NeXpose sites using STRM, you must increase the Rapid7 NeXpose session timeout value.

To configure your Rapid7 NeXpose session timeout value:

Step 1 Log in to the Rapid7 NeXpose user interface.

Step 2 Select the **Administration** tab.

You must have Administrative privileges on your Rapid7 NeXpose device to view the **Administration** tab.

Step 3 From NeXpose Security Console, select **Manage**.

The NeXpose Security Console Configuration window is displayed.

Step 4 From the navigation menu on the left side of the NeXpose Security Console Configuration window, select **Web Server**.

Step 5 Increase the value for **Session timeout (in seconds)**.

Step 6 Click **Save**.

For more information about your Rapid7 NeXpose device, see your vendor documentation.

If you are still having issues importing large sites using the API, you can use the local file import by moving completed XML scans to your STRM Console or managed host responsible for importing the vulnerability data. For more information, see [Import Rapid7 NeXpose Vulnerabilities from a Local File](#).

Import Rapid7 NeXpose Vulnerabilities from a Local File

Importing site vulnerability data using the local files allows STRM to import completed vulnerability scans based on completed scan reports copied from your Rapid7 NeXpose scanner to STRM.

To configure STRM to import local Rapid7 NeXpose files:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Click **Add**.

The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 13-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Rapid7 Nexpose Scanner . |

Step 6 From the **Import Type** list box, select **Import Site Data - Local File**.

Step 7 Configure values for the following parameters:

Table 13-2 Rapid7 NeXpose Parameters

| Parameter | Description |
|---------------------|--|
| Import Folder | Type the directory path on the STRM Console or managed host containing the XML vulnerability data. If you specify an import folder, you must move the vulnerability data from your Rapid7 NeXpose Security Console to STRM. STRM imports the asset information from the local file folder using the Import File Pattern field. |
| Import File Pattern | Type a regular expression (regex) pattern to determine which Rapid7 NeXpose XML files to include in the scan report. All file names matching the regex pattern are included when importing the vulnerability scan report. You must use a valid regex pattern in this field. The default value <code>*\.xml</code> imports all files located in the import folder. <i>Note: Scan reports imported and processed by STRM are not deleted from the import folder, but renamed to end in <code>.processed0</code>. We recommend you schedule a cron job to delete previously processed scan reports on a scheduled basis.</i> |

Step 8 To configure the CIDR ranges that you want this scanner to consider:

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

Step 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

You are now ready to add a scan schedule to determine the frequency with which STRM imports local vulnerability data reports from the local files on the STRM Console or managed host. For more information on scheduling a scan, see [Manage Scan Schedules](#).

Edit a Rapid7 NeXpose Scanner

To edit a Rapid7 NeXpose scanner configuration in STRM:

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

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary. See [Table 13-2](#).

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete a Rapid7 NeXpose Scanner

To delete a Rapid7 NeXpose scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

14

MANAGE netVigilance SecureScout SCANNERS

You can collect vulnerabilities from netVigilance SecureScout NX and SecureScout SP devices.

netVigilance SecureScout NX and SecureScout SP store all scan results to an SQL database (Microsoft MSDE or SQL Server). STRM connects to the database, locates the latest scan results for a given IP address, and returns the discovered services and vulnerabilities to the asset profile. This allows you to search for assets and vulnerabilities using the **Asset** tab in STRM. 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, 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 database user you create must have select permissions to the following tables:

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

The user must have execute permissions on the stored procedure IPSORT.

After you add the SecureScout scanner in STRM, you can schedule a scan. For more information, see [Manage Scan Schedules](#).

Add a SecureScout Scanner

To add a SecureScout scanner:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 14-1 SecureScout Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select SecureScout Scanner . |

- Step 6** Configure values for the following parameters:

Table 14-2 SecureScout Parameters

| Parameter | Description |
|-------------------|---|
| Database Hostname | Type the IP address or hostname of the SecureScout database server that runs the SQL server. |
| Login Username | Type the SQL database username that you want STRM to use to log in to the SecureScout database. |
| Login Password | Type the corresponding password for the Login Username. |
| Database Name | Type the name of the database within the SQL server that contains the SecureScout data. The default is SCE. |
| Database Port | Type 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, type 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** On the **Admin** tab, click **Deploy Changes**.

Edit a SecureScout Scanner

To edit a SecureScout scanner:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window is displayed.
- Step 6** Update parameters, as necessary. See [Table 14-2](#).
- Step 7** Click **Save**.
- Step 8** On the **Admin** tab, click **Deploy Changes**.

Delete a SecureScout Scanner

To delete a SecureScout Scanner from STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window is displayed.
- Step 6** Click **OK**.
- Step 7** On the **Admin** tab, click **Deploy Changes**.

15

MANAGE eEye SCANNERS

STRM supports both eEye REM Security Management Console and eEye Retina CS scanners. eEye scanners use SNMPv1, SNMPv2, or SNMPv3 to send SNMP traps to STRM.

To configure eEye scanners with STRM, you must:

- 1 Configure your eEye scanner to forward SNMP traps to STRM. For more information, see your eEye vendor documentation.
- 2 Add your eEye scanner to STRM.
- 3 Optional. Install the Java™ Cryptography Extension for high level SNMPv3 decryption algorithms.
- 4 Schedule a scan for your eEye scanner in STRM.

After a scan completes, the results are pushed to STRM using SNMP and the results are stored on STRM or your managed host in a temporary directory. STRM constantly monitors the listening port to obtain asset and vulnerability information from the eEye scanner. To ensure the host and port profile information is updated in STRM, you must configure a scan schedule for your eEye scanner. The scan schedule determines the frequency with which STRM imports the SNMP data stored in the **Base Directory** field. This scan schedule allows the port and host profiles to be available in the profile database.

To connect STRM to the eEye scanner, you must have administrative access to STRM and your eEye appliance. You must also ensure that any firewalls between your eEye scanner and STRM allows SNMP traffic.

Add an eEye Scanner

To add an eEye REM scanner to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.

Step 4 Click **Add**.

The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:**Table 15-1** eEye REM Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select eEye REM Scanner . |

Step 6 Configure values for the following parameters:**Table 15-2** eEye Parameters

| Parameter | Description |
|-------------------------|--|
| Base Directory | Type the location where you want to store the temporary files resulting from the scan. The default is /store/tmp/vis/eEye/. |
| Cache Size | Type the number of transactions you want to store in the cache before writing the information to disk. The default is 40. |
| Retention Period | Type the time period, in days, that 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 retention period is 5 days. |
| Use Vulnerability Data | Select this check box to correlate vulnerability data to Common Vulnerabilities and Exposures (CVE) identifiers and description information from your eEye REM or eEye CS Retina scanner. By default, the audits.xml vulnerability data file is located in the following directory: %ProgramFiles(x86)%\eEye Digital Security\Retina CS\Applications\RetinaManager\Database\audits.xml Note: This option requires that you copy the audits.xml file from your eEye REM or eEye Retina CS appliance to STRM. |
| Vulnerability Data File | Type the directory path to the eEye audits.xml file. The default is /opt/qradar/conf/audits.xml. Note: For the most up-to-date eEye audit information, you must periodically update STRM with the latest audits.xml file from your eEye REM or eEye Retina scanner. For more information, see your eEye vendor documentation. |

Table 15-2 eEye Parameters (continued)

| Parameter | Description |
|-------------------------|---|
| Listen Port | Type the port number used to monitor for incoming SNMP vulnerability information from your eEye scanner. The default is 1162. |
| Source Host | Type the IP address for your eEye REM or eEye Retina CS scanner. |
| SNMP Version | From the list box, select the SNMP version you configured for your eEye scanner to forward. The options include: <ul style="list-style-type: none"> • v1 - Select v1 if your eEye scanner is forwarding SNMPv1 traps. • v2 - Select v2 if your eEye scanner is forwarding SNMPv2 traps. • v3 - Select v3 if your eEye scanner is forwarding SNMPv3 traps. The default is SNMPv2. |
| Community String | Type the SNMP community string for the SNMPv2 protocol, such as Public. This parameter is only used if you select v2 for your SNMP version. The default community string is public. |
| Authentication Protocol | From the list box, select the algorithm you want to use to authenticate SNMP traps. This parameter is required if you are using SNMPv3. The options include: <ul style="list-style-type: none"> • SHA - Select this option to use Secure Hash Algorithm (SHA) as your authentication protocol. • MD5 - Select this option to use Message Digest 5 (MD5) as your authentication protocol. The default is SHA. |
| Authentication Password | Type the password you want to use to authenticate SNMP. This parameter only applies to SNMPv3. Note: Your authentication password must include a minimum of 8 characters. |

Table 15-2 eEye Parameters (continued)

| Parameter | Description |
|---------------------|---|
| Encryption Protocol | <p>From the list box, select the algorithm you want to use to decrypt the SNMP traps. This parameter is required if you are using SNMPv3.</p> <p>The decryption algorithms include:</p> <ul style="list-style-type: none"> • DES • AES128 • AES192 • AES256 <p>The default is DES.</p> <p>Note: If you select AES192 or AES256 as your decryption algorithm, you must install additional software for STRM. For more information, see Install the Java Cryptography Extension.</p> |
| Encryption Password | <p>Type the password used to decrypt SNMP traps. This parameter is required if you are using SNMPv3.</p> <p>Note: Your encryption password must include a minimum of 8 characters.</p> |

Step 7 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 On the **Admin** tab, click **Deploy Changes**.

Changes made to your SNMP configuration for your eEye scanner do not take effect until the next scheduled scan begins. If the configuration change requires an immediate update, you must complete a full deploy in STRM. For more information, see [Edit an eEye Scanner, Step 9](#).

The configuration in STRM is complete.

If you selected SNMPv3 as your eEYe configuration with AES192 or AES256 encryption, you must install an additional Java™ component on your STRM Console or Event Collector.

Install the Java Cryptography Extension

The Java™ Cryptography Extension (JCE) is a Java™ framework that is required for STRM to decrypt advanced cryptography algorithms for AES192 or AES256.

The following information describes how to install Oracle JCE on STRM.

To install the Unrestricted JCE Policy Files on STRM.

Step 1 Download the latest version of the Java™ Cryptography Extension:

<https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk>

There may be several versions of the JCE available for download. The version you download should match the version of the Java™ installed on STRM.

Step 2 Extract the JCE file.

The following archive files are included in the JCE download:

- local_policy.jar
- US_export_policy.jar

Step 3 Using SSH, log in to your STRM Console or managed host as a root user.

Username: `root`

Password: `<password>`

Step 4 Copy the JCE jar files to the following directory on your STRM Console or managed host:

`/opt/ibm/java-x86_64-60/jre/lib/security/US_export_policy.jar`

`/opt/ibm/java-x86_64-60/jre/lib/security/local_policy.jar`

The jar files are only copied to the system receiving the AES192 or AE256 encrypted files. Depending on your configuration, this could be your STRM Console or a managed host.

The installation of the Java™ Cryptography Extension for STRM is complete. You are now ready to schedule a scan for your eEye scanner in STRM. For more information, see [Manage Scan Schedules](#).

Edit an eEye Scanner

To edit an eEye scanner configuration in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary. See [Table 15-2](#).

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Changes made to the SNMP configuration for your eEye scanner do not take effect until the next scheduled scan begins. If the configuration change requires an immediate update, you must complete a full deploy in STRM.

Step 9 Optional. On the **Admin** tab, select **Advanced > Deploy Full Configuration**.

Deploying Full Configuration restarts multiple services on the STRM. Event collection is unavailable on STRM until the Deploy Full Configuration completes.

Delete an eEye Scanner

To delete an eEye REM scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

16

MANAGE PatchLink SCANNERS

You can integrate a PatchLink scanner (version 6.4.4. and above) with STRM.

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.

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 between your PatchLink appliance and STRM are configured to allow communications.

After you configure your PatchLink appliance and add a PatchLink scanner in STRM, then you are ready to schedule a scan. Scan schedules allow you to determine the frequency with which STRM requests data from your PatchLink appliance using the SOAP API. For more information, see [Manage Scan Schedules](#).

Add a PatchLink Scanner

To add a PatchLink scanner to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 16-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Lumension PatchLink Scanner . |

Step 6 Configure values for the following parameters:

Table 16-2 PatchLink Parameters

| Parameter | Description |
|----------------------------|---|
| Engine Address | Type 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 HKLM\Software\Harris\reportcenter_listenport registry key, specify the new port number. |
| Username | Type 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 | Type the password corresponding to the Username. |
| Job Name | Type the job name that exists in the PatchLink scanner. The job must be complete before you schedule the scan in STRM. |
| Result Refresh Rate (mins) | Type 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 configured 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, type 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 On the **Admin** tab, click **Deploy Changes**.

Edit a PatchLink Scanner

To edit a PatchLink scanner configuration in STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window is displayed.
- Step 6** Update parameters, as necessary. See [Table 16-2](#).
- Step 7** On the **Admin** tab, click **Deploy Changes**.

Delete a PatchLink Scanner

To delete a PatchLink scanner from STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window is displayed.
- Step 6** Click **OK**.
- Step 7** On the **Admin** tab, click **Deploy Changes**.

17

MANAGE McAfee VULNERABILITY MANAGER SCANNERS

The McAfee Vulnerability Manager scanner for STRM allows STRM to import vulnerabilities using an XML file or query for a results file using the McAfee OpenAPI.

The McAfee Vulnerability Manager scanner for STRM does not start scans remotely, but gathers scan result data after a scan completes on the McAfee Vulnerability Manager appliance. STRM supports McAfee Vulnerability Manager versions 6.8 or 7.0.

After you configure the McAfee Foundstone Enterprise system and the McAfee Vulnerability Manager scanner in STRM, you can schedule a scan. Scan schedules allow you to determine the frequency with which STRM requests data from your McAfee appliance. For more information, see [Manage Scan Schedules](#).

The following data collection options are available for McAfee Vulnerability Manager:

- **Remote XML Import** - Allows STRM to connect to a remote server and import the XML vulnerability data created by your McAfee Vulnerability Manager appliance. This allows you to configure your McAfee Vulnerability Manager to publish or export your scan results to a remote server, then import the XML data. STRM connects to the repository using SFTP and imports completed scan report files from the remote directory.
- **SOAP API** - Allows STRM to use the McAfee OpenAPI to retrieve completed vulnerability scan data. To retrieve scan data using the Open API, you must specify the configuration name for the live scan data you want to retrieve. As the live scan runs, STRM updates the percentage complete in the scan status. After the live scan completes, STRM retrieves the data and updates the vulnerability assessment information for your assets.

Add a McAfee Vulnerability Manager Scanner

The McAfee Vulnerability Manager scanner module for STRM provides several collection types for retrieving vulnerability data from your server.

- [Configure a Remote XML Import](#)
- [Configure a OpenAPI Scan](#)

Configure a Remote XML Import

Remote XML importing allow you to retrieve your McAfee Vulnerability Manager data from a remote server. The data is retrieved using SFTP.

To add a McAfee Vulnerability Manager scanner using XML Import:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 17-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select McAfee Vulnerability Manager . |

- Step 6** From the **Collection Type** list box, select **Remote XML Import**.

- Step 7** Configure values for the following parameters:

Table 17-2 McAfee Remote XML Import Parameters

| Parameter | Description |
|-----------------|--|
| Remote Hostname | Type the IP address or hostname of the remote server hosting your McAfee Vulnerability Manager XML data. If the server process and the client are located on the same host, you can use localhost as the server hostname. |
| Server Remote | Type the port for the remote host to retrieve the XML vulnerability data using SFTP. The default is port 22. |
| Login Username | Type the username that STRM can use to authenticate with the remote server. |

Table 17-2 McAfee Remote XML Import Parameters (continued)

| Parameter | Description |
|---------------------------|--|
| Enable Key Authentication | <p>Select this check box to enable public or private key authentication.</p> <p>If the check box is selected, STRM attempts to authenticate the connection using the private key that is provided and the Login Password field is ignored.</p> |
| Login Password | <p>Type the password that corresponds to the username for the remote server.</p> <p>Note: Your server password must not contain the ! character. This character could cause authentication failures over SFTP.</p> |
| Remote Directory | Type the directory location of the scan result files. |
| File Name Pattern | <p>Type a regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing.</p> <p>For example, if you want to list all files ending with XML, use the following entry:</p> <p><code>.*\ .xml</code></p> <p>Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/</p> |
| Max Report Age (Days) | <p>Type the maximum file age to include when importing your XML result file during a scheduled scan. By default, the results file maximum age is 7 days.</p> <p>Files that are older than the specified days and timestamp on the report file are excluded from the scheduled import.</p> |

Step 8 To configure the CIDR ranges you want this scanner to consider:

- a** In the text field, type 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 9 Click **Save**.

On the **Admin** tab, select **Deploy Changes**.

The configuration is complete. You are now ready to add a scan schedule to determine the frequency with which STRM imports XML data from your McAfee Vulnerability Manager appliance.

Configure a OpenAPI Scan

Your McAfee Foundstone Enterprise system must include a configuration appropriate for STRM and a scan that runs regularly ensures the results are 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 user interface for STRM to retrieve the scan results. If the scan is not displayed in the McAfee Foundstone Enterprise user interface or is scheduled to be removed after completion, STRM needs to retrieve the results before the scan is removed or the scan fails.
- The appropriate user privileges must be configured in the McAfee Foundstone Configuration Manager application, which allows STRM to communicate with McAfee Foundstone Enterprise.

Since the FoundScan OpenAPI only provides host and vulnerability information to STRM, your Asset Profile information displays 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 [Configure Certificates](#).

To add a McAfee Vulnerability Manager scanner:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 17-3 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |

Table 17-3 Scanner Parameters (continued)

| Parameter | Description |
|--------------|---|
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select McAfee Vulnerability Manager . |

Step 6 From the **Collection Type** list box, select **Open API Import**.

Step 7 Configure values for the following parameters:

Table 17-4 McAfee Open API Import Parameters

| Parameter | Description |
|--------------------|--|
| SOAP API URL | Type the web address for the Foundscan Open API in the following format: <code>https://<IP address>:<SOAP port></code> 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 <code>https://localhost:3800</code> . |
| Customer Name | Type 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 | Type 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 | Type the password corresponding to the Login User Name for access to the Open API. |
| Client IP Address | Type 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. Type the portal name. This field can be left blank for STRM purposes. See your McAfee Vulnerability Manager administrator for more information. |
| Configuration Name | Type the scan configuration name that exists in McAfee Foundstone Enterprise and to which the user has access. |
| CA Truststore | Type the directory path and filename for the CA truststore file. The default is <code>/opt/qradar/conf/mvm.keystore</code> . Note: For more information on certificates for McAfee Vulnerability Manager, see Configure Certificates . |

Table 17-4 McAfee Open API Import Parameters (continued)

| Parameter | Description |
|--------------------------------------|---|
| Client Keystore | Type the directory path and filename for the client keystore. The default is /opt/qradar/conf/mvm.truststore. <i>Note: For more information on certificates for McAfee Vulnerability Manager, see Configure Certificates.</i> |
| McAfee Vulnerability Manager Version | From the list box, specify the version of your McAfee Vulnerability Manager software. |

Step 8 To configure the CIDR ranges you want this scanner to consider:

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

The McAfee Vulnerability Manager can only accept CIDR addresses to a 0/0 subnet that is added as 0.0.0.0/0. CIDR addresses added that end in 0/0 are no longer accepted in the configuration. This is due to limitations of the McAfee OpenAPI.

- b Click **Add**.

Step 9 Click **Save**.

Step 10 On the **Admin** tab, select **Deploy Changes**.

The configuration is complete. You are now ready to add a scan schedule to determine the frequency with which STRM imports data from your McAfee Vulnerability Manager appliance.

Edit a McAfee Vulnerability Manager Scanner

To edit an McAfee Vulnerability Manager scanner configuration in:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window is displayed.
- Step 6** Update parameters, as necessary.
 - For Remote XML Import parameters, see [Table 17-2](#).
 - For OpenAPI parameters, see [Table 17-4](#).

Step 7 Click **Save**.

Step 8 On the **Admin** tab, select **Deploy Changes**.

Delete a McAfee Vulnerability Manager Scanner

To delete a McAfee Vulnerability Manager scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, select **Deploy Changes**.

Configure 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>.

Generate Certificates To obtain the necessary certificates:

Step 1 Run the Foundstone Certificate Manager.

Step 2 Click the **Create SSL Certificates** tab.

Step 3 Configure the host address for STRM.

If you are using a remote Event Collector, the certificate must be generated using the host address of the remote Event Collector.

Step 4 Optional. Click **Resolve**.

We recommend entering an IP address into the host address field if you receive an error from the Foundstone Certificate Manager.

If you do not resolve the host name, see [Step 6](#).

Step 5 Click **Create Certificate Using Common Name**.

Step 6 Click **Create Certificate Using Host Address**.

McAfee Certificate Manager Tool creates a zip file, and provides a certificate passphrase.

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 accessible location.

We recommend that you save this pass phrase for future use. If you misplace your pass phrase from [Step 8](#), you must create new certificates.

You are now ready to process the certificates for STRM.

Process Certificates To process the certificates:

Step 1 Extract the zip file containing the certificates from [Step 7](#) to a directory on your McAfee Vulnerability Manager.

Step 2 From the Juniper customer support or <http://www.ibm.com/support> website, download the following files to the same directory as the extracted certificate files.

`VulnerabilityManager-Cert.bat.gz`

`qllabs_vis_mvm_cert.jar`

Step 3 Type the following command to extract the gz file:

`gzip -d VulnerabilityManager-Cert.bat.gz`

Step 4 Run the `VulnerabilityManager-Cert.bat` command including the file path to your Java™ home directory.

For example:

`VulnerabilityManager-Cert.bat "C:\Program Files\Java\jdk1.6.0_20"`

Quotation marks are required when specifying your Java™ home directory for the batch file.

If `VulnerabilityManager-Cert.bat` can not find the Java™ files cannot be located by the batch file, an error is generated.

Step 5 When prompted, type the pass phrase provided in [Step 6](#).

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

Keystore File Created

Truststore File Created

You are now ready to import the certificates into STRM. See [Import Certificates](#).

Import Certificates 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.

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

Step 1 To import the certificates, secure copy both **mvm.keystore** and **mvm.truststore** files to the following directories in STRM:

```
/opt/qradar/conf
/opt/qradar/conf/trusted_certificates
```

Depending on your configuration, your system might not contain the /opt/qradar/conf/trusted_certificates directory. If this directory does not exist, do not create the directory and you can ignore the file copy to /opt/qradar/conf/trusted_certificates.

Step 2 Log in to STRM.

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

Where <IP Address> is the IP address of the STRM Console.

Step 3 Click the **Admin** tab.

The Administration tab is displayed.

Step 4 On the **Admin** tab, select **Advanced > Deploy Full Configuration**.

Selecting Deploy Full Configuration restarts STRM services, resulting in a gap in data collection for events and flows until the deployment completes.

18

MANAGE SAINT SCANNERS

You can integrate a Security Administrator's Integrated Network Tool (SAINT) vulnerability scanner with STRM using SAINT version 7.4.x.

Using STRM, you can schedule and launch SAINT vulnerability scans or you can generate reports using existing vulnerability data. The SAINT scanner identifies vulnerabilities based on the specified scan level and uses SAINTwriter to generate custom reports for STRM. Therefore, your SAINT system must include a SAINTwriter report template that is appropriate for STRM and a scan that runs regularly to ensure results are current.

To integrate STRM with a SAINT scanner, you must have appropriate administrative access to STRM and your SAINT appliance. You must also ensure that firewalls are configured to allow a communication between your SAINT appliance and STRM. For more information, see your product documentation.

After you configure the SAINTwriter, you can schedule a scan. Scan schedules allow you to determine the frequency with which STRM requests data from your SAINT appliance. For more information, see [Manage SAINT Scanners](#).

Configure a SAINTwriter Report Template

To configure a SAINTwriter report template:

- Step 1** Log in to the SAINT user interface.
- Step 2** Select **Data > SAINTwriter**.
- Step 3** Click **Type**.
- Step 4** From the list box, select **Custom**.
- Step 5** In the **File Name** field, specify a configuration file name.
The configuration file name must correspond to the STRM Saint Writer Config parameter in [Table 18-2](#).
- Step 6** In the **Template Type** list box, select **Technical Overview**.
- Step 7** Click **Continue**.
The Category menu is displayed.

- Step 8** Select **Lists**.
- Step 9** In **Columns to include in host list**, change any column marked None to **MAC Address**.
- Step 10** In the **Columns to include in vulnerability list**, change any column marked as None to **Port**.
- Step 11** In the **Columns to include in vulnerability list**, change any column marked as None to **Service**.
- Step 12** Click **Save**.
- You are now ready to add a SAINT vulnerability scanner to STRM.

Add a SAINT Scanner

To add a SAINT vulnerability scanner to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.
- Step 5** Configure values for the following parameters:

Table 18-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select SAINT Scanner . |

- Step 6** Configure values for the following parameters:

Table 18-2 SAINT Scanner Parameters

| Parameter | Description |
|-----------------|---|
| Remote Hostname | Type the host name or IP address of the system hosting the SAINT scanner. |
| Login Username | Type the username used by STRM to authenticate the SSH connection. |

Table 18-2 SAINT Scanner Parameters (continued)

| Parameter | Description |
|--------------------------|---|
| Enable Key Authorization | <p>Select this check box to enable public/private key authentication.</p> <p>If the check box is selected, STRM attempts to authenticate the SSH connection using the provided private key and the Login Password parameter is ignored. By default, the check box is clear. For more information, see your SSH documentation for configuring public key authentication.</p> |
| Login Password | <p>Type the password associated with the Login Username for SSH access.</p> <p>If Enable Key Authentication is enabled, this parameter is ignored.</p> |
| Private Key File | <p>Type 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 <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 type another file name.</p> <p>This parameter is mandatory if the Enable Key Authentication check box is selected. If the Enable Key Authentication check box is clear, this parameter is ignored.</p> |
| SAINT Base Directory | Type the path to the install directory for SAINT. |
| Scan Type | <p>You can configure a scanner to retrieve SAINT data using a Live Scan or you can select Report Only.</p> <p>From the list box, select the collection type:</p> <ul style="list-style-type: none"> • Live Scan - Launches a vulnerability scan and generates report data from the scan results based on the session name. • Report Only - Generates a scan report based on the session name. |
| Ignore Existing Data | <p>This option only applies when Live Scan is the selected scan type. This option indicates if the live scan ignores existing data and gathers new vulnerability information from the network.</p> <p>If the Ignore Existing Data check box is selected, the SAINT scanner removes existing session data before a live scan launches. By default, the check box is clear.</p> |

Table 18-2 SAINT Scanner Parameters (continued)

| Parameter | Description |
|---------------------|---|
| Scan Level | Select the scan level using the list box: <ul style="list-style-type: none"> • Vulnerability Scan - Scans for all vulnerabilities. • Port Scan - Scans for TCP and UDP services listening on the network. • PCI Compliance Scan - Scans ports and services with emphasis on DSS PCI compliance. • SANS Top 20 Scan - Scans for the top 20 most critical security vulnerabilities. • FISMA Scan - Scans for all vulnerabilities and including all custom scans and PCI levels. |
| Session Name | Type the session name for the SAINT scanner session configuration. |
| SAINT Writer Config | Type the configuration file name for SAINTwriter. |

- Step 7** To configure the CIDR ranges you want this scanner to consider:
- In the text field, type 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** On the **Admin** tab, click **Deploy Changes**.

Edit a SAINT Scanner

To edit an SAINT vulnerability scanner in STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window is displayed.
- Step 6** Update parameters, as necessary. See [Table 18-2](#).
- Step 7** Click **Save**.
- Step 8** On the **Admin** tab, click **Deploy Changes**.

Delete a SAINT Scanner

To delete a SAINT vulnerability scanner from STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window is displayed.
- Step 6** Click **OK**.
- Step 7** On the **Admin** tab, click **Deploy Changes**.

19

MANAGE AXIS SCANNERS

The Asset Export Information Source (AXIS) scanner allows STRM to retrieve scan results from unknown scanner devices for correlation.

This allows AXIS to be used for importing scan results for devices created by scanner vendors that supply vulnerabilities in an XML format that complies with the AXIS format schema. This allows vendors of scanner products and software to create a generic format that is compatible with STRM. The AXIS scanner for STRM is designed to periodically retrieve the scan results in XML format and interpret the scanned data. STRM monitors the server for updates to the scan results and downloads the latest results for processing. STRM only supports scan results the AXIS XML format.

To successfully integrate an AXIS scanner with STRM, the XML results files must be read from a remote server using SFTP or the scanner creating the results file, if the scanner itself supports access using SFTP. The term remote server refers to a system or 3rd party appliance to host the XML scan results that is separate from STRM.

The scan results contain identification information regarding the scan configuration from the unknown scanner device. The most recent scan results are used when a new scan is requested from STRM. Scan schedules allow you to determine the frequency with which STRM requests data from your AXIS-compatible scanner. For more information, see [Manage Scan Schedules](#).

Add an AXIS Scanner

To add an AXIS scanner to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 19-1 AXIS Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Axis Scanner . |

Step 6 Configure values for the following parameters:

Table 19-2 AXIS Scanner Parameters

| Parameter | Description |
|--------------------------|---|
| Remote Hostname | Type the hostname or IP address of the remote server. |
| Login Username | Type the username used by STRM to authenticate the SFTP connection. |
| Login Password | <p>If Enable Key Authentication is disabled, you must type the password corresponding to the Login Username parameter that STRM uses to authenticate the SFTP connection.</p> <p>If Enable Key Authentication is enabled, the Login Password parameter is ignored.</p> |
| Enable Key Authorization | <p>Select this check box to enable private key authorization for the server.</p> <p>If the check box is selected, the authentication is completed using a private key and the password is ignored. The default value is disabled.</p> |
| Private Key File | <p>Type the directory path to the file that contains the private key information. If you are using key-based authentication, STRM uses the private key to authenticate the 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 type another file name.</p> <p>This parameter is mandatory if the Enable Key Authentication check box is selected. If the Enable Key Authentication check box is clear, this parameter is ignored.</p> |
| Remote Directory | Type the directory location of the scan result files. |

Table 19-2 AXIS Scanner Parameters (continued)

| Parameter | Description |
|-----------------------|---|
| File Name Pattern | <p>Type a regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing.</p> <p>For example, if you want to list all files ending with XML, use the following entry:</p> <p><code>. * \ . xml</code></p> <p>Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/</p> |
| Max Report Age (Days) | <p>Type the maximum file age to include when importing your XML result file during a scheduled scan. By default, the results file maximum age is 7 days.</p> <p>Files that are older than the specified days and timestamp on the report file are excluded from the scheduled import.</p> |
| Ignore Duplicates | <p>Select this check box to track files that have already been processed and you do not want the files to be processed a second time.</p> <p>Note: <i>If a result file is not seen for 10 days, it is removed from the tracking list and is processed the next time the file is discovered.</i></p> |

Step 7 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 On the **Admin** tab, click **Deploy Changes**.

Edit an AXIS Scanner

To edit an AXIS scanner configuration in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to edit.

Step 5 Click **Edit**.

The Edit Scanner window is displayed.

Step 6 Update parameters, as necessary. See [Table 19-2](#).

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Delete an AXIS Scanner

To delete an AXIS scanner from STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The VA Scanners window is displayed.

Step 4 Select the scanner you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

20

MANAGE TENABLE SECURITYCENTER SCANNERS

A Tenable SecurityCenter scanner can be used with STRM to schedule and retrieve any open vulnerability scan report records from multiple Nessus vulnerability scanners on your network.

STRM accesses the Tenable SecurityCenter remotely using an HTTPS connection.

After you have added the Tenable SecurityCenter scanner in STRM, you can schedule a scan to retrieve open vulnerability report records. Scan schedules allow you to determine the frequency with which STRM requests data from your Tenable SecurityCenter appliance. For more information, see [Manage Scan Schedules](#).

Add a Tenable SecurityCenter Scanner

To add Tenable SecurityCenter to STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Click **Add**.
The Add Scanner window is displayed.

Step 5 Configure values for the following parameters:

Table 20-1 Scanner Parameters

| Parameter | Description |
|--------------|---|
| Scanner Name | Type the name you want to assign to this scanner. The name can be up to 255 characters in length. |
| Description | Type a description for this scanner. The description can be up to 255 characters in length. |
| Managed Host | From the list box, select the managed host you want to use to configure the scanner. |
| Type | From the list box, select Tenable Security Center . |

Step 6 Configure values for the parameters:

Table 20-2 Tenable SecurityCenter Parameters

| Parameter | Description |
|----------------|---|
| Server Address | Type the IP address or host name of the Tenable SecurityCenter appliance. |
| API Location | Type the path to the request.php file for your version of Tenable SecurityCenter. By default, the path for accessing the API is <code>sc4/request.php</code> . If you have problems logging in to your Tenable SecurityCenter from STRM, you can verify the file path to your request.php file and update this field. |
| Username | Type the username required to log in to your Tenable SecurityCenter appliance. |
| Password | Type the password that corresponds to the username for your Tenable SecurityCenter appliance. |

Step 7 To configure the CIDR ranges you want this scanner to consider:

- a In the text field, type 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 On the **Admin** tab, click **Deploy Changes**.

Edit a Tenable SecurityCenter Scanner

To edit a previously configured Tenable SecurityCenter scanner in STRM:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to edit.
- Step 5** Click **Edit**.
The Edit Scanner window is displayed.
- Step 6** Update parameters, as necessary. See [Table 20-2](#).
- Step 7** Click **Save**.
- Step 8** On the **Admin** tab, click **Deploy Changes**.

Delete a Tenable SecurityCenter Scanner

To delete Tenable SecurityCenter scanner from STRM:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **VA Scanners** icon.
The VA Scanners window is displayed.
- Step 4** Select the scanner you want to delete.
- Step 5** Click **Delete**.
A confirmation window is displayed.
- Step 6** Click **OK**.
- Step 7** On the **Admin** tab, click **Deploy Changes**.
If you selected SNMPv3 as your eEYe configuration with AES192 or AES256 encryption, you must install an additional Java™ component on your STRM Console or Event Collector.

Install the Java Cryptography Extension

The Java™ Cryptography Extension (JCE) is a Java™ framework that is required for STRM to decrypt advanced cryptography algorithms for AES192 or AES256.

The following information describes how to install Oracle JCE on STRM. Depending on your configuration, you might require the JCE to communication with STRM

To install the Unrestricted JCE Policy Files on STRM.

- Step 1** Download the latest version of the Java™ Cryptography Extension:
<https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk>
There may be several versions of the JCE available for download. The version you download should match the version of the Java™ installed on STRM.

Step 2 Extract the JCE file.

The following archive files are included in the JCE download:

- local_policy.jar
- US_export_policy.jar

Step 3 Using SSH, log in to your STRM Console or managed host as a root user.

Username: `root`

Password: `<password>`

Step 4 Copy the JCE jar files to the following directory on your STRM Console or managed host:

```
/opt/ibm/java-x86_64-60/jre/lib/security/US_export_policy.jar
```

```
/opt/ibm/java-x86_64-60/jre/lib/security/local_policy.jar
```

The jar files are only copied to the system receiving the AES192 or AE256 encrypted files. Depending on your configuration, this could be your STRM Console or a managed host.

The installation of the Java™ Cryptography Extension for STRM is complete. You are now ready to schedule a scan for your eEye scanner in STRM. For more information, see [Manage Scan Schedules](#).

21

MANAGE SCAN SCHEDULES

After you have configured the individual scanners to allow STRM to access the client or appliance for vulnerability data, you must create a schedule for STRM to retrieve vulnerability data.

A scan schedule can be ran once or configured to retrieve vulnerability data on a reoccurring basis. When a scan schedule completes, STRM is updated with the latest vulnerability data.

You can manage scan schedules from the **Admin** tab or the **Assets** tab in STRM.

View Scheduled Scans

The Scan Scheduling window displays when STRM is scheduled to collect vulnerability assessment data from vulnerability appliances on your network. The name of each scan is displayed, along with the CIDR range, port or port range, priority, potency, status, concurrency mask, and next run time.

To view scheduled scans:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **Schedule VA Scanners** icon.

The Scan Scheduling is displayed.

The following information is provided for each scheduled scan:

Table 21-1 Scheduled Scan Parameters

| Parameter | Description |
|------------|--|
| VA Scanner | Displays the name of the schedule scan. |
| CIDR | Displays the IP address(es) to be included in this scan. |

Table 21-1 Scheduled Scan Parameters (continued)

| Parameter | Description |
|-----------|---|
| Ports | <p>Displays the port range 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, nCircle IP360 and Qualys scanners report vulnerabilities on all ports, but require you to specify what port information to pull from the full report for display in the user interface.</p> |
| Priority | <p>Displays the priority of the scan.</p> <p>Scheduled scans with a high priority are queued above in priority and run before low priority scans.</p> |
| Potency | <p>Displays 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 - Indicates a safe, non-intrusive assessment. They can generate false results. • Safe - Indicates an intermediate assessment and produces safe, banner-based results. • Medium - Indicates a safe intermediate assessment with accurate results. • Somewhat safe - Indicates an intermediate assessment but can leave service unresponsive. • Somewhat unsafe - Indicates an intermediate assessment, however, can result in your host or server cease functioning. • Unsafe - Indicates an intermediate assessment, however, this can cause your service to become unresponsive. • Very unsafe - Indicates an unsafe, aggressive assessment that can result in your host or server becoming unresponsive. <p>Note: Potency levels only apply to NMap scanners. We recommend you select Medium from the Potency list box for most NMap scans.</p> |

Table 21-1 Scheduled Scan Parameters (continued)

| Parameter | Description |
|------------------|---|
| Status | <p>Displays the status of the scan. A descriptive status message is displayed by holding the mouse (hovering over) the status message:</p> <ul style="list-style-type: none"> • New - Indicates the schedule scan entry is newly created. When the status is New, you can edit the scan entry. When 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 - Indicates the scan has been placed in the job queue. The status remains Pending until removed from the queue by the scanner module, or the status is changed to percentage (%) complete or failed. 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. Percentage Complete indicates the percentage (%) complete status for the scan as a numeric value. • Complete - When Percentage Complete reaches 100%, the scan status changes to complete. • Failed - Indicates an error has occurred in the scan process. <p>Note: Place your mouse over any scanner to view detailed information about errors or live scans that might be in progress.</p> |
| Concurrency Mask | Displays the size of the subnet scanned during a Vulnerability Assessment (VA) scan. |
| Next Run Time | <p>Displays a countdown timer to indicate the interval until the next vulnerability scan is scheduled to start.</p> <p>If the scan is scheduled with an interval of 0, this indicates the scan is not scheduled to repeat. Scans that do not repeat display the next run time as N/A.</p> <p>The Next Run Time updates when the Scan Scheduling window refreshes.</p> |

Schedule a Scan

After you have configured vulnerability scanners in STRM, then you are ready to create a scan schedule.

Scan schedules are created for each scanner product in your network and are used to retrieve vulnerability data for STRM.

To schedule a Vulnerability Assessment scan:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **Schedule VA Scanners** icon.
The Scan Scheduling window is displayed.
- Step 4** Click **Add**.
The Add Schedule window is displayed.

If you do not have any scanners configured, an error message is displayed. You must configure the scanner before you can schedule a scan.

- Step 5** Configure values for the following parameters:

Table 21-2 Scan Schedule Parameters

| Parameter | Description |
|--------------|--|
| VA Scanner | From the list box, select the scanner for which you want to create a schedule. |
| Network CIDR | <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Network CIDR - Select the option and select the network CIDR range to which you want this scan to apply. • Subnet/CIDR - Select the option and type the subnet or CIDR range to which you want this scan to apply. The subnet/CIDR must be within the selected Network CIDR. <p>The Network CIDR or Subnet/CIDR values must be available by the scanner selected in the VA Scanner list box.</p> |

Table 21-2 Scan Schedule Parameters (continued)

| Parameter | Description |
|------------|---|
| Potency | <p>From the Potency list box, select the level of scan that you want to perform. The precise interpretation of the levels depends on the scanner. For more precise potency information, see your vendor documentation. In general, the potency levels indicate the aggressiveness of the scan:</p> <ul style="list-style-type: none"> • Very safe - Indicates a safe, non-intrusive assessment. They can generate false results. • Safe - Indicates an intermediate assessment and produces safe, banner-based results. • Medium - Indicates a safe intermediate assessment with accurate results. • Somewhat safe - Indicates an intermediate assessment but can leave service unresponsive. • Somewhat unsafe - Indicates an intermediate assessment, however, can result in your host or server cease functioning. • Unsafe - Indicates an intermediate assessment, however, this can cause your service to become unresponsive. • Very unsafe - Indicates an unsafe, aggressive assessment that can result in your host or server becoming unresponsive. <p>Note: Potency levels only apply to NMap scanners.</p> |
| Priority | <p>From the Priority list box, select the priority level to assign to the scan.</p> <ul style="list-style-type: none"> • Low - Indicates the scan is of normal priority. Low priority is the default scan value. • High - Indicates the scan is high priority. High priority scans are always placed above low priority scans in the scan queue. |
| Ports | Type the port range you want the scanner to scan. |
| Start Time | <p>Configure the start date and time for the scan. The default is the local time of your STRM.</p> <p>Note: If you select a start time that is in the past, the scan begins immediately after saving the scan schedule.</p> |
| Interval | <p>Type a time interval to indicate how often you want this scan to run. Scan intervals can be scheduled by the hour, day, week, or month.</p> <p>An interval of 0 indicates that the scheduled scan runs one time and does not repeat.</p> |

Table 21-2 Scan Schedule Parameters (continued)

| Parameter | Description |
|---------------------------|--|
| Concurrency Mask | Type a CIDR range to specify the size of the subnet to be scanned during a vulnerability scan. The value configured for the concurrency mask represents the largest portion of the subnet that the scanner is allowed to scan at a time. Concurrency mask allows the entire network CIDR or subnet/CIDR to be scanned in subnet segments to optimize the scan. The maximum subnet segment scan is /24 and the minimum subnet segment scan is /32. |
| Clean Vulnerability Ports | Select this check box if you want the scan to exclude previous collected vulnerability data. |

Step 6 Click **Save**.

Edit a Scan Schedule

After you create a new scan schedule, you can edit the parameters of the scan schedule.

Editing a scan schedule is only possible before you deploy the configuration in STRM. After configuration changes are deployed in STRM, the edit button is unavailable and you are no longer able to edit a scan schedule.

To edit a Vulnerability Assessment scan schedule:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.
- Step 3** Click the **Schedule VA Scanners** icon.
The Scan Scheduling window is displayed.
- Step 4** Select the schedule you want to edit.
- Step 5** Click **Edit**.
The Edit Schedule window is displayed.
- Step 6** Update values, as necessary. See [Table 21-2](#).
- Step 7** Click **Save**.

Delete a Scan Schedule

To delete a schedule Vulnerability Assessment scan:

- Step 1** Click the **Admin** tab.
- Step 2** On the navigation menu, click **Data Sources**.
The Data Sources pane is displayed.

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

The VA Scanners is displayed.

Step 4 Select the scan you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

22 SUPPORTED SCANNERS

Table 22-1 provides information on the vulnerability assessment scanners STRM supports.

STRM integrates with many manufacturers and vendors of security products. Our list of supported scanners and documentation is constantly increasing. If your scanner is not listed in this document, contact your sales representative.

Table 22-1 Supported Vulnerability Assessment Scanners

| Manufacturer | Scanner | Version | Option in STRM | Connection Type |
|-----------------------|---------------------------------|--|------------------------------|--|
| Beyond Security | AVDS | AVDS Management v12 (minor version 129) and above | Beyond Security AVDS Scanner | File import of vulnerability data using SFTP |
| eEye Digital Security | eEye REM or eEye Retina CS | REM v3.5.6 or Retina CS v3.0 to v4.0 | eEye REM Scanner | SNMP trap |
| Generic | AXIS | N/A | Axis Scanner | File import of vulnerability data using SFTP |
| IBM | InfoSphere Guardium | v9.0 and above | IBM Guardium SCAP Scanner | File import of vulnerability data using SFTP |
| IBM | IBM Security AppScan Enterprise | AppScan Enterprise 8.6 | IBM AppScan Scanner | IBM REST web service using HTTP or HTTPS |
| IBM | SiteProtector | SiteProtector v2.9.x | IBM SiteProtector Scanner | JDBC polling |
| IBM | Tivoli EndPoint Manager | IBM Tivoli EndPoint Manager v8.2.x | IBM Tivoli EndPoint Manager | SOAP-based API using HTTP or HTTPS |
| Juniper | NSM Profiler | 2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1, and 2010.x | Juniper NSM Profiler Scanner | JDBC polling |
| Lumenison | Patchlink | 6.4.4 and above | Lumenison Patchlink Scanner | SOAP-based API using HTTPS |
| McAfee | Foundstone | 5.0 to 6.5 | Foundscan Scanner | SOAP-based API using HTTPS |
| | Vulnerability Manager | 6.8 or 7.0. | McAfee Vulnerability Manager | SOAP-based API using HTTPS |

Table 22-1 Supported Vulnerability Assessment Scanners (continued)

| Manufacturer | Scanner | Version | Option in STRM | Connection Type |
|---------------------|----------------|---|--------------------------|--|
| nCircle | ip360 | VnE Manager 6.5.2 to 6.8.28 | nCircle ip360 Scanner | File import of vulnerability data using SFTP |
| Nessus | Nessus | Linux 4.0.2 to 4.4.x, Windows 4.2 to 4.4.x | Nessus Scanner | File import using SFTP and SSH command execution |
| | Nessus | Linux 4.2 to 5.x, Windows 4.2 to 5.x | Nessus Scanner | Nessus XMLRPC API using HTTPS |
| netVigilance | SecureScout | 2.6 | SecureScout Scanner | JDBC polling |
| Open Source | NMap | 3.7 to 6.0 | NMap Scanner | File import of vulnerability data using SFTP and SSH command execution |
| Qualys | QualysGuard | 4.7 to 7.2 | Qualys Scanner | APIv2 using HTTPS |
| | QualysGuard | 4.7 to 7.2 | Qualys Detection Scanner | API Host Detection List using HTTPS |
| Rapid7 | NeXpose | 4.x to v5.4 | Rapid7 NeXpose Scanner | Remote Procedure Call using HTTPS |
| | | | | Local file import of XML file from a STRM directory |
| Saint Corporation | SAINT | 7.4.x | Saint Scanner | File import of vulnerability data using SFTP and SSH command execution |
| Tenable | SecurityCenter | v4.6.0 | Tenable SecurityCenter | JSON request using HTTPS |

INDEX

A

- audience 9
- AXIS
 - about 125
 - adding 125
 - deleting 128
 - editing 127

B

- Beyond Security AVDS
 - about 17
 - adding 17
 - deleting 20
 - editing 19

C

- conventions 9
- customer support
 - contacting 10

E

- eEye REM Scanner 99
- eEye Retina CS 99
- eEye scanners
 - adding 99
 - deleting 104
 - editing 103

F

- FoundScan
 - adding 78
 - custom certificates 81
 - deleting 80
 - editing 79

I

- IBM AppScan Enterprise
 - about 21
 - adding 24
 - configuring 21
 - deleting 26
 - editing 26
- IBM Guardium
 - about 27
 - adding 27
 - deleting 30
 - editing 29

- IBM SiteProtector

 - about 31
 - adding 31
 - deleting 34
 - editing 33

- IBM Tivoli Endpoint Manager

 - about 35
 - adding 35
 - deleting 37
 - editing 37

- installing scanners 14

- IP360

 - adding 39
 - deleting 42
 - editing 41
 - exporting reports 42

J

- Java Cryptography Extension (JCE) 103, 131

- Juniper NSM Profiler

 - adding 85
 - deleting 87
 - editing 86

M

- McAfee

 - about 109
 - adding OpenAPI scan 112
 - adding remote XML import 110
 - deleting 115
 - editing 114
 - remote XML import 109
 - SOAP API 109
 - using certificates 115

N

- Nessus

 - adding 46, 50
 - deleting 52
 - editing 52

- Nmap

 - adding 58
 - deleting 60
 - editing 60

P

- PatchLink

 - adding 105
 - deleting 107

editing 107

Q

Qualys

about 63

Qualys Detection Scanner 64

adding 64

deleting 67

editing 66

Qualys Scanner

about 68

adding a live scan 68

adding asset report data import 70

adding scheduled scan import 72

deleting 76

editing 75

R

Rapid7 NeXpose

adding 89, 92

deleting 94

editing 93

troubleshooting 91

S

Saint

adding 120

configuring 119

deleting 123

editing 122

scan schedule

adding 136

deleting 138

editing 138

SecureScout

about 95

adding 96

deleting 97

editing 97

Supported vulnerability scanners 141

T

Tenable SecurityCenter

adding 129

deleting 131

editing 130

V

vulnerability assessment

about 13

installing scanners 14

viewing scanners 15