IBM Security QRadar Network Anomaly Detection
Version 7.1.0 (MR2)

Vulnerability Assessment Configuration Guide

Note: Before using this information and the product that it supports, read the information in "Notices and Trademarks" on page 135.

CONTENTS

ABOUT THIS GUIDE

1 OVERVIEW

2 MANAGE BEYOND SECURITY AVDS SCANNERS

3 MANAGE IBM SECURITY APPSCAN ENTERPRISE SCANNERS

4 MANAGE IBM GUARDIUM SCANNERS

5 MANAGE IBM SITEPROTECTOR SCANNERS

12 Manage Juniper Networks NSM Profiler Scanners

13 Manage Rapid7 NeXpose Scanners

14 Manage netVigilance SecureScout Scanners

15 Manage eEye Scanners

16 Manage PatchLink Scanners

17 Manage McAfee Vulnerability Manager Scanners

ABOUT THIS GUIDE

The *IBM Security QRadar Network Anomaly Detection Vulnerability Assessment Configuration Guide* provides you with information on managing vulnerability scanners and configuring scan schedules to work with QRadar Network Anomaly Detection.

Intended audience

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

Conventions

The following conventions are used throughout this guide:

▶ Indicates that the procedure contains a single instruction.

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION: *Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING: *Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical documentation

For information on how to access more technical documentation, technical notes, and release notes, see the **Accessing IBM Security QRadar Network Anomaly Detection Documentation Technical Note.** (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacting customer support

For information on contacting customer support, see the **Support and Download Technical Note**. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

1 OVERVIEW

Vulnerability assessment integration enables QRadar Network Anomaly Detection 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.

QRadar Network Anomaly Detection integration with vulnerability assessment tools allows you to schedule scans to keep your vulnerability assessment data up-to-date.

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

Note: Information found in this documentation about configuring scanners is based on the latest RPM files located at *https://qmmunity.q1labs.com/* or *http://www.ibm.com/support*.

Configure vulnerability assessment

To configure vulnerability assessment scans in QRadar Network Anomaly Detection, 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.

Note: 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 QRadar Network Anomaly Detection. 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 QRadar Network Anomaly Detection 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 Qmmunity website or from *http://www.ibm.com/support*.

To manually install a scanner:

Step 1 Download the scanner rpm file from one of the following websites:

https://qmmunity.q1labs.com/

http://www.ibm.com/support

Step 2 Copy the file to your QRadar Network Anomaly Detection.

Step 3 Using SSH, log in to your QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection.

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

Where <IP Address> is the IP address of the QRadar Network Anomaly Detection.

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 IBM Security QRadar Network Anomaly Detection.

To successfully integrate a Beyond Security AVDS vulnerabilities with QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection when a scan schedule is launched by QRadar Network Anomaly Detection. Scan schedules allow you to determine the frequency with which QRadar Network Anomaly Detection requests data from an AXIS-compatible scanner, such as Beyond Security AVDS. After you add your Beyond Security AVDS appliance to QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection.

Add a Beyond Security AVDS Scanner

To add an Beyond Security AVDS scanner to QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection to authenticate the connection.
Enable Key Authorization	Select this check box to enable private key authorization for the server. 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.
Login Password	If Enable Key Authentication is disabled, you must type the password corresponding to the Login Username parameter that QRadar Network Anomaly Detection uses to authenticate the connection. If Enable Key Authentication is enabled, the Login Password parameter is ignored.
Remote Directory	Type the directory location of the scan result files.
File Name Pattern	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. For example, if you want to list all files ending with XML, use the following entry: `.*\.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/*

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

Parameter	Description
Private Key File	Type the directory path to the file that contains the private key information. If you are using key-based authentication, QRadar Network Anomaly Detection 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. 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.
Max Report Age (Days)	Type the maximum file age to include when importing your XML vulnerabilities file during a scheduled scan. By default, the value is 7 days. Files that are older than the specified days and timestamp on the report file are excluded from the scheduled import.
Ignore Duplicates	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. ***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.*

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 QRadar Network Anomaly Detection:

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

QRadar Network Anomaly Detection 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. QRadar Network Anomaly Detection retrieves AppScan Enterprise reports using the Representational State Transfer (REST) web service to import vulnerability data and generate offenses in QRadar Network Anomaly Detection for your security team.

To integrate AppScan Enterprise with QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection access to report data.
3. Configure your AppScan Enterprise scanner in QRadar Network Anomaly Detection.
4. Create a schedule in QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection.

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

To configure AppScan Enterprise to grant QRadar Network Anomaly Detection access to scan reports:

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

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 QRadar Network Anomaly Detection Integration** - Select this check box to allow users to access the QRadar Network Anomaly Detection integration options for AppScan Enterprise.
- **Publish to QRadar Network Anomaly Detection** - Select this check box to allow QRadar Network Anomaly Detection access to published scan report data.
- **QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection integration with AppScan Enterprise.

Enable QRadar Network Anomaly Detection integration

To complete these steps, you must be logged in as a user with the Configuration QRadar Network Anomaly Detection Integration user type enabled.

To enable AppScan Enterprise with QRadar Network Anomaly Detection:

Step 1 Click the **Administration** tab.

Step 2 On the navigation menu, select **Network Security Systems**.

Step 3 From the QRadar Network Anomaly Detection Integration Settings pane, click **Edit**.

The QRadar Network Anomaly Detection Integration Settings configuration is displayed.

Step 4 Select the **Enable QRadar Network Anomaly Detection Integration** check box.

Any reports previously published to QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, 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.

Note: To add vulnerability information to QRadar Network Anomaly Detection, your Application Deployment Mapping must include an IP address. Any vulnerability data without an IP address is excluded from QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection.

Publish reports to QRadar Network Anomaly Detection

Completed vulnerability reports generated by AppScan Enterprise must be made accessible to QRadar Network Anomaly Detection by publishing the report.

To complete these steps, you must be logged in as a user with the Publish to QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection.

Step 3 On the menu bar of any security report, select **Publish > Grant report access to QRadar Network Anomaly Detection**.

You are now ready to add your AppScan Enterprise scanner to QRadar Network Anomaly Detection.

Configure a scanner in QRadar Network Anomaly Detection

After you have configured AppScan Enterprise and published reports, you can add the AppScan Enterprise scanner in QRadar Network Anomaly Detection.

Adding a scanner allows QRadar Network Anomaly Detection to know which scan reports to collect. You can add multiple AppScan Enterprise scanners in QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection allows you to determine the frequency with which QRadar Network Anomaly Detection imports the scan result data from AppScan Enterprise using the REST web service.

Note: 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 QRadar Network Anomaly Detection 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.
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, `http://myasehostname/ase/`.
Authentication Type	Select an Authentication Type: • **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 QRadar Network Anomaly Detection. You can specify a group of vulnerability reports or an individual report using a regex pattern. By default, the **Report Name Pattern** field contains `.*` as the regex pattern. The .* pattern imports all scan reports that are published to QRadar Network Anomaly Detection. 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 QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection. 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 InfoSphereTM 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. QRadar Network Anomaly Detection can then retrieve the scan results from the remote server storing the vulnerability using SFTP.

Note: 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 QRadar Network Anomaly Detection to import the results from the remote server hosting the vulnerability data. You must add an IBM Guardium scanner to QRadar Network Anomaly Detection and configure the scanner to retrieve data from your remote server. The most recent vulnerabilities are imported by QRadar Network Anomaly Detection when you create a scan schedule. Scan schedules allow you to determine the frequency with which QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection to authenticate the SFTP connection.
Login Password	If Enable Key Authentication is disabled, you must type the password corresponding to the Login Username parameter that QRadar Network Anomaly Detection uses to authenticate the SFTP connection. If Enable Key Authentication is enabled, the Login Password parameter is ignored.
Enable Key Authorization	Select this check box to enable private key authorization for the server. If the check box is selected, the authentication is completed using a private key and the password is ignored. The default value is disabled.
Private Key File	Type the directory path to the file that contains the private key information. If you are using key-based authentication, QRadar Network Anomaly Detection uses the private key to authenticate the connection. 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.
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	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. For example, if you want to list all files ending with XML, use the following entry: `.*\.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/*
Max Report Age (Days)	Type the maximum file age to include when importing your XML result file during a scheduled scan. Files that are older than the specified days and timestamp on the report file are excluded from the scheduled import.

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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to retrieve only the latest information from the RealSecureDB table and import any new vulnerabilities to QRadar Network Anomaly Detection.

When you configure your IBM SiteProtector, we recommend that you create a SiteProtector user account specifically for QRadar Network Anomaly Detection. Creating a user account ensures that QRadar Network Anomaly Detection has the credentials required to poll the IBM SiteProtector database to retrieve vulnerability data. After you create a user account for QRadar Network Anomaly Detection, you should verify communication between QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection, you can create a scan schedule to determine the frequency with which QRadar Network Anomaly Detection polls the IBM SiteProtector database.

To add an IBM SiteProtector scanner in QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection.
Port	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. The JDBC configuration port must match the listener port of the database. The database must have incoming TCP connections enabled to communicate with QRadar Network Anomaly Detection. The default port number for all options include: • **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.

Table 5-2 IBM SiteProtector Scanner Parameters (continued)

Parameter	Description
Domain	Type the domain required, if required, to connect to your IBM SiteProtector database. 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. The domain can be up to 255 alphanumeric characters in length. The domain can include the following special characters: underscore (_), en dash (-), and period(.).
Database Name	Type the name of the database to which you want to connect. The default database name is **RealSecureDB**.
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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection. We recommend that you create a user in IBM Tivoli Endpoint Manager for QRadar Network Anomaly Detection.

Note: QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection, you can create a scan schedule to determine the frequency with which QRadar Network Anomaly Detection accesses IBM Tivoli Access Manager. This allows you to schedule how often QRadar Network Anomaly Detection requests data from IBM Tivoli Endpoint Manager using the SOAP API.

To add an IBM Tivoli Endpoint Manager scanner in QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection.
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 QRadar Network Anomaly Detection Console or managed host to the following directory: `/opt/qradar/conf/trusted_certificates` ***Note:*** *QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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

QRadar Network Anomaly Detection uses SSH to access the remote server (SSH export server) to retrieve and interpret the scanned data.

QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, these XML2 format files must be read from the remote server (using SSH). QRadar Network Anomaly Detection 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. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection.
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	Type the private key path. The private key path is the full directory path on your QRadar Network Anomaly Detection where the private key to be used for SSH key-based authentication is stored. The default path is /opt/qradar/conf/vis.ssh.key, but this file does not exist. You must create a vis.ssh.key file for your remote host or type another file name. If the **Enable Key Authentication** check box is clear, the Private Key Path is ignored.

Note: If the scanner is configured to use a password, the SSH scanner server to which QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection to integrate with your nCircle device.

8 MANAGE NESSUS SCANNERS

QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection. Creating a user account ensures that QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, you should attempt to SSH from QRadar Network Anomaly Detection to your Nessus client to verify QRadar Network Anomaly Detection’s credentials. This ensures that QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to connect to a Nessus client and launch a pre-configured scan. QRadar Network Anomaly Detection uses SSH to retrieve the scan report data from the client’s temporary results directory after the live scan completes.
- **Scheduled Results Import** - Allows QRadar Network Anomaly Detection to connect to the location hosting your Nessus scan reports. QRadar Network Anomaly Detection connects to the repository using SSH and imports completed scan report files from the remote directory. QRadar Network Anomaly Detection supports importing Nessus scan reports or scan reports in a Nessus supported output format.
- **Scheduled Live Scan - XMLRPC API** - Allows QRadar Network Anomaly Detection to use the XMLRPC API to start a pre-configured scan. To start a live scan from QRadar Network Anomaly Detection, you must specify the policy name for the live scan data you want to retrieve. As the live scan runs, QRadar Network Anomaly Detection updates the percentage complete in the scan status. After the live scan completes, QRadar Network Anomaly Detection retrieves the data and updates the vulnerability assessment information for your assets.
- **Scheduled Completed Report Import - XMLRPC API** - Allows QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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**.

Note: 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 QRadar Network Anomaly Detection 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 XMLPRC API**
- **Add a Nessus Completed Report Import using the XMLRPC API**

Note: 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, QRadar Network Anomaly Detection downloads the scan data from the temporary directory and updates the vulnerability information for your assets.

To add a Nessus live scan in QRadar Network Anomaly Detection:

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.
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 QRadar Network Anomaly Detection can use to store temporary files. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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.

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

Parameter	Description
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 QRadar Network Anomaly Detection to authenticate the SSH connection.
Client Password	Type the password that corresponds to the **Client Username** field. This field is required if the **Enable Key Authentication** check box is clear. If Enable Key Authentication is enabled, the Login Password parameter is ignored. ***Note:*** *If the scanner is configured to use a password, the SSH scanner server to which QRadar Network Anomaly Detection 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:* `PasswordAuthentication yes.` *If your scanner server does not use OpenSSH, the configuration can differ. For more information, see the vendor documentation for your scanner.*
Enable Key Authentication	Select this check box to enable public or private key authentication. If the check box is selected, QRadar Network Anomaly Detection attempts to authenticate the SSH connection using the private key that is provided and the **SSH Password** field is ignored.

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. QRadar Network Anomaly Detection 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. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection 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.*

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

Parameter	Description
Enable Key Authentication	Select this check box to enable public or private key authentication. If the check box is selected, QRadar Network Anomaly Detection attempts to authenticate the SSH connection using the private key provided and the **SSH Password** field is ignored.
Remote Results Directory	Type the full path for the directory containing the Nessus scan report files on the Nessus client. The directory path uses `./` 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: **.*\.nessus**. 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 XMLPRC API

The XMLRPC API allows QRadar Network Anomaly Detection to start a pre-configured live scan on your Nessus server.

To start a live scan from QRadar Network Anomaly Detection, 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, QRadar Network Anomaly Detection uses the XMLRPC API to retrieve the scan data and update the vulnerability information for your assets.

Note: 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection 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.

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

Parameter	Description
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 “QRadar Network Anomaly Detection Scan”. ***Note:*** *QRadar Network Anomaly Detection does not support using the ampersand (&) character in this field.*
Policy Name	Type the name of a policy on your Nessus server to start a live scan. The policy you define must exist on the Nessus server when QRadar Network Anomaly Detection attempts to launch the scan. If the policy does not exist, then an error is displayed in the status when QRadar Network Anomaly Detection attempts to start the live scan. In most cases the policy name is customized to your Nessus server, but several default policies are included with Nessus. For example, • External Network Scan • Internal Network Scan • Web App Tests • Prepare for PCI DSS audits For more information on policies, see your Nessus vendor documentation.

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 QRadar Network Anomaly Detection to retrieve completed Nessus scan reports from the Nessus server.

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

Note: 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection 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.

Table 8-8 Scheduled Completed Report Import XMLRPC API Parameters (continued)

Parameter	Description
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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection.

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

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

  Several types of Nmap port scans require Nmap to run as root. Therefore, QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection with root access or configure the Nmap binary with setuid root. For assistance, contact your Nmap administrator.
- **Remote Results Import** - Allows QRadar Network Anomaly Detection 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. QRadar Network Anomaly Detection can only import remote results stored in XML format. When configuring your Nmap scanner to generate a file for QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, you can schedule the frequency with which QRadar Network Anomaly Detection imports vulnerability data. For more information, see **Manage Scan Schedules**.

Add an Nmap Remote Live Scan

Adding a Remote Live Scan allows QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection. The scan schedule determines how often QRadar Network Anomaly Detection 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.

Table 9-2 Nmap Live Scan Parameters (continued)

Parameter	Description
Enable Key Authentication	Select this check box to enable QRadar Network Anomaly Detection to use public or private key authentication. Selecting this check box requires you to specify the directory path to your key file on QRadar Network Anomaly Detection 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	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. If you are using SSH key based authentication, QRadar Network Anomaly Detection uses the private key to authenticate the SSH connection. The default directory path 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. This parameter is mandatory if the **Enable Key Authentication** check box is selected, otherwise this parameter is ignored.
Nmap Executable	Type the full directory path and filename of the executable file for the Nmap binary file. The default directory path to the executable file is /usr/bin/Nmap.
Disable Ping	In some networks, the ICMP protocol is partially or completely disabled. In situations where ICMP is not enabled, you 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	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. The options include: **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. **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.
Max RTT Timeout	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). ***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.*

Note: If the scanner is configured to use a password, the SSH scanner server to which QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to launch a live scan on your Nmap scanner. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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.

Table 9-3 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 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 QRadar Network Anomaly Detection to use public or private key authentication. Selecting this check box requires you to specify the directory path to your key file on QRadar Network Anomaly Detection 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	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. If you are using SSH key based authentication, QRadar Network Anomaly Detection uses the private key to authenticate the SSH connection. The default directory path 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. This parameter is mandatory if the **Enable Key Authentication** check box is selected, otherwise this parameter is ignored.
Remote Folder	Type the directory path on the Nmap scanner containing the XML vulnerability data.

Table 9-4 Nmap Remote Results Import Parameters (continued)

Parameter	Description
Remote File Pattern	Type a regular expression (regex) pattern to determine which Nmap XML result 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. For example, the following pattern imports all XML files located in the remote folder: `.*\.xml` ***Note:*** *Scan reports imported and processed by QRadar Network Anomaly Detection are not deleted from the remote folder. We recommend you schedule a cron job to delete previously processed scan reports on a scheduled basis.*

Note: If the scanner is configured to use a password, the SSH scanner server to which QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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

IBM Security QRadar Network Anomaly Detection 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.

QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, you can schedule a scan in QRadar Network Anomaly Detection to collect vulnerabilities using the API or by downloading the scan report. Scan schedules allow you schedule how frequently QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection. This is the **Qualys Vulnerability Retention Period** field. To force QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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	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: • 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	Type the username necessary for requesting scans. This is the same username used to log in to the Qualys server. ***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.*
Qualys Password	Type the password that corresponds to the Qualys Username.
Operating System Filter	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. If you type an invalid regular expression in the **Operating System Filter** field, the scan fails when QRadar Network Anomaly Detection initializes the scanner. To view the error message from a failed scan, move your mouse over the text in the **Status** column.
Asset Group Names	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. 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 QRadar Network Anomaly Detection, to retrieve vulnerability information for both of these assets, type **Building1,Webserver** without spaces in the **Asset Group Names** field. When the scan completes, the **Asset** tab in QRadar Network Anomaly Detection displays vulnerabilities by their IP address. For the example above, QRadar Network Anomaly Detection would display all vulnerabilities for assets 192.168.0.1 and 191.168.255.255.

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 QRadar Network Anomaly Detection. The default is 7 days. If a scan is scheduled and the retention period has expired, QRadar Network Anomaly Detection downloads an updated Qualys Vulnerability Knowledge Base.
Force Qualys Vulnerability Update	Select this check box to force QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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.

CAUTION: *Selecting **Deploy Full Configuration** restarts QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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, QRadar Network Anomaly Detection 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.

***CAUTION:** 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 QRadar Network Anomaly Detection.*

Add a Qualys Scheduled Live Scan Report

Live scans allow QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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: • 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to authenticate with your proxy server.

Table 10-4 Qualys Live Scan Parameters (continued)

Parameter	Description
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.*
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. QRadar Network Anomaly Detection retrieves the completed live scan data after the live scan completes. ***Note:*** *Live scans only support one option profile name per scanner configuration.*

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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to retrieve an asset report from your Qualys scanner. QRadar Network Anomaly Detection determines which asset report to import from the file specified in the **Import File** field. If an import file is not specified, then QRadar Network Anomaly Detection attempts to import the asset report based on the **Report Template Title** field.

To add a Qualys scheduled asset data report import to QRadar Network Anomaly Detection:

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.
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: • 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to authenticate with your proxy server.

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

Parameter	Description
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.
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 QRadar Network Anomaly Detection Console or managed host. For example, to download an asset report named QRadar Network Anomaly Detection_scan.xml from a logs directory on your managed host, type the following: `/qualys_logs/QRadar Network Anomaly Detection_scan.xml` If you specify an import file location, QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to retrieve completed scans from your Qualys scanner.

To add a Qualys scan report data import to QRadar Network Anomaly Detection:

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.

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

Parameter	Description
	For example: • 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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:*** *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.*
Scan Report Name Pattern	Type a file pattern, using a regular expression (regex), for the scan reports you are attempting to import. By default, QRadar Network Anomaly Detection attempts to download all available scan reports using the following file pattern: **.***.

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

Parameter	Description
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.
Import File (Optional)	Optional. Type a directory path to download and import a single scan report from Qualys to your QRadar Network Anomaly Detection Console or managed host. For example, to download a scan report named QRadar Network Anomaly Detection_scan.xml from a logs directory on your managed host, type the following: `/qualys_logs/QRadar Network Anomaly Detection_scan.xml` If you specify an import file location, QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 data 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 QRadar Network Anomaly Detection imports the asset data report from your Qualys scanner. For more information, see **Manage Scan Schedules**.

Editi a Qualys Scanner

To edit a Qualys Scanner configuration in QRadar Network Anomaly Detection:

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.

CAUTION: *Selecting* ***Deploy Full Configuration*** *restarts QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 IBM Security QRadar Network Anomaly Detection allows you 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. QRadar Network Anomaly Detection supports Foundstone FoundScan versions 5.0 to 6.5.

Your FoundScan system must include a configuration appropriate for QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection must be complete and visible in the FoundScan user interface for QRadar Network Anomaly Detection to retrieve the scan results. If the scan is not displayed in the FoundScan user interface or is scheduled to be removed after completion, QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to communicate with FoundScan.

Since the FoundScan OpenAPI only provides host and vulnerability information to QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection to authenticate using client-side certificates. By default, FoundScan includes default certificate authority and client certificates that are the same for all installations. The QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection host. For more information, see **Import certificates**.

After you configure the FoundScan system and the FoundScan scanner in QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection:

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. ***Note:*** *Certificates for your FoundScan scanner must reside on the managed host selected in the* ***Managed Host*** *list box.*
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.`
Customer Name	Type the name of the customer under which the Login User Name belongs.
User Name	Type the user name you want QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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.

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 QRadar Network Anomaly Detection host as the hostname for the certificate.

You are now ready to import the certificate on each QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, see **Add a FoundScan scanner**.

To import certificates to QRadar Network Anomaly Detection:

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.

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

Step 3 On the QRadar Network Anomaly Detection 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.

Step 6 Repeat the certificate import for all managed hosts in your deployment.

The configuration is complete.

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.

QRadar Network Anomaly Detection connects to the Profiler database stored on the NSM server to retrieve these records. The QRadar Network Anomaly Detection server must have access to the Profiler database. QRadar Network Anomaly Detection supports NSM versions 2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1, and 2010.x. For more information, see your vendor documentation.

QRadar Network Anomaly Detection collects data from the PostgreSQL database on the NSM using JDBC. To collect data, QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, you can schedule a scan. Scan schedules allow you to configure the frequency with which QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection from all sites connected to your NeXpose Security Console.

QRadar Network Anomaly Detection supports two methods for importing Rapid7 NeXpose vulnerability data:

- Import Site Data - Adhoc Report via API

  Site data importing allows QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to import scan reports for a site based from a local file downloaded to your QRadar Network Anomaly Detection Console. The Rapid7 NeXpose XML file containing the vulnerability data must be copied from your Radid7 NeXpose appliance to the QRadar Network Anomaly Detection Console or managed host that is performing the local import. You must create a directory on the QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, you can schedule a scan. Scheduling a scan allows you to schedule when QRadar Network Anomaly Detection imports vulnerability data from Rapid7 NeXpose using the API or when QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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. ***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.*
Login Password	Type the password to log in to the Rapid7 NeXpose Security Console.

Table 13-2 Rapid7 NeXpose Parameters (continued)

Parameter	Description
Port	Type the port used to connect to the Rapid7 NeXpose Security Console. ***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.*
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 **.*** 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**.

Note: Since QRadar Network Anomaly Detection imports scan reports from Radip7 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, 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.

Note: 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to import completed vulnerability scans based on completed scan reports copied from your Rapid7 NeXpose scanner to QRadar Network Anomaly Detection.

To configure QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection. QRadar Network Anomaly Detection 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 .*\.xml imports all files located in the import folder. ***Note:*** *Scan reports imported and processed by QRadar Network Anomaly Detection are not deleted from the import folder, but renamed to end in .processed0. We recommend you schedule a cron job to delete previously processed scan reports on a scheduled basis.*

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 QRadar Network Anomaly Detection imports local vulnerability data reports from the local files on the QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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). IBM Security QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection. QRadar Network Anomaly Detection supports SecureScout scanner version 2.6.

To connect QRadar Network Anomaly Detection to the SecureScout database and query for results, you must have appropriate administrative access to QRadar Network Anomaly Detection 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. IBM Security QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection. The database user you create must have select permissions to the following tables:

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

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

After you add the SecureScout scanner in QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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

IBM Security QRadar Network Anomaly Detection supports both eEye REM Security Management Console and eEye Retina CS scanners. eEye scanners use SNMPv1, SNMPv2, or SNMPv3 to send SNMP traps to QRadar Network Anomaly Detection.

To configure eEye scanners with QRadar Network Anomaly Detection, you must:

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

After a scan completes, the results are pushed to QRadar Network Anomaly Detection using SNMP and the results are stored on QRadar Network Anomaly Detection or your managed host in a temporary directory. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, you must configure a scan schedule for your eEye scanner. The scan schedule determines the frequency with which QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to the eEye scanner, you must have administrative access to QRadar Network Anomaly Detection and your eEye appliance. You must also ensure that any firewalls between your eEye scanner and QRadar Network Anomaly Detection allows SNMP traffic.

Add an eEye scanner

To add an eEye REM scanner to QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection.*

Table 15-2 eEye Parameters (continued)

Parameter	Description
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 QRadar Network Anomaly Detection with the latest audits.xml file from your eEye REM or eEye Retina scanner. For more information, see your eEye vendor documentation.*
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: • **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: • **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	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. The decryption algorithms include: • DES • AES128 • AES192 • AES256 The default is DES. ***Note:*** *If you select AES192 or AES256 as your decryption algorithm, you must install additional software for QRadar Network Anomaly Detection. For more information, see* **Install the Java Cryptography Extension***.*
Encryption Password	Type the password used to decrypt SNMP traps. This parameter is required if you are using SNMPv3. ***Note:*** *Your encryption password must include a minimum of 8 characters.*

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 QRadar Network Anomaly Detection. For more information, see **Edit an eEye scanner**, **Step 9**.

The configuration in QRadar Network Anomaly Detection is complete.

If you selected SNMPv3 as your eEYe configuration with AES192 or AES256 encryption, you must install an additional Java^{TM} component on your QRadar Network Anomaly Detection Console or Event Collector.

Install the Java Cryptography Extension

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

The following information describes how to install Oracle JCE on QRadar Network Anomaly Detection.

To install the Unrestricted JCE Policy Files on QRadar Network Anomaly Detection.

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 QRadar Network Anomaly Detection.

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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection Console or a managed host.

The installation of the Java™ Cryptography Extension for QRadar Network Anomaly Detection is complete. You are now ready to schedule a scan for your eEye scanner in QRadar Network Anomaly Detection. For more information, see **Manage Scan Schedules**.

Edit an eEye scanner

To edit an eEye scanner configuration in QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection.

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

CAUTION: *Deploying Full Configuration restarts multiple services on the QRadar Network Anomaly Detection. Event collection is unavailable on QRadar Network Anomaly Detection until the Deploy Full Configuration completes.*

Delete an eEye scanner

To delete an eEye REM scanner from QRadar Network Anomaly Detection:

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 a integrate a PatchLink scanner (version 6.4.4. and above) with IBM Security QRadar Network Anomaly Detection.

The PatchLink scanner queries the PatchLink Scanner Engine using the PatchLink API. QRadar Network Anomaly Detection collects vulnerability data from existing scan results with PatchLink. Therefore, your PatchLink system must include configuration that is appropriate for QRadar Network Anomaly Detection to use and a scan that runs regularly to ensure results are current. Since the API provides access to the PatchLink application, make sure the PatchLink application runs continuously on the PatchLink server.

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

To connect QRadar Network Anomaly Detection to the PatchLink scanner, you must have appropriate administrative access to QRadar Network Anomaly Detection and your PatchLink device. For more information, see your product documentation. Ensure that all firewalls between your PatchLink appliance and QRadar Network Anomaly Detection are configured to allow communications.

After you configure your PatchLink appliance and add a PatchLink scanner in QRadar Network Anomaly Detection, then you are ready to schedule a scan. Scan schedules allow you to determine the frequency with which QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection to use for authenticating the PatchLink engine. The user much 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 QRadar Network Anomaly Detection.
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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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 IBM Security QRadar Network Anomaly Detection allows QRadar Network Anomaly Detection to import vulnerabilities using an XML file or query for a results file using the McAfee OpenAPI.

The McAfee Vulnerability Manager scanner for QRadar Network Anomaly Detection does not start scans remotely, but gathers scan result data after a scan completes on the McAfee Vulnerability Manager appliance. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, you can schedule a scan. Scan schedules allow you to determine the frequency with which QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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. QRadar Network Anomaly Detection connects to the repository using SFTP and imports completed scan report files from the remote directory.
- **SOAP API** - Allows QRadar Network Anomaly Detection 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, QRadar Network Anomaly Detection updates the percentage complete in the scan status. After the live scan completes, QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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.

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

Parameter	Description
Login Username	Type the username that QRadar Network Anomaly Detection can use to authenticate with the remote server.
Enable Key Authentication	Select this check box to enable public or private key authentication. If the check box is selected, QRadar Network Anomaly Detection attempts to authenticate the connection using the private key that is provided and the **Login Password** field is ignored.
Login Password	Type the password that corresponds to the username for the remote server. ***Note:*** *Your server password must not contain the ! character. This character could cause authentication failures over SFTP.*
Remote Directory	Type the directory location of the scan result files.
File Name Pattern	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. For example, if you want to list all files ending with XML, use the following entry: `.*\.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/*
Max Report Age (Days)	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. Files that are older than the specified days and timestamp on the report file are excluded from the scheduled 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**.

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 QRadar Network Anomaly Detection imports XML data from your McAfee Vulnerability Manager appliance.

Configure a OpenAPI scan

Your McAfee Foundstone Enterprise system must include a configuration appropriate for QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection must be complete and visible in the McAfee Foundstone Enterprise user interface for QRadar Network Anomaly Detection 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, QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to communicate with McAfee Foundstone Enterprise.

Since the FoundScan OpenAPI only provides host and vulnerability information to QRadar Network Anomaly Detection, 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. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection. 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.
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: **`https://<IP address>:<SOAP port>`** Where: **`<IP address>`** is the IP address or hostname of the McAfee Foundstone Enterprise Manager Server. **`<SOAP port>`** is the port number for the Open API server's incoming connection. The default is **`https://localhost:3800.`**
Customer Name	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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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.

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

Parameter	Description
CA Truststore	Type the directory path and filename for the CA truststore file. The default is /opt/qradar/conf/mvm.keystore. ***Note:*** *For more information on certificates for McAfee Vulnerability Manager, see* **Configure certificates***.*
Client Keystore	Type the directory path and filename for the client keystore. The default is /opt/qradar/conf/mvm.truststore. ***Note:*** *For more information on certificates for McAfee Vulnerability Manager, see* **Configure certificates***.*
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.

Note: 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection 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^{TM} Software Development Kit (Java^{TM} SDK) must be present on this server for this processing. To obtain the latest Java^{TM} 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 QRadar Network Anomaly Detection.

Note: 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**.

Note: 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.

Note: 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 QRadar Network Anomaly Detection.

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 Qmmunity or *http://www.ibm.com/support* website, download the following files to the same directory as the extracted certificate files.

```
VulnerabilityManager-Cert.bat.gz
q1labs_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"
```

Note: 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 QRadar Network Anomaly Detection. See **Import Certificates**.

Import Certificates

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

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

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

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

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

CAUTION: *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 QRadar Network Anomaly Detection.

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

Where <IP Address> is the IP address of the QRadar Network Anomaly Detection Console.

Step 3 Click the **Admin** tab.

The Administration tab is displayed.

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

CAUTION: *Selecting Deploy Full Configuration restarts QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection using SAINT version 7.4.x.

Using QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection. Therefore, your SAINT system must include a SAINTwriter report template that is appropriate for QRadar Network Anomaly Detection and a scan that runs regularly to ensure results are current.

To integrate QRadar Network Anomaly Detection with a SAINT scanner, you must have appropriate administrative access to QRadar Network Anomaly Detection and your SAINT appliance. You must also ensure that firewalls are configured to allow a communication between your SAINT appliance and QRadar Network Anomaly Detection. 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection.

Add a SAINT scanner

To add a SAINT vulnerability scanner to QRadar Network Anomaly Detection:

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.

Table 18-2 SAINT Scanner Parameters (continued)

Parameter	Description
Login Username	Type the username used by QRadar Network Anomaly Detection to authenticate the SSH connection.
Enable Key Authorization	Select this check box to enable public/private key authentication. If the check box is selected, QRadar Network Anomaly Detection 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.
Login Password	Type the password associated with the Login Username for SSH access. If Enable Key Authentication is enabled, this parameter is ignored.
Private Key File	Type the directory path to the file that contains the private key information. If you are using SSH key-based authentication, QRadar Network Anomaly Detection uses the private key to authenticate the SSH connection. The default is /opt/qradar/conf/vis.ssh.key. However, by default, this file does not exist. You must create the vis.ssh.key file or type another file name. 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.
SAINT Base Directory	Type the path to the install directory for SAINT.
Scan Type	You can configure a scanner to retrieve SAINT data using a Live Scan or you can select Report Only. From the list box, select the collection type: • **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	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. 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.

Table 18-2 SAINT Scanner Parameters (continued)

Parameter	Description
Scan Level	Select the scan level using the list box: • **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:

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 SAINT scanner

To edit an SAINT vulnerability scanner in QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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 IBM Security QRadar Network Anomaly Detection 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 IBM Security QRadar Network Anomaly Detection. The AXIS scanner for QRadar Network Anomaly Detection is designed to periodically retrieve the scan results in XML format and interpret the scanned data. QRadar Network Anomaly Detection monitors the server for updates to the scan results and downloads the latest results for processing. QRadar Network Anomaly Detection only supports scan results the AXIS XML format.

To successfully integrate an AXIS scanner with QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection.

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 QRadar Network Anomaly Detection. Scan schedules allow you to determine the frequency with which QRadar Network Anomaly Detection requests data from your AXIS-compatible scanner. For more information, see **Manage Scan Schedules**.

Add an AXIS scanner

To add an AXIS scanner to QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection to authenticate the SFTP connection.
Login Password	If Enable Key Authentication is disabled, you must type the password corresponding to the Login Username parameter that QRadar Network Anomaly Detection uses to authenticate the SFTP connection. If Enable Key Authentication is enabled, the Login Password parameter is ignored.
Enable Key Authorization	Select this check box to enable private key authorization for the server. If the check box is selected, the authentication is completed using a private key and the password is ignored. The default value is disabled.
Private Key File	Type the directory path to the file that contains the private key information. If you are using key-based authentication, QRadar Network Anomaly Detection 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. 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.
Remote Directory	Type the directory location of the scan result files.

Table 19-2 AXIS Scanner Parameters (continued)

Parameter	Description
File Name Pattern	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. For example, if you want to list all files ending with XML, use the following entry: `.*\.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/*
Max Report Age (Days)	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. Files that are older than the specified days and timestamp on the report file are excluded from the scheduled import.
Ignore Duplicates	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. ***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.*

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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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 IBM Security QRadar Network Anomaly Detection to schedule and retrieve any open vulnerability scan report records from multiple Nessus vulnerability scanners on your network.

QRadar Network Anomaly Detection accesses the Tenable SecurityCenter remotely using an HTTPS connection.

After you have added the Tenable SecurityCenter scanner in QRadar Network Anomaly Detection, you can schedule a scan to retrieve open vulnerability report records. Scan schedules allow you to determine the frequency with which QRadar Network Anomaly Detection requests data from your Tenable SecurityCenter appliance. For more information, see **Manage Scan Schedules**.

Add a Tenable SecurityCenter scanner

To add Tenable SecurityCenter to QRadar Network Anomaly Detection:

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 `sc4/request.php`. If you have problems logging in to your Tenable SecurityCenter from QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection:

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 QRadar Network Anomaly Detection:

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 JavaTM component on your QRadar Network Anomaly Detection Console or Event Collector.

Install the Java Cryptography Extension

The JavaTM Cryptography Extension (JCE) is a JavaTM framework that is required for QRadar Network Anomaly Detection to decrypt advanced cryptography algorithms for AES192 or AES256.

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

To install the Unrestricted JCE Policy Files on QRadar Network Anomaly Detection.

Step 1 Download the latest version of the JavaTM 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 JavaTM installed on QRadar Network Anomaly Detection.

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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection Console or a managed host.

The installation of the JavaTM Cryptography Extension for QRadar Network Anomaly Detection is complete. You are now ready to schedule a scan for your eEye scanner in QRadar Network Anomaly Detection. For more information, see **Manage Scan Schedules**.

21 MANAGE SCAN SCHEDULES

After you have configured the individual scanners to allow IBM Security QRadar Network Anomaly Detection to access the client or appliance for vulnerability data, you must create a schedule for QRadar Network Anomaly Detection 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, QRadar Network Anomaly Detection is updated with the latest vulnerability data.

Note: You can manage scan schedules from the **Admin** tab or the **Assets** tab in QRadar Network Anomaly Detection.

View scheduled scans

The Scan Scheduling window displays when QRadar Network Anomaly Detection 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	Displays the port range included in the scan. 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. 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.
Priority	Displays the priority of the scan. Scheduled scans with a high priority are queued above in priority and run before low priority scans.
Potency	Displays the aggressiveness of the scan. The precise interpretation of the levels depends on the scanner, however, typically, the levels indicate: • **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. ***Note:*** *Potency levels only apply to NMap scanners. We recommend you select* ***Medium*** *from the* ***Potency*** *list box for most NMap scans.*

Table 21-1 Scheduled Scan Parameters (continued)

Parameter	Description
Status	Displays the status of the scan. A descriptive status message is displayed by holding the mouse (hovering over) the status message: • **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%, t the scan status changes to complete. • **Failed** - Indicates an error has occurred in the scan process. ***Note:*** *Place your mouse over any scanner to view detailed information about errors or live scans that might be in progress.*
Concurrency Mask	Displays the size of the subnet scanned during a Vulnerability Assessment (VA) scan.
Next Run Time	Displays a countdown timer to indicate the interval until the next vulnerability scan is scheduled to start. If the scan is scheduled with an interval of 0, this indicates the scan is not schedule to repeat. Scans that do not repeat display the next run time as N/A. The Next Run Time updates when the Scan Scheduling window refreshes.

Schedule a scan

After you have configured vulnerability scanners in QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection.

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.

Note: 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	Choose one of the following options: • **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. The Network CIDR or Subnet/CIDR values must be available by the scanner selected in the **VA Scanner** list box.

Table 21-2 Scan Schedule Parameters (continued)

Parameter	Description
Potency	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: • **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. ***Note:*** *Potency levels only apply to NMap scanners.*
Priority	From the **Priority** list box, select the priority level to assign to the scan. • **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	Configure the start date and time for the scan. The default is the local time of your QRadar Network Anomaly Detection. ***Note:*** *If you select a start time that is in the past, the scan begins immediately after saving the scan schedule.*
Interval	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. An interval of 0 indicates that the scheduled scan runs one time and does not repeat.

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.

Note: Editing a scan schedule is only possible before you deploy the configuration in QRadar Network Anomaly Detection. After configuration changes are deployed in QRadar Network Anomaly Detection, 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 IBM Security QRadar Network Anomaly Detection supports.

QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection	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

Table 22-1 Supported Vulnerability Assessment Scanners (continued)

Manufacturer	Scanner	Version	Option in QRadar Network Anomaly Detection	Connection Type
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
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 5.50	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 QRadar Network Anomaly Detection 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

A NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *www.ibm.com/legal/copytrade.shtml*.

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.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

INDEX