



# Extreme Networks Security Vulnerability Assessment Configuration Guide

Copyright © 2007–2015 All rights reserved.

## Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

[www.extremenetworks.com/company/legal/trademarks/](http://www.extremenetworks.com/company/legal/trademarks/)

## Support

For product support, including documentation, visit: [www.extremenetworks.com/documentation/](http://www.extremenetworks.com/documentation/)

For information, contact:

Extreme Networks, Inc.  
145 Rio Robles  
San Jose, California 95134  
USA

# Table of Contents

---

<b>Introduction to Extreme Security vulnerability assessment configurations.....</b>	<b>5</b>
Conventions.....	5
Providing Feedback to Us.....	6
Getting Help.....	7
Related Publications.....	7
<b>Chapter 1: Vulnerability assessment scanner overview.....</b>	<b>9</b>
Installing the unrestricted Java™ Cryptography Extension.....	9
<b>Chapter 2: AXIS scanner.....</b>	<b>11</b>
Adding an AXIS vulnerability scan.....	11
<b>Chapter 3:</b>	
<b>Beyond Security Automatic Vulnerability Detection System scanner overview.....</b>	<b>13</b>
Adding a Beyond Security AVDS vulnerability scanner.....	13
<b>Chapter 4: Digital Defense Inc AVS scanners.....</b>	<b>15</b>
<b>Chapter 5: eEye scanner overview.....</b>	<b>17</b>
Adding an eEye REM SNMP scan.....	17
Adding an eEye REM JDBC scan.....	18
<b>Chapter 6: Foundstone FoundScan scanner overview.....</b>	<b>20</b>
Adding a Foundstone FoundScan scanner.....	20
Importing certificates for Foundstone FoundScan.....	21
<b>Chapter 7: Security AppScan™ Enterprise scanner overview.....</b>	<b>23</b>
Creating a customer user type for AppScan®.....	23
Enabling integration with AppScan® Enterprise.....	24
Creating an application deployment map in Security AppScan® Enterprise.....	24
Publishing completed reports in IBM AppScan®.....	25
Adding an AppScan® vulnerability scanner.....	25
<b>Chapter 8: IBM® Security Guardium scanner overview.....</b>	<b>27</b>
Adding an IBM Security Guardium® vulnerability scanner.....	27
<b>Chapter 9: IBM® Security SiteProtector™ scanner overview.....</b>	<b>30</b>
Adding an IBM® SiteProtector™ vulnerability scanner.....	30
<b>Chapter 10: Security Tivoli® Endpoint Manager scanner overview.....</b>	<b>32</b>
Adding an IBM Security Tivoli Endpoint Manager vulnerability scanner.....	32
<b>Chapter 11: Juniper Profiler NSM scanner overview.....</b>	<b>34</b>
Adding a Juniper NSM Profiler scanner.....	34
<b>Chapter 12: McAfee Vulnerability Manager scanner overview.....</b>	<b>36</b>
Adding a remote XML import scan.....	36
Adding a McAfee Vulnerability Manager SOAP API scan.....	37
Creating certificates for McAfee Vulnerability Manager.....	38
Processing certificates for McAfee Vulnerability Manager.....	39
Importing certificates for McAfee Vulnerability Manager.....	40
<b>Chapter 13: Microsoft SCCM scanner overview.....</b>	<b>41</b>

<b>Chapter 14: WMI enablement on scanner host.....</b>	<b>42</b>
<b>Chapter 15: Adding a Microsoft SCCM scanner.....</b>	<b>43</b>
<b>Chapter 16: nCircle IP360 scanner overview.....</b>	<b>44</b>
Exporting nCircle IP360 scan results to an SSH server.....	44
Adding a nCircle IP360 scanner.....	45
<b>Chapter 17: Nessus scanner overview.....</b>	<b>46</b>
Adding a Nessus scheduled live scan.....	47
Adding a Nessus scheduled result import.....	49
Adding a Nessus live scan with the XMLRPC API.....	50
Adding a Nessus completed report import with the XMLRPC API.....	51
Adding a Nessus live scan with the JSON API.....	52
Adding a Nessus completed report import with the JSON API .....	53
<b>Chapter 18: netVigilance SecureScout scanner overview.....</b>	<b>55</b>
Adding a netVigilance SecureScout scan.....	55
<b>Chapter 19: Nmap scanner overview.....</b>	<b>57</b>
Adding a Nmap remote result import.....	57
Adding a Nmap remote live scan.....	58
<b>Chapter 20: Outpost24 Vulnerability Scanner overview.....</b>	<b>61</b>
Creating an Outpost24 API authentication token for Extreme Security.....	62
<b>Chapter 21: Positive Technologies MaxPatrol.....</b>	<b>63</b>
Integrating Positive Technologies MaxPatrol with Extreme Security.....	63
Adding a Positive Technologies MaxPatrol scanner.....	64
<b>Chapter 22: Qualys scanner overview.....</b>	<b>66</b>
Adding a Qualys detection scanner.....	66
Adding a Qualys scheduled live scan.....	69
Adding a Qualys scheduled import asset data report.....	70
Adding a Qualys scheduled import scan report.....	71
<b>Chapter 23: Rapid7 NeXpose scanners overview.....</b>	<b>73</b>
Adding a Rapid7 NeXpose scanner API site import.....	73
Adding a Rapid7 NeXpose scanner local file import.....	74
<b>Chapter 24: SAINT scanner overview.....</b>	<b>76</b>
Configuring a SAINTwriter template.....	76
Adding a SAINT vulnerability scan.....	77
<b>Chapter 25: Tenable SecurityCenter scanner overview.....</b>	<b>79</b>
Adding a Tenable SecurityCenter scan.....	79
<b>Chapter 26: Scheduling a vulnerability scan.....</b>	<b>81</b>
<b>Chapter 27: Viewing the status of a vulnerability scan.....</b>	<b>82</b>
<b>Chapter 28: Supported vulnerability scanners.....</b>	<b>84</b>
<b>Index.....</b>	<b>86</b>

# Introduction to Extreme Security vulnerability assessment configurations

---

Integration with vulnerability assessment scanners provides administrators and security professionals information to build vulnerability assessment profiles for network assets.

## Intended audience

Administrators must have Extreme Security access and a knowledge of the corporate network and networking technologies.

## 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. Extreme Networks® systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. EXTREME NETWORKS 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.

---

### Note



Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. Extreme Networks Security Analytics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of Extreme Networks Security Analytics.

---

## Conventions






---

This section discusses the conventions used in this guide.

### Text Conventions

The following tables list text conventions that are used throughout this guide.

**Table 1: Notice Icons**

Icon	Notice Type	Alerts you to...
	Tip	Helpful tips for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

**Table 2: Text Conventions**

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words <b>enter</b> and <b>type</b>	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
Words in <i>italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

## Terminology

When features, functionality, or operation is specific to a switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the “switch.”

## Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at [InternalInfoDev@extremenetworks.com](mailto:InternalInfoDev@extremenetworks.com).

## Getting Help

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods:

Web	<a href="http://www.extremenetworks.com/support">www.extremenetworks.com/support</a>
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: <a href="http://www.extremenetworks.com/support/contact">www.extremenetworks.com/support/contact</a>
Email	<a href="mailto:support@extremenetworks.com">support@extremenetworks.com</a> To expedite your message, enter the product name or model number in the subject line.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

## Related Publications

The Extreme Security product documentation listed below can be downloaded from <http://documentation.extremenetworks.com>.

### Extreme Security Analytics Threat Protection

- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Security DSM Configuration Guide Addendum*
- *Extreme Networks Security Hardware Guide*
- *Extreme Networks Security Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *Extreme Networks Security Log Manager Administration Guide*

- *Extreme Networks Security Log Sources User Guide*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Security Release Notes*
- *Extreme Networks Security Risk Manager Adapter Configuration Guide*
- *Extreme Networks Security Risk Manager Getting Started Guide*
- *Extreme Networks Security Risk Manager Installation Guide*
- *Extreme Networks Security Risk Manager Migration Guide*
- *Extreme Networks Security Risk Manager User Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security Vulnerability Manager Release Notes*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Troubleshooting Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks SIEM Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*

## Extreme Security Threat Protection

- *Extreme Security Intrusion Prevention System Hardware Replacement Guide*
- *Extreme Security Threat Protection Release Notes*



# 1 Vulnerability assessment scanner overview

## Installing the unrestricted Java Cryptography Extension

Integrate vulnerability assessment scanners with Extreme Networks Security Analytics to provide vulnerability assessment profiles for network assets.

References to Extreme Security apply to all products capable of collecting vulnerability assessment information.

Asset profiles for servers and hosts in your network provide information that can help you to resolve security issues. Using asset profiles, you can connect offenses that occur on your system to the physical or virtual assets as part of your security investigation. Asset data is helpful to identify threats, to identify vulnerabilities, services, ports, and monitor asset usage in your network.

The **Assets** tab provides a unified view of the information that is known about your assets. As more information is provided to the system through vulnerability assessment, the system updates the asset profile. 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. You can schedule scans and ensure that vulnerability information is relevant for assets in the network.

## Installing the unrestricted Java™ Cryptography Extension

The Java™ Cryptography Extension (JCE) is a Java™ framework that is required to decrypt advanced cryptography algorithms for AES 192-bit or AES 256-bit SNMPv3 traps.

Each managed host that receives SNMPv3 high-level traps requires the unrestricted JCE. If you require advanced cryptography algorithms for SNMP communication, you must update the existing cryptography extension on your managed host with an unrestricted JCE.

- 1 Using SSH, log in to your Extreme Security Console.
- 2 To verify the version of Java on the Console, type the following command:

```
java -version.
```

The JCE file must match the version of the Java™ installed on the Console.

- 3 Download the latest version of the Java™ Cryptography Extension from the IBM® website.  
<https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk>
- 4 Secure copy (SCP) the `local.policy.jar` and `US_export_policy.jar` file to the following directory of the Console:

```
/opt/ibm/java-[version]/jre/lib/security/.
```

- 5 Optional. Distributed deployments require administrators to copy the `local.policy.jar` and `US_export_policy.jar` files from the Console appliance to the managed host.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.

# 2 AXIS scanner

## Adding an AXIS vulnerability scan

You can import vulnerability data from any scanner that outputs data in Asset Export Information Source (AXIS) format. Axis is an XML data format that was created specifically for asset and vulnerability compatibility with Extreme Networks Security Analytics products.

AXIS is a standard format for scan result imports of vulnerability data. Vulnerability data for Axis scanners must comply with the AXIS format schema to be imported successfully. To successfully integrate an AXIS scanner with Extreme Security, XML result files must be available on a *remote server* or a scanner that supports SFTP or SMB Share communication. A remote server is a system or third-party appliance that can host the XML scan results.

## Adding an AXIS vulnerability scan

Add an AXIS scanner configuration to collect specific reports or start scans on the remote scanner.

The following table describes AXIS scanner parameters when you select SFTP as the import method:

**Table 3: AXIS scanner - SFTP properties**

Parameter	Description
Remote Hostname	The IP address or host name of the server that has the scan results files.
Login Username	The user name that Extreme Security uses to log in to the server.
Enable Key Authentication	Specifies that Extreme Security authenticates with a key-based authentication file.
Remote directory	The location of the scan result files.
Private Key File	The full path to the file that contains the private key. If a key file does not exist, you must create the <code>vis.ssh.key</code> file.
File Name Pattern	The regular expression (regex) required to filter the list of files that are in the <i>Remote Directory</i> . The <code>.*\.*.xml</code> pattern imports all XML files from the remote directory.

The following table describes AXIS scanner parameters when you select *SMB Share* as the import method:

**Table 4: AXIS scanner - SMB Share properties**

Parameter	Description
Hostname	The IP address or host name of the SMB Share.
Login Username	The user name that Extreme Security uses to log in to SMB Share.
Domain	The domain that is used to connect to the SMB Share.
SMB Folder Path	The full path to the share from the root of the SMB host. Use forward slashes, for example, /share/logs/.
File Name Pattern	The regular expression (regex) required to filter the list of files in the Remote Directory. The .*\.xml pattern imports all xml files in the remote directory.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify the AXIS scanner.
- 5 From the **Managed Host** list, select the managed host that manages the scanner import.
- 6 From the **Type** list, select **Axis Scanner**.
- 7 From the **Import Method** list, select **SFTP** or **SMB Share**.
- 8 Configure the parameters.
- 9 Configure a CIDR range for the scanner.
- 10 Click **Save**.
- 11 On the **Admin** tab, click **Deploy Changes**.

For more information about how to create a scan schedule, see [Scheduling a vulnerability scan](#) on page 81.



# 3 Beyond Security Automatic Vulnerability Detection System scanner overview

## Adding a Beyond Security AVDS vulnerability scanner

Vulnerability assessment is the evaluation of assets in the network to identify and prioritize potential security issues. Extreme Security products that support Vulnerability Assessment can import vulnerability data from external scanner products to identify vulnerabilities profiles for assets.

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. As external scanners generate scan data, Extreme Security can retrieve the vulnerability data with a scan schedule.

To configure a Beyond Security AVDS scanner, see [Adding a Beyond Security AVDS vulnerability scanner](#) on page 13.

## Adding a Beyond Security AVDS vulnerability scanner

Beyond Security Automated Vulnerability Detection System (AVDS) appliances create vulnerability data in Asset Export Information Source (AXIS) format. AXIS formatted files can be imported by XML files that can be imported.

To successfully integrate Beyond Security AVDS vulnerabilities with Extreme Security, you must configure your Beyond Security AVDS 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 by using Secure File Transfer Protocol (SFTP). The term remote server refers to any appliance, third-party host, or network storage location that can host the published XML scan result files.

The most recent XML results that contain Beyond Security AVDS vulnerabilities are imported to when a scan schedule starts. Scan schedules determine the frequency with which vulnerability data created by Beyond Security AVDS is imported. After you add your Beyond Security AVDS appliance to Extreme Security, create a scan schedule to import the scan result files. Vulnerabilities from the scan schedule updates the **Assets** tab after the scan schedule completes.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Beyond Security AVDS scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.

- 6 From the **Type** list, select **Beyond Security AVDS**.
- 7 In the **Remote Hostname** field, type the IP address or host name of the system that contains the published scan results from your Beyond Security AVDS scanner.
- 8 Choose one of the following authentication options:

Option	Description
<b>Login Username</b>	<p>To authenticate with a user name and password:</p> <ol style="list-style-type: none"> <li>1 In the <b>Login Username</b> field, type a username that has access to retrieve the scan results from the remote host.</li> <li>2 In the <b>Login Password</b> field, type the password that is associated with the user name.</li> </ol>

<b>Enable Key Authorization</b>	<p>To authenticate with a key-based authentication file:</p> <ol style="list-style-type: none"> <li>1 Select the <b>Enable Key Authentication</b> check box.</li> <li>2 In the <b>Private Key File</b> field, type the directory path to the key file.</li> </ol> <p>The default directory for the key file is <code>/opt/qradar/conf/vis.ssh.key</code>.</p> <p>If a key file does not exist, you must create the vis.ssh.key file.</p>
---------------------------------	--

- 9 In the **Remote Directory** field, type the directory location of the scan result files.
- 10 In the **File Name Pattern** field, type a regular expression (regex) to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing.
 

The default value is `.*\.*xml`. The `.*\.*xml` pattern imports all xml files in the remote directory.
- 11 In the **Max Reports Age (Days)** field, type the maximum file age for your scan results file. Files that are older than the specified days and timestamp on the report file are excluded when the schedule scan starts. The default value is 7 days.
- 12 To configure the **Ignore Duplicates** option:
  - Select this check box to track files that are already processed by a scan schedule. This option prevents a scan result file from being processed a second time.
  - Clear this check box to import vulnerability scan results each time the scan schedule starts. This option can lead to multiple vulnerabilities associated with one asset.

If a result file is not scanned within 10 days, the file is removed from the tracking list and is processed the next time the scan schedule starts.

- 13 To configure a CIDR range for your scanner:
  - a Type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 14 Click **Save**.
- 15 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.

# 4 Digital Defense Inc AVS scanners

You can add a Digital Defense Inc AVS scanner to your Extreme Networks Security Analytics deployment.

Before you add this scanner, a server certificate is required to support HTTPS connections. Extreme Security supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

At intervals that are determined by a scan schedule, Extreme Security imports the most recent XML results that contain Digital Defense Inc AVS vulnerabilities. To enable communication with the Digital Defense Inc AVS scanner, Extreme Security uses the credentials that you specify in the scanner configuration.

The following list provides more information about Digital Defense Inc AVS scanner parameters:

<b>Remote Hostname</b>	The host name of the remote server that hosts the Digital Defense Inc AVS scanner.
<b>Remote Port</b>	The port number of the remote server that hosts the Digital Defense Inc AVS scanner.
<b>Remote URL</b>	The URL of the remote server that hosts the Digital Defense Inc AVS scanner.
<b>Client ID</b>	The master client ID that uses to connect to the Digital Defense Inc AVS scanner.
<b>Host Scope</b>	When set to Internal, retrieves the active view for the internal hosts of the Digital Defense Inc AVS scanner. When set to External, retrieves the external active view of the Digital Defense Inc AVS scanner.
<b>Retrieve Data For Account</b>	The <b>Default</b> option indicates that the data is included from only the specified <b>Client ID</b> . If you want to include data from the Client ID and all its sub accounts, select <b>All Sub Accounts</b> . If you want to specify a single, alternate client ID, select <b>Alternate Client ID</b> .
<b>Correlation Method</b>	Specifies the method by which vulnerabilities are correlated. <ul style="list-style-type: none"><li>• The <b>All Available</b> option queries the Digital Defense Inc vulnerability catalog and attempts to correlate vulnerabilities that are based on all the references that are returned for that specific vulnerability. References might include CVE, Bugtraq, Microsoft Security Bulletin, and OSVDB. Multiple references often correlate to the same vulnerability, but returns more results and take longer to process than the <b>CVE</b> option.</li><li>• The <b>CVE</b> option correlates vulnerabilities that are based only on the CVE-ID.</li></ul>

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Data Sources**.

- 3 Click the **VA Scanners** icon.
- 4 Click **Add**.
- 5 From the **Type** list box, select **Digital Defense Inc AVS**.
- 6 Configure the parameters.
- 7 To configure the CIDR ranges you want this scanner to consider, type the CIDR range, or click **Browse** to select the CIDR range from the network list.
- 8 Click **Add**.
- 9 Click **Save**.
- 10 On the **Admin** tab, click **Deploy Changes**.

After you add your Digital Defense Inc AVS scanner, you can add a scan schedule to retrieve your vulnerability information.



# 5 eEye scanner overview

## Adding an eEye REM SNMP scan Adding an eEye REM JDBC scan

Extreme Security can collect vulnerability data from eEye REM Security Management Console or eEye Retina CS scanners.

The following protocol options are available to collect vulnerability information from eEye scanners:

- Add an SNMP protocol eEye scanner. See [Adding an eEye REM SNMP scan](#) on page 17.
- Add a JDBC protocol eEye scanner. See [Adding an eEye REM JDBC scan](#) on page 18

### Related Links

[Installing the unrestricted Java Cryptography Extension](#) on page 9

The Java™ Cryptography Extension (JCE) is a Java™ framework that is required to decrypt advanced cryptography algorithms for AES 192-bit or AES 256-bit SNMPv3 traps.

## Adding an eEye REM SNMP scan

You can add a scanner to collect vulnerability data over SNMP from eEye REM or CS Retina scanners.

To use CVE identifiers and descriptions, you must copy the `audits.xml` file from your eEye REM scanner to the managed host responsible for listening for SNMP data. If your managed host is in a distributed deployment, you must copy the `audits.xml` to the Console first and SSH the file to `/opt/qradar/conf/audits.xml` on the managed host. The default location of `audits.xml` on the eEye scanner is `%ProgramFiles(x86)%\eEye Digital Security\Retina CS\Applications\RetinaManager\Database\audits.xml`.

To receive the most up-to-date CVE information, periodically update Extreme Security with the latest `audits.xml` file.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your SecureScout server.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **eEye REM Scanner**.
- 7 From the **Import Type** list, select **SNMP**.
- 8 In the **Base Directory** field, type a location to store the temporary files that contain the eEye REM scan data.

The default directory is `/store/tmp/vis/eEye/`.

- 9 In the **Cache Size** field, type the number of transactions you want to store in the cache before the SNMP data is written to the temporary file. The default is 40.  
The default value is 40 transactions.
- 10 In the **Retention Period** field, type the time period, in days, that the system stores scan information.  
If a scan schedule did not import data before the retention period expires, the scan information from the cache is deleted.
- 11 Select the **Use Vulnerability Data** check box to correlate eEye vulnerabilities to Common Vulnerabilities and Exposures (CVE) identifiers and description information.
- 12 In the **Vulnerability Data File** field, type the directory path to the eEye `audits.xml` file.
- 13 In the **Listen Port** field, type the port number that is used to monitor for incoming SNMP vulnerability information from your eEye REM scanner.  
The default port is 1162.
- 14 In the **Source Host** field, type the IP address of the eEye scanner.
- 15 From the **SNMP Version** list, select the SNMP protocol version.  
The default protocol is SNMPv2.
- 16 In the **Community String** field, type the SNMP community string for the SNMPv2 protocol, for example, `Public`.
- 17 From the **Authentication Protocol** list, select the algorithm to authenticate SNMPv3 traps.
- 18 In the **Authentication Password** field, type the password that you want to use to authenticate SNMPv3 communication.  
The password must include a minimum of 8 characters.
- 19 From the **Encryption Protocol** list, select the SNMPv3 decryption algorithm.
- 20 In the **Encryption Password** field, type the password to decrypt SNMPv3 traps.
- 21 To configure a CIDR range for your scanner:
  - a Type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 22 Click **Save**.
- 23 On the **Admin** tab, click **Deploy Changes**.

Select one of the following options:

- If you do not use SNMPv3 or use low-level SNMP encryption, you are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.
- If your SNMPv3 configuration uses AES192 or AES256 encryption, you must install the unrestricted Java™ cryptography extension on each Console or managed host that receives SNMPv3 traps. See [Installing the unrestricted Java Cryptography Extension](#) on page 9.

## Adding an eEye REM JDBC scan

You can add a scanner to collect vulnerability data over JDBC from eEye REM or CS Retina scanners.

Before you configure Extreme Security to poll for vulnerability data, we suggest you create a database user account and password for Extreme Security. If you assign the user account read-only permission to the RetinaCSDatabase, you can restrict access to the database that contains the eEye vulnerabilities. The JDBC protocol enables Extreme Security to log in and poll for events from the MSDE database.

Ensure that no firewall rules block communication between the eEye scanner and the Console or managed host responsible for polling with the JDBC protocol. If you use database instances, you must verify port 1433 is available for the SQL Server Browser Service to resolve the instance name.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify the eEye scanner.
- 5 From the **Managed Host** list, select the managed host from the Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **eEye REM Scanner**.
- 7 From the **Import Type** list, select **JDBC**.
- 8 In the **Hostname** field, type the IP address or the host name of the eEye database.
- 9 In the **Port** field, type 1433.
- 10 Optional. In the **Database Instance** field, type the database instance for the eEye database.  
If a database instance is not used, leave this field blank.
- 11 In the **Username** field, type the username required to query the eEye database.
- 12 In the **Password** field, type the password required to query the eEye database.
- 13 In the **Domain** field, type the domain required, if required, to connect to the eEye database.

If the database is configured for Windows and inside a domain, you must specify the domain name.

- 14 In the **Database Name** field, type `RetinaCSDatabase` as the database name.
- 15 Select the **Use Named Pipe Communication** check box if named pipes are required to communicate to the eEye database. By default, this check box is clear.
- 16 Select the **Use NTLMv2** check box if the eEye scanner 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. The Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.

- 17 To configure a CIDR range for the scanner:
  - a In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 18 Click **Save**.
- 19 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.

# 6 Foundstone FoundScan scanner overview

## Adding a Foundstone FoundScan scanner Importing certificates for Foundstone FoundScan

The Foundstone FoundScan scanner queries the FoundScan Engine for host and vulnerability information from the FoundScan OpenAPI.

Extreme Security supports Foundstone FoundScan versions 5.0 to 6.5.

The FoundScan appliance must include a scan configuration that runs regularly to keep the host and vulnerability results current. To ensure that the FoundScan scanner is able to retrieve scan information, make sure the FoundScan system meets the following requirements:

- The FoundScan application must be active. Since the API provides access to the FoundScan application, administrators can verify that the FoundScan application runs continuously on the FoundScan server.
- The scan data to import must be complete and visible in the FoundScan user interface to retrieve scan results. If the scan is scheduled to be removed after completion, the results must be imported by the scan schedule before the scan is removed from FoundScan.
- The appropriate user privileges must be configured in the FoundScan application to enable communication between Extreme Security and FoundScan. The FoundScan OpenAPI provides host and vulnerability information. All vulnerabilities for a host assigned are assigned to port 0.

To connect to FoundScan, the FoundScan Engine requires authentication with client-side certificates. FoundScan includes a default certificate authority and client certificates that are the same for all scanner installations. The FoundScan plug-in also includes certificates for use with FoundScan 5.0. If the FoundScan Server uses custom certificates, administrators must import the appropriate certificates and keys. Instructions on how to import certificates is provided in this configuration documentation.

To add a FoundScan API vulnerability scan, see [Adding a Foundstone FoundScan scanner](#) on page 20.

## Adding a Foundstone FoundScan scanner

Administrators can add a Foundstone FoundScan scanner to collect host and vulnerability information through the FoundScan OpenAPI.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your FoundScan server.

- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.  
Certificates for your FoundScan scanner must reside on the managed host selected in the Managed Host list box.
- 6 From the **Type** list, select **FoundScan Scanner**.
- 7 In the **SOAP API URL** field, type the IP address or hostname of the Foundstone FoundScan that contains the vulnerabilities you want to retrieve with the SOAP API.  
For example, `https://foundstone IP address:SOAP port` The default value is `https://localhost:3800`.
- 8 In the **Customer Name** field, type the name of the customer that belongs to the user name.
- 9 In the **User Name** field, type the username required to access the Foundstone FoundScan server.
- 10 Optional. In the **Client IP Address** field, type the IP address of the server that you want to perform the scan.  
By default, this value is not used; however, is necessary when administrators validate some scan environments.
- 11 Optional. In the **Password** field, type the password required to access the Foundstone FoundScan server.
- 12 In the **Portal Name** field, type the portal name.  
This field can be left blank for Extreme Security. See your FoundScan administrator for more information.
- 13 In the **Configuration Name** field, type the scan configuration name that exists in FoundScan and to which the user has access.  
Make sure this scan configuration is active or runs frequently.
- 14 In the **CA Truststore** field, type the directory path and filename for the CA truststore file.  
The default path is `/opt/qradar/conf/foundscan.keystore`.
- 15 In the **CA Keystore** field, type the directory path and filename for the client keystore.  
The default path is `/opt/qradar/conf/foundscan.truststore`.
- 16 To configure a CIDR range for the scanner:
  - a In the text field, type the CIDR range for the scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 17 Click **Save**.
- 18 On the **Admin** tab, click **Deploy Changes**.

Administrators can now import certificates from your FoundScan server to enable communication. See [Importing certificates for Foundstone FoundScan](#) on page 21.

## Importing certificates for Foundstone FoundScan

Administrators that use custom certificates or a version of Foundstone FoundScan lower than V5.0 must import the appropriate certificates to the managed host from the scanner configuration.

The scanner must be add to a managed host in the scan configuration before certificates are imported from the FoundScan server. The certificates must be imported to the correct managed host to collect vulnerability and host scan data.

- 1 Obtain the two certificate files and the pass phrase from your FoundScan administrator.
  - The `TrustedCA.pem` file is the CA certificate for the FoundScan engine.
  - The `Portal.pem` file certificate is the private key that includes the certificate chain for the client.
- 2 Using SSH, copy the two pem files to the managed host assigned in your FoundScan configuration. If you have a distributed deployment, you must copy the files to the Console and SSH the files from the Console appliance to the managed host.
- 3 Navigate to the directory location of the pem files.
- 4 To remove the previous keystore certificate from the managed host, type the following command:  
`rm -f /opt/qradar/conf/foundscan.keystore`
- 5 To remove the previous truststore certificate from the managed host, type the following command:  
`rm -f /opt/qradar/conf/foundscan.truststore`
- 6 To import the pem files to your managed host, type the following command: `/opt/qradar/bin/foundstone-cert-import.sh [TrustedCA.pem] [Portal.pem]`
- 7 Repeat the certificate import for any more managed hosts in your deployment that connect to the Foundstone FoundScan appliance.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.

# 7 Security AppScan™ Enterprise scanner overview

---

Creating a customer user type for AppScan  
Enabling integration with AppScan Enterprise  
Creating an application deployment map in Security AppScan Enterprise  
Publishing completed reports in IBM AppScan  
Adding an AppScan vulnerability scanner

Extreme Security retrieves AppScan Enterprise reports with the Representational State Transfer (REST) web service to import vulnerability data and generate offenses for your security team.

You can import scan results from Security AppScan Enterprise report data, providing you a centralized security environment for advanced application scanning and security compliance reporting. You can import Security AppScan Enterprise scan results to collect asset vulnerability information for malware, web applications, and web services in your deployment.

To integrate AppScan Enterprise with Extreme Security, you must complete the following tasks:

- 1 Generate scan reports in AppScan Enterprise.

Report configuration information can be found in your Security AppScan Enterprise documentation.

- 2 Configure AppScan Enterprise to grant Extreme Security access to report data.
- 3 Configure your AppScan Enterprise scanner in Extreme Security.
- 4 Create a schedule in Extreme Security to import AppScan Enterprise results.

To configure AppScan Enterprise to grant permission to report data, your AppScan administrator must determine which users have permissions to publish reports to Extreme Security. After AppScan Enterprise users configure reports, the reports that are generated by AppScan Enterprise can be published to Extreme Security, making them available for download.

To configure AppScan Enterprise to grant access to scan report data, see [Creating a customer user type for AppScan](#) on page 23.

## Creating a customer user type for AppScan®

---

You can create custom user types to assign permissions for limited and specific administrative tasks to administrators.

- 1 Log in to your AppScan® Enterprise appliance.
- 2 Click the **Administration** tab.
- 3 On the User Types page, click **Create**.

- 4 Select all of the following user permissions:
  - **Configure QRadar Integration** - Select this check box to allow users to access the Extreme Security integration options for AppScan Enterprise.
  - **Publish to QRadar** - Select this check box to allow Extreme Security access to published scan report data.
  - **QRadar Service Account** - Select this check box to add access to the REST API for the user account. This permission does not provide access the user interface.
- 5 Click **Save**.

You are now ready to enable integration permissions. See [Enabling integration with AppScan Enterprise](#) on page 24

## Enabling integration with AppScan® Enterprise

---

AppScan® Enterprise must be configured to enable integration with Extreme Security.

To complete these steps, you must be logged in with a custom user type.

- 1 Click the **Administration** tab.
- 2 On the **Navigation** menu, select **Network Security Systems**.
- 3 On the Integration Setting pane, click **Edit**.
- 4 Select the **Enable QRadar Integration** check box.

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

You are now ready to configure the Application Deployment Mapping in AppScan Enterprise. See [Creating an application deployment map in Security AppScan Enterprise](#) on page 24.

## Creating an application deployment map in Security AppScan® Enterprise

---

The Application Deployment Map allows AppScan® Enterprise to determine the locations that host 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.

- 1 Click the **Administration** tab.
- 2 On the navigation menu, select **Network Security Systems**.
- 3 On the Integration Setting pane, click **Edit**.
- 4 In the **Application test location (host or pattern)** field, type the test location of your application.
- 5 In the **Application production location (host)** field, type the IP address of your production environment.

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

- 6 Click **Add**.



- 7 Repeat this procedure to map any more production environments in AppScan® Enterprise.
- 8 Click **Done**.

You are now ready to publish completed reports. See [Publishing completed reports in IBM AppScan](#) on page 25.

## Publishing completed reports in IBM AppScan®

Completed vulnerability reports that are generated by AppScan Enterprise must be made accessible to Extreme Security by publishing the report.

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

You are now ready to enable integration permissions. See [Adding an AppScan vulnerability scanner](#) on page 25.

## Adding an AppScan® vulnerability scanner

You can add a scanner to define which scan reports in IBM Security AppScan are collected by Extreme Security.

If your AppScan installation is set up to use HTTPS, a server certificate is required. Extreme Security supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

You can add multiple AppScan® scanners to Extreme Security, each with a different configuration. Multiple configurations provide Extreme Security the ability to import AppScan data for specific results. The scan schedule determines the frequency with which scan results are imported from the REST web service in AppScan Enterprise.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your AppScan® Enterprise scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **AppScan Scanner**.
- 7 In the **ASE Instance Base URL** field, type the full base URL of the AppScan Enterprise instance.

This field supports HTTP and HTTPS addresses, for example, `http://myasehostname/ase/`.

- 8 From the **Authentication Type** list, select one of the following options:
  - **Windows Authentication** - Select this option to use Windows Authentication with the REST web service.
  - **Jazz Authentication** - Select this option to use Jazz™ Authentication with the REST web service.
- 9 In the **Username** field, type the user name to retrieve scan results from AppScan® Enterprise.
- 10 In the **Password** field, type the password to retrieve scan results from AppScan® Enterprise.
- 11 In the **Report Name Pattern** field, type a regular expression (regex) to filter the list of vulnerability reports available from AppScan Enterprise.

By default, the **Report Name Pattern** field contains `. *` as the regex pattern. The `. *` pattern imports all scan reports that are published to Extreme Security. All matching files from the file pattern are processed by Extreme Security. You can specify a group of vulnerability reports or an individual report by using a regex pattern.
- 12 To configure a CIDR range for your scanner:
  - a Type the CIDR range for the scanner or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 13 Click **Save**.
- 14 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule for Security AppScan® Enterprise. See [Scheduling a vulnerability scan](#) on page 81

# 8 IBM® Security Guardium scanner overview

## Adding an IBM Security Guardium vulnerability scanner

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

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

IBM Guardium only exports vulnerability from databases containing failed CVE test results. If there are no failed CVE tests, IBM Guardium may not export a file at the end of the security assessment. For information on configuring security assessment tests and creating an audit process to export vulnerability data in SCAP format, see your IBM InfoSphere Guardium documentation.

After you have configured your IBM Guardium appliance, you are ready to configure Extreme Security to import the results from the remote server hosting the vulnerability data. You must add an IBM Guardium scanner to Extreme Security and configure the scanner to retrieve data from your remote server. The most recent vulnerabilities are imported by Extreme Security when you create a scan schedule. Scan schedules allow you to determine the frequency with which Extreme Security requests data from the remote server host your IBM Guardium vulnerability data.

Integration overview for IBM InfoSphere Guardium and Extreme Security.

- 1 On your IBM InfoSphere® Guardium® appliance, create an SCAP file with your vulnerability information. See your IBM Security InfoSphere Guardium documentation.
- 2 On your Extreme Security Console, add an IBM Guardium® scanner. See [Adding an IBM Security Guardium vulnerability scanner](#) on page 27
- 3 On your Extreme Security Console, create a scan schedule to import scan result data. See [Scheduling a vulnerability scan](#) on page 81

## Adding an IBM Security Guardium® vulnerability scanner

Adding a scanner allows Extreme Security to collect SCAP vulnerability files from IBM InfoSphere Guardium.

Administrators can add multiple IBM Guardium® scanners to Extreme Security, each with a different configuration. Multiple configurations provide Extreme Security the ability to import vulnerability data

for specific results. The scan schedule determines the frequency with which the SCAP scan results are imported from IBM InfoSphere Guardium.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your IBM Guardium® scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **IBM Guardium SCAP Scanner**.
- 7 Choose one of the following authentication options:

Option	Description
<b>Login Username</b>	<p>To authenticate with a user name and password:</p> <ol style="list-style-type: none"> <li>1 In the <b>Login Username</b> field, type a username that has access to retrieve the scan results from the remote host.</li> <li>2 In the <b>Login Password</b> field, type the password associated with the user name.</li> </ol>

<b>Enable Key Authorization</b>	<p>To authenticate with a key-based authentication file:</p> <ol style="list-style-type: none"> <li>1 Select the <b>Enable Key Authentication</b> check box.</li> <li>2 In the <b>Private Key File</b> field, type the directory path to the key file.</li> </ol> <p>The default is directory for the key file is <code>/opt/gradar/conf/vis.ssh</code>. If a key file does not exist, you must create the <code>vis.ssh</code> key file.</p>
---------------------------------	---

- 8 In the **Remote Directory** field, type the directory location of the scan result files.
- 9 In the **File Name Pattern** field, type a regular expression (regex) required to filter the list of SCAP vulnerability files specified in the **Remote Directory** field. All matching files are included in the processing.
 

By default, the Report Name Pattern field contains `.*\.*.xml` as the regex pattern. The `.*\.*.xml` pattern imports all xml files in the remote directory.
- 10 In the **Max Reports Age (Days)** field, type the maximum file age for your scan results file. Files that are older than the specified days and timestamp on the report file are excluded when the schedule scan starts. The default value is 7 days.
- 11 To configure the **Ignore Duplicates** option:
  - Select this check box to track files that have already been processed by a scan schedule. This option prevents a scan result file from being processed a second time.
  - Clear this check box to import vulnerability scan results each time the scan schedule starts. This option can lead to multiple vulnerabilities being associated with an asset.

If a result file is not scanned within 10 days, the file is removed from the tracking list and is processed the next time the scan schedule starts.

- 12 To configure a CIDR range for your scanner:
  - a In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 13 Click **Save**.

14 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule for IBM InfoSphere Guardium. See [Scheduling a vulnerability scan](#) on page 81

# 9 IBM® Security SiteProtector™ scanner overview

## Adding an IBM SiteProtector vulnerability scanner

The IBM SiteProtector scanner module for Extreme Security accesses vulnerability data from IBM SiteProtector™ scanners through Java Database Connectivity (JDBC) queries.

The IBM SiteProtector scanner retrieves vulnerability data from the RealSecureDB table and polls for new vulnerabilities each time a scan schedule starts. The **Compare** field enables the query to retrieve any new vulnerabilities from the RealSecureDB table to ensure that duplicate vulnerabilities are not imported. When the IBM SiteProtector scanner is configured, the administrator can create a SiteProtector user account specifically for polling vulnerability data. After the user account is created, the administrator can verify that there are no firewalls that reject queries on the port configured to poll the database.

To configure an IBM Security SiteProtector scanner, see [Adding an IBM SiteProtector vulnerability scanner](#) on page 30.

## Adding an IBM® SiteProtector™ vulnerability scanner

Extreme Security can poll IBM® InfoSphere® SiteProtector™ appliances for vulnerability data with JDBC.

Administrators can add multiple IBM® SiteProtector™ scanners to Extreme Security, each with a different configuration. Multiple configurations provide Extreme Security with the ability to query SiteProtector and only import results from specific CIDR ranges. The scan schedule determines the frequency with which the database on the SiteProtector scanner is queried for vulnerability data.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify the IBM SiteProtector scanner.
- 5 From the **Managed Host** list, select the managed host from the Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **IBM SiteProtector Scanner**.
- 7 In the **Hostname** field, type the IP address or host name of the IBM SiteProtector that contains vulnerabilities to import.
- 8 In the **Port** field, type 1433 as the port for the IBM SiteProtector database.
- 9 In the **Username** field, type the username required to query the IBM SiteProtector database.
- 10 In the **Password** field, type the password required to query the IBM SiteProtector database.

- 11 In the **Domain** field, type the domain required, if required, to connect to the IBM SiteProtector database.

If the database is configured for Windows and inside a domain, you must specify the domain name.

- 12 In the **Database Name** field, type `RealSecureDB` as the database name.
- 13 In the **Database Instance** field, type the database instance for the IBM SiteProtector database. If you are not using a database instance, you can leave this field blank.
- 14 Select the **Use Named Pipe Communication** if named pipes are required to communicate to the IBM SiteProtector database. By default, this check box is clear.
- 15 Select the **Use NTLMv2** check box if the 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. The Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.

- 16 To configure a CIDR range for the scanner:
  - a In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 17 Click **Save**.
- 18 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81

# 10 Security Tivoli® Endpoint Manager scanner overview

## Adding an IBM Security Tivoli Endpoint Manager vulnerability scanner

The Tivoli® Endpoint Manager scanner module accesses vulnerability data from 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 Extreme Security. Administrators can create a user in Tivoli Endpoint Manager for Extreme Security to use when the system collects vulnerabilities.



### Note

Extreme Security is compatible with Tivoli Endpoint Manager versions 8.2.x. However, administrators can use the latest version of Tivoli Endpoint Manager that is available.

To add a Tivoli® Endpoint Manager scanner, see [Adding an IBM Security Tivoli Endpoint Manager vulnerability scanner](#) on page 32

## Adding an IBM Security Tivoli Endpoint Manager vulnerability scanner

Extreme Security accesses vulnerability data from IBM Tivoli Endpoint Manager by using the SOAP API installed with the Web Reports application.

You can add multiple IBM Tivoli Endpoint Manager scanners in Extreme Security. Each scanner requires a different configuration to determine which CIDR ranges you want the scanner to consider.

Use multiple configurations for a single IBM Tivoli Endpoint Manager scanner to create individual scanners that collect specific result data from specific locations or vulnerabilities for specific types of operating systems.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your IBM Tivoli Endpoint Manager.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **IBM Tivoli Endpoint Manager**.
- 7 In the **Hostname** field, type the IP address or host name of the IBM Tivoli Endpoint Manager containing the vulnerabilities that you want to retrieve with the SOAP API.



- 8 In the **Port** field, type the port number that is used to connect to the IBM Tivoli Endpoint Manager by using the SOAP API.

By default, port 80 is the port number for communicating with IBM Tivoli Endpoint Manager. If you use HTTPS, you must update this field with the HTTPS port number. For most configuration, use port 443.

- 9 Select the **Use HTTPS** check box to connect securely with the HTTPS protocol.

If you select this check box, the host name or IP address that you specify uses HTTPS to connect to your IBM Tivoli Endpoint Manager. When you use HTTPS, a server certificate is required. Certificates must be placed in `/opt/qradar/conf/trusted_certificates` folder. Extreme Security supports certificates with the following file extensions: `.crt`, `.cert`, or `.der`. You can either use SCP or SFTP to manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory. Alternatively, you can download a copy of the certificate directly from the Extreme Security host. To do this, use SSH to connect the host and type the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into the `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

- 10 In the **Username** field, type the user name access IBM Tivoli Endpoint Manager.
- 11 In the **Password** field, type the password that is required to access IBM Tivoli Endpoint Manager.
- 12 To configure a CIDR range for your scanner:
  - a In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 13 Click **Save**.

- 14 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule for IBM Security Tivoli Endpoint Manager. See [Scheduling a vulnerability scan](#) on page 81

# 11 Juniper Profiler NSM scanner overview

## Adding a Juniper NSM Profiler scanner

Extreme Security can collect vulnerability data from the PostgreSQL database on the Juniper Profiler NSM scanner by polling for data with JDBC.

The Juniper Networks Netscreen Security Manager (NSM) console passively collects valuable asset information from your network through deployed Juniper Networks IDP sensors. Extreme Security connects to the Profiler database stored on the NSM server to retrieve these records. The Extreme Security server must have access to the Profiler database. Extreme Security supports NSM versions 2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1, and 2010.x. For more information, see your vendor documentation. To collect data from the PostgreSQL database, Extreme Security must have access to the Postgres database port through TCP port 5432. Access is provided in the `pg_hba.conf` file, which is located in `/var/netscreen/DevSvr/pgsql/data/pg_hba.conf` on the system that hosts the Juniper NSM Profiler.

To add a Juniper NSM Profiler scanner, see [Adding a Juniper NSM Profiler scanner](#) on page 34.

## Adding a Juniper NSM Profiler scanner

Administrators can add a Juniper NSM Profiler scanner to poll for vulnerability data with JDBC.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your FoundScan server.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.  
Certificates for your FoundScan scanner must reside on the managed host selected in the Managed Host list box.
- 6 From the **Type** list, select **Juniper NSM Profiler Scanner**.
- 7 In the **SOAP API URL** field, type the IP address or hostname of the Foundstone FoundScan that contains the vulnerabilities you want to retrieve with the SOAP API.  
For example, `https://foundstone IP address:SOAP port`. The default value is `https://localhost:3800`.
- 8 In the **Customer Name** field, type the name of the customer that belongs to the user name.
- 9 In the **User Name** field, type the username required to access the Foundstone FoundScan server.

- 10 Optional. In the **Client IP Address** field, type the IP address of the server that you want to perform the scan.  
By default, this value is not used; however, is necessary when administrators validate some scan environments.
- 11 Optional. In the **Password** field, type the password required to access the Foundstone FoundScan server.
- 12 In the **Portal Name** field, type the portal name.  
This field can be left blank for Extreme Security. See your FoundScan administrator for more information.
- 13 In the **Configuration Name** field, type the scan configuration name that exists in FoundScan and to which the user has access.  
Make sure this scan configuration is active or runs frequently.
- 14 In the **CA Truststore** field, type the directory path and filename for the CA truststore file.  
The default path is `/opt/qradar/conf/foundscan.keystore`.
- 15 In the **CA Keystore** field, type the directory path and filename for the client keystore.  
The default path is `/opt/qradar/conf/foundscan.truststore`.
- 16 To configure a CIDR range for your scanner:
  - a In the text field, type the CIDR range for the scanner or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 17 Click **Save**.
- 18 On the **Admin** tab, click **Deploy Changes**.

You are now ready to import certificates from your FoundScan server. See [Importing certificates for Foundstone FoundScan](#) on page 21.

# 12 McAfee Vulnerability Manager scanner overview

[Adding a remote XML import scan](#)  
[Adding a McAfee Vulnerability Manager SOAP API scan](#)  
[Creating certificates for McAfee Vulnerability Manager](#)  
[Processing certificates for McAfee Vulnerability Manager](#)  
[Importing certificates for McAfee Vulnerability Manager](#)

The McAfee Vulnerability Manager scanner enables Extreme Security to import vulnerabilities from an XML file or query for a results file from the McAfee OpenAPI.

Extreme Security can collect vulnerability data from McAfee Vulnerability Manager appliances. The following software versions are supported

- v6.8 and v7.0 for the McAfee Vulnerability Manager SOAP API
- v6.8, v7.0, and v7.5 for remote XML imports

The following import options are available to collect vulnerability information from McAfee Vulnerability Manager:

- To add a remote XML import for vulnerability data, see [Adding a remote XML import scan](#) on page 36.
- To retrieve vulnerabilities from the SOAP API, see [Adding a McAfee Vulnerability Manager SOAP API scan](#) on page 37

## Adding a remote XML import scan

Remote XML imports enable Extreme Security to connect to a remote server and import the HostData XML vulnerability data that is created by your McAfee Vulnerability Manager appliance.

Remote XML file imports enable you to configure the McAfee Vulnerability Manager to export scan results to a remote server. Extreme Security connects to the remote repository over SFTP and imports completed XML scan reports from a remote directory. You can use the file import collection method to import completed scan reports from McAfee Vulnerability Manager V7.0 and V7.5.

### Attention



The import might contain HostData and RiskData XML files. Only HostData XML files are supported as they contain the required host and vulnerability information. Ensure that only HostData XML files are placed in the remote directory or that the file name pattern that you configure matches only HostData reports.

- 1 Click the **Admin** tab.

- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify McAfee Vulnerability Manager.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **McAfee Vulnerability Manager**.
- 7 From the **Import Type** list, select **Remote XML Import**.
- 8 In the **Remote Hostname** field, type the IP address or host name of the remote server that hosts your McAfee Vulnerability Manager XML data.
- 9 In the **Remote Port** field, type the port to retrieve the XML vulnerability data.
- 10 Choose one of the following authentication options:

Option	Description
<b>Login Username</b>	Authenticates with a user name and password. The password must not contain the ! character. This character might cause authentication failures over SFTP.
<b>Enable Key Authorization</b>	Authenticate with a key-based authentication file. If a key file does not exist, you must create the <code>vis.ssh.key</code> file and place it in the <code>/opt/gradar/conf/vis.ssh.key</code> directory.

- 11 In the **Remote Directory** field, type the directory path to the XML vulnerability data.
- 12 In the **File Name Pattern** field, type a regular expression (regex) to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing. Ensure that this pattern matches only HostData XML reports.
- 13 In the **Max Reports Age (days)** field, type the maximum file age for your scan results file.
- 14 To configure a CIDR range for the scanner:
  - a In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 15 Click **Save**.
- 16 On the **Admin** tab, click **Deploy Changes**.

## Adding a McAfee Vulnerability Manager SOAP API scan

You can add a McAfee Vulnerability Manager scanner to enable Extreme Security to collect host and vulnerability information through the McAfee OpenAPI.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify the scanner.
- 5 From the **Managed Host** list, select the managed host that manages the scanner import.  
Certificates for the scanner must be on the managed host that is selected in the **Managed Host** list.
- 6 From the **Type** list, select **McAfee Vulnerability Manager**.

- 7 In the **SOAP API URL** field, type the IP address or hostname of the McAfee Vulnerability Manager that contains the vulnerabilities you want to retrieve with the SOAP API.  
For example, `https://foundstone IP address:SOAP port`. The default value is `https://localhost:3800`.
- 8 In the **Customer Name** field, type the name of the customer that belongs to the user name.
- 9 In the **User Name** field, type the user name to access McAfee Vulnerability Manager.
- 10 Optional: In the **Client IP Address** field, type the IP address of the server that you want to perform the scan.

**Tip**

This field is typically not used; however, it may be required for you to validate some scan environments.

- 11 In the **Password** field, type the password to access McAfee Vulnerability Manager.
- 12 In the **Configuration Name** field, type the scan configuration name that exists in McAfee Vulnerability Manager and to which the user has access.  
Make sure that this scan configuration is active or runs frequently.
- 13 In the **CA Truststore** field, type the directory path and filename for the CA truststore file.  
The default path is `/opt/gradar/conf/mvm.keystore`.
- 14 In the **CA Keystore** field, type the directory path and filename for the client keystore.  
The default path is `/opt/gradar/conf/mvm.truststore`.
- 15 From the **McAfee Vulnerability Manager Version** list, select the software version of your McAfee Vulnerability Manager.
- 16 To remove previously detected vulnerabilities that were not detected by the most recent scan, select the **Vulnerability Cleanup** check box.
- 17 To configure a CIDR range for the scanner:
  - a Type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.  
The McAfee Vulnerability Manager accepts only CIDR addresses ranges to a 0/0 subnet that are added as 0.0.0.0/0.
  - b Click **Add**.
- 18 Click **Save**.
- 19 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create certificates from McAfee Vulnerability Manager. See [Creating certificates for McAfee Vulnerability Manager](#) on page 38.

## Creating certificates for McAfee Vulnerability Manager

To connect through the Foundstone Open API, configure third-party certificates with the McAfee Certificate Manager Tool.

If the Certificate Manager Tool is not 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 Extreme Security on the McAfee Foundstone Enterprise Manager server.

The McAfee Foundstone Enterprise Manager server must be compatible with the version of the FIPS-Capable OpenSSL used by the Foundstone Certificate Manager to correctly create the certificates. A

Java™ Software Development Kit (Java™ SDK) must be present on this server for this processing. To obtain the most recent Java™ SDK go to the following website:

<http://java.sun.com>.

- 1 Log in to the McAfee Foundstone Enterprise Manager server.
- 2 Run the Foundstone Certificate Manager.
- 3 Click the **Create SSL Certificates** tab.
- 4 Type the host address for Extreme Security.  
The certificate must be created with the host address for the Extreme Security appliance that retrieves vulnerability data from the McAfee Vulnerability Manager.
- 5 Optional: Click **Resolve**.  
If an error occurs when the Foundstone Certificate Manager attempts to resolve the host, type the IP address in the **Host Address** field . If the host cannot resolve, see Step 7 on page 39.
- 6 Click **Create Certificate Using Common Name**.
- 7 Click **Create Certificate Using Host Address**.
- 8 Save the compressed file that contains the certificate files to a directory on your McAfee Vulnerability Manager.
- 9 Copy the pass phrase that is provided to a text file.
- 10 Repeat this process to generate any more certificates for managed hosts in your deployment.

You are now ready to process the certificates to create the required keystore and truststore files. See [Processing certificates for McAfee Vulnerability Manager](#) on page 39.

## Processing certificates for McAfee Vulnerability Manager

To create the keystore and truststore files required by Extreme Security, process the certificates that Foundstone Certificate Manager created.

You must have access to the support portal to download the files that are required to create the truststore and keystore files. The batch files require the path to the Java™ home directory on the McAfee Vulnerability Manager.

- 1 Log in to the support portal to download the following files:
  - `VulnerabilityManager-Cert.bat.gz`
  - `qllabs_vis_mvm_cert.jar`
- 2 Extract the compressed files and copy the certificates and the downloaded files to the same directory on your McAfee Vulnerability Manager.
- 3 Open the command-line interface on the McAfee Vulnerability manager.
- 4 Go to the directory location of the files.
- 5 To run the batch file, type the following command: `VulnerabilityManager-Cert.bat "C:\Program Files\Java\jdk1.6.0_20"`.  
The quotation marks in the command specify the Java™ home directory.
- 6 Repeat this process to create keystore and truststore files for any more managed hosts in your deployment.

The keystore and truststore files are created. If an error is displayed, administrators can verify the path to the Java™ home directory.

You are now ready to import the certificates for your Extreme Security appliance. See [Importing certificates for McAfee Vulnerability Manager](#) on page 40

## Importing certificates for McAfee Vulnerability Manager

---

The keystore and truststore files must be imported to the managed host responsible for the scan.

You must add the scanner to a managed host in the scan configuration before you import the certificates. For security purposes, a secure file transfer protocol to copy a certificate file.

- 1 To import the certificates, secure copy the `mvm.keystore` and `mvm.truststore` files to the following directories in Extreme Security:
  - `/opt/qradar/conf/`
  - `/opt/qradar/conf/trusted_certificates/`



### Note

If the `/opt/qradar/conf/trusted_certificates/` directory does not exist, do not create the directory. If the directory does not exist, administrators can ignore the file copy for the missing directory.

---

If you have a distributed deployment, you must copy the files to the Console and SSH the files from the Console appliance to the managed host.

- 2 Log in to Extreme Security.
- 3 Click the **Admin** tab.
- 4 On the **Admin** tab, select **Advanced > Deploy Full Configuration**.



### Note

When you click **Deploy Full Configuration**, Extreme Security restarts all services. Service restart results in a gap in data collection for events and flows until the deployment process completes.

---

- 5 Repeat the certificate import for any more managed hosts in your deployment that collect vulnerabilities from McAfee Vulnerability Manager.



# 13 Microsoft SCCM scanner overview

---

Extreme Networks Security Analytics can import scan reports from Microsoft System Center Configuration Manager (SCCM) scanners.

To integrate an Microsoft SCCM scanner, perform the following steps:

- 1 On your Microsoft SCCM scanner, configure WMI. See [WMI enablement on scanner host](#) on page 42.
- 2 If automatic updates are not enabled on your Extreme Security Console, download and install the Microsoft SCCM RPM.
- 3 On your Extreme Security Console, add an Microsoft SCCM scanner. See [Adding a Microsoft SCCM scanner](#) on page 43.
- 4 On your Extreme Security Console, create a scan schedule to import scan result data. See [Scheduling a vulnerability scan](#) on page 81.

# 14 WMI enablement on scanner host

---

Before you can configure a Microsoft SCCM scanner, you must configure your system DCOM settings for each host you want to monitor.

Ensure that the scanner host meets the following conditions:

- You are a member of the Administrators group on that host.
- One the following operating systems is installed:
  - Windows 2000
  - Windows 2003
  - Windows 2008
  - XP
  - Vista software
  - Windows 7



## Note

32-bit and 64-bit operating systems are supported.

---

- DCOM is configured and enabled.

If a firewall is installed on the host or is located between the host and Extreme Security (such as a hardware or other intermediary firewall), the firewall must be configured to allow DCOM communication. Configure the firewall to allow port 135 to be accessible on the host and allow DCOM ports (random ports above 1024). Depending on the version of Windows that you use, you might also need to configure specific ports to be accessible to DCOM. For more information, see your Windows documentation.

- Windows Management Instrumentation (WMI) is enabled.
- The remote registry service is activated.

For specific instructions about how to configure DCOM and WMI on Windows 2008 and Windows 7, see the documents on the IBM support website:

- [Windows 2008](http://www-01.ibm.com/support/docview.wss?uid=swg21681046) (http://www-01.ibm.com/support/docview.wss?uid=swg21681046)
- [Windows 7](http://www-01.ibm.com/support/docview.wss?uid=swg21678809) (http://www-01.ibm.com/support/docview.wss?uid=swg21678809)

# 15 Adding a Microsoft SCCM scanner

---

Ensure that WMI is enabled on your scanner host.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 Configure the following Microsoft SCCM parameters:

Parameter	Description
Scanner Name	The name to identify your scanner instance.
Managed Host	The managed host from your Extreme Security deployment that manages the scanner import.
Type	Microsoft SCCM
Host Name	The IP address or host name of the remote server that hosts the scan result files.
Domain	The domain used to connect to the remote server.

- 5 Configure the remaining parameters.
- 6 To configure a CIDR range for your scanner:
  - a Type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 7 Click **Save**.

# 16 nCircle IP360 scanner overview

## Exporting nCircle IP360 scan results to an SSH server Adding a nCircle IP360 scanner

Extreme Security can import XML2 scan reports from SSH servers that contain nCircle IP360 vulnerability information.

Extreme Security cannot connect directly with nCircle devices. You can configure an nCircle IP360 scanner device to export scan results in XML2 format to a remote SSH server. To import the most recent scan results from the remote server to Extreme Security, you can schedule a scan or poll the remote server for updates to the scan results.

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

To integrate an nCircle IP360 scanner, perform the following steps:

- 1 On your nCircle IP360 scanner, configure your nCircle scanner to export scan reports. See [Exporting nCircle IP360 scan results to an SSH server](#) on page 44.
- 2 On your Extreme Security Console, add an nCircle IP360 scanner. See [Adding a nCircle IP360 scanner](#) on page 45
- 3 On your Extreme Security Console, create a scan schedule to import scan result data. See [Scheduling a vulnerability scan](#) on page 81

## Exporting nCircle IP360 scan results to an SSH server

Extreme Security uses an automated export function to publish XML2 scan data from nCircle IP360 appliances. Extreme Security supports VnE Manager version IP360-6.5.2 to 6.8.2.8.

Ensure that the remote server is a UNIX system with SSH enabled.

- 1 Log in to the IP360 VNE Manager user interface.
- 2 From the navigation menu, select **Administer > System > VNE Manager > Automated Export**.
- 3 Click the **Export to File** tab.
- 4 Configure the export settings.

The export must be configured to use the XML2 format.

- 5 Record the target settings that are displayed in the user interface for the scan export. These settings are necessary to configure Extreme Security to integrate with your nCircle IP360 device.

## Adding a nCircle IP360 scanner

Extreme Security uses a Secure Shell (SSH) to access a remote server (SSH export server) to retrieve and interpret the scan data from nCircle IP360 appliances. Extreme Security supports VnE Manager version IP360-6.5.2 to 6.8.2.8.

This configuration requires the target settings that you recorded when you exported the XML2 scan data to the remote server.

If the scanner is configured to use a password, the SSH scanner server to which Extreme Security 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.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 Configure the following nCircle IP360 parameters:

Parameter	Description
Scanner Name	The name to identify your nCircle IP360 instance.
Managed Host	The managed host from your Extreme Security deployment that manages the scanner import.
Type	nCircle IP360
SSH Server Host Name	The IP address or host name of the remote server that hosts the scan result files.
SSH Port	The port number to connect to the remote server.
Remote Directory	The location of the scan result files.
File Pattern	The regular expression (regex) to filter the list of files that are specified in the <b>Remote Directory</b> field. To list all XML2 format files that end with XML, use the following entry: <code>XML2.*\ .xml</code>

- 5 Configure the remaining parameters.
- 6 To configure a CIDR range for your scanner:
  - a Type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 7 Click **Save**.
- 8 On the **Admin** tab, click **Deploy Changes**.

# 17 Nessus scanner overview

- Adding a Nessus scheduled live scan
- Adding a Nessus scheduled result import
- Adding a Nessus live scan with the XMLRPC API
- Adding a Nessus completed report import with the XMLRPC API
- Adding a Nessus live scan with the JSON API
- Adding a Nessus completed report import with the JSON API

Extreme Security can use a Nessus client and server relationship to retrieve vulnerability scan reports. You can also use the Nessus XMLRPC API or JSON API to access scan data directly from Nessus.

When you configure your Nessus client, you need to create a Nessus user account for your Extreme Security system. A unique user account ensures that Extreme Security has the correct credentials to log in and communicate with the Nessus server. After you create the user account, a connection test verifies the user credentials and remote access.



## Note

Do not install Nessus software on a critical system due to the CPU requirements when scans are active.

## Data collection options

The following options are available for data collection of vulnerability information from Nessus scanners:

<b>Scheduled Live Scan</b>	Live scans enable predefined scans to be started remotely over SSH in Nessus and the data is imported at the completion of the scan.
<b>Scheduled Results Import</b>	Static result files from completed scans are imported from a repository over SSH that contains the Nessus scan results.
<b>Scheduled Live Scan - XMLRPC API</b>	The XMLRPC enables predefined scans to be started remotely and actively collected by using XMLRPC API.  The Nessus XMLRPC API is only available on Nessus servers and clients with software V4.2 and higher.
<b>Scheduled Live Scan - JSON API</b>	Enables predefined scans to be started remotely and actively collected by using JSON API.
<b>Scheduled Completed Report Import - XMLRPC API</b>	Enables completed reports to be imported from the Nessus server using XMLRPC API.
<b>Scheduled Completed Report Import - JSON API</b>	Enables completed reports to be imported from the Nessus server.

## Server certificates

Before you add a scanner, a server certificate is required to support HTTPS connections. Extreme Security supports certificates with the following file extensions: `.crt`, `.cert`, or `.der`. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using Secure Copy (SCP) or Secure File Transfer Protocol (SFTP).
- To automatically download the certificate to the `/opt/qradar/conf/trusted_certificates` directory, SSH into the Console or managed host and type the following command:

```
/opt/qradar/bin/getcert.sh <IP_or_Hostname>  
<optional_port_(443_default)>
```

## Adding a Nessus scheduled live scan

A live scan runs on your Nessus server and imports the result data from a temporary directory on the Nessus client that contains the scan report data.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Nessus scanner.
- 5 From the **Managed Host** list, select the managed host that manages the scanner import.
- 6 From the **Type** list, select **Nessus Scanner**.
- 7 From the **Collection Type** list, select **Scheduled Live Scan**.
- 8 .

- 9 Configure the following parameters:

Parameter	Description
Server Username	The user name to access Nessus server.
Server Password	Your Nessus server password must not contain the exclamation mark (!) character or authentication failures can occur over SSH.
Client Temp Dir	The directory path of the Nessus client that Extreme Security can use to store temporary files.  Extreme Security uses the temporary directory on the Nessus client to upload scan targets and read scan results. Temporary files are removed from the temporary directory when the scan completes and the scan report is downloaded.
Nessus Executable	The directory path to the executable file on the Nessus server.
Nessus Configuration File	The directory path to the Nessus configuration file on the Nessus client.
Client Hostname	The host name or IP address of the Nessus client.
Client SSH Port	The SSH port on the Nessus server that can be used to retrieve scan result files.
Client Username	The user name to authenticate the SSH connection.
Client Password	If the <b>Enable Key Authentication</b> field is enabled, the password is ignored.  If the scanner is configured to use a password, the SSH scanner server that connects to Extreme Security must support password authentication. If it does not, SSH authentication for the scanner fails. Ensure the following line is displayed in your <code>/etc/ssh/sshd_config</code> file: <code>PasswordAuthentication yes</code> . If your scanner server does not use OpenSSH, see the vendor documentation for the scanner configuration information.
Private Key File	The directory path to the key file. If a key file does not exist, you must create the <code>vis.ssh.key</code> file.
CIDR Mask	The size of the subnet that you want to scan. The value represents the largest portion of the subnet the scanner can scan at one time. The mask segments the scan to optimize the scan performance.

- 10 To configure a CIDR range for your scanner:
- Type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - Click **Add**.
- 11 Click **Save**.
- 12 On the **Admin** tab, click **Deploy Changes**.



## Adding a Nessus scheduled result import

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

A completed scan report can be stored on a Nessus server or a file repository. Extreme Security connects to the Nessus server or file repository by using SSH and then imports completed scan report files. The reports are filtered by a defined regular expression or maximum report age. Extreme Security supports imports of Nessus scan reports in `.nessus` format or scan reports that are exported to a Nessus output format, such as XML2.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Nessus scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Nessus Scanner**.
- 7 From the **Collection Type** list, select **Scheduled Results Import**.
- 8 In the **Remote Results Hostname** field, type the IP address or hostname of the Nessus client or server that hosts your Nessus or XML2 scan result files.
- 9 Choose one of the following authentication options:

Option	Description
<b>Login Username</b>	<p>To authenticate with a user name and password:</p> <ol style="list-style-type: none"> <li>1 In the <b>SSH Username</b> field, type the user name to access the Nessus scanner or the repository that hosts the scan result files.</li> <li>2 In the <b>SSH Password</b> field, type the password that is associated with the user name.</li> </ol> <p>The password must not contain the exclamation mark (!) character. This character might cause authentication failures over SSH.</p>
<b>Enable Key Authorization</b>	<p>To authenticate with a key-based authentication file:</p> <ol style="list-style-type: none"> <li>1 Select the <b>Enable Key Authentication</b> check box.</li> <li>2 In the <b>Private Key File</b> field, type the directory path to the key file.</li> </ol> <p>The default directory for the key file is <code>/opt/gradar/conf/vis.ssh.key</code>. If a key file does not exist, you must create the <code>vis.ssh.key</code> file.</p>

- 10 In the **Remote Results Directory** field, type the directory location of the scan result files.  
The default directory path is `./`.
- 11 In the **File Name Pattern** field, type a regular expression (regex) to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing.  
By default, the **Report Name Pattern** field contains `.*\ .nessus` as the regex pattern. The `.*\ .nessus` pattern imports all Nessus formatted result files in the remote directory.
- 12 In the **Max Reports Age (Days)** field, type the maximum file age for your scan results file.  
Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts. The default value is 7 days.

- 13 To configure a CIDR range for your scanner:
  - a In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 14 Click **Save**.

## Adding a Nessus live scan with the XMLRPC API

---

Extreme Networks Security Analytics can use the XMLRPC API to start a pre-configured scan that is based on a scan name and optional policy name on the Nessus server.

To start a live scan from Extreme Security, 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 point your mouse over the Nessus scanner in the **Scan Scheduling** window to view the percentage of the live scan that is complete. After the live scan reaches completion, Extreme Security uses the XMLRPC API to retrieve the scan data and update the vulnerability information for your assets.

The Nessus XMLRPC API is only available on Nessus servers and clients with software v4.2 and higher.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Nessus scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Nessus Scanner**.
- 7 From the **Collection Type** list, select **Scheduled Live Scan - XMLRPC API**.

- 8 Configure the following parameters:

Parameter	Description
Hostname	The IP address or host name of the Nessus server.
Port	The port number the Nessus server.
Username	The user name that is required to access to access Nessus server
Password	Your Nessus server password must not contain the exclamation mark (!) character or authentication failures can occur over SSH.
Scan Name	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 Extreme Security Scan. This field does not support by using the ampersand (&) character in this field.
Policy Name	The name of a policy on your Nessus server to start a live scan.  The policy must exist on the Nessus server when the system attempts to start the scan. If the policy does not exist, an error is displayed in the <b>Status</b> column. Systems can have custom policy names, but several default policy names are included. <b>External Network Scan</b> , <b>Internal Network Scan</b> , <b>Web App Tests</b> , <b>Prepare for PCI DSS audits</b> are default policy names.

- 9 To configure a CIDR range for your scanner:
- In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - Click **Add**.
- 10 Click **Save**.

## Adding a Nessus completed report import with the XMLRPC API

A scheduled results import using the XMLRPC API enables completed vulnerability reports to be downloaded from the Nessus server.

Extreme Security connects to your Nessus server and downloads data from any completed reports matching the report name and maximum report age filter. The Nessus XMLRPC API is available on Nessus servers and clients using software v4.2 and higher.

- Click the **Admin** tab.
- Click the **VA Scanners** icon.
- Click **Add**.
- In the **Scanner Name** field, type a name to identify your Nessus server.
- From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.

- 6 From the **Type** list, select **Scheduled Completed Report Import - XMLRPC AP**.
- 7 In the **Hostname** field, type the IP address or hostname of the IBM Tivoli Endpoint Manager containing the vulnerabilities you want to retrieve with the SOAP API.
- 8 In the **Port** field, type the port number the Nessus server.  
The default API port value is 8834 .
- 9 In the **Username** field, type the username required to access the Nessus server.
- 10 In the **Password** field, type the password required to access the Nessus server.
- 11 In the **Report Name Pattern** field, 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.  
By default, the Report Name Pattern field contains `. *` as the regex pattern. The `. *` pattern imports all nessus formatted result files in the remote directory.
- 12 In the **Max Reports Age (Days)** field, type the maximum file age for your scan results file.  
Files that are older than the specified days and timestamp on the report file are excluded when the schedule scan starts. The default value is 7 days.
- 13 To configure a CIDR range for your scanner:
  - a In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 14 Click **Save**.

## Adding a Nessus live scan with the JSON API

Extreme Networks Security Analytics can use the JSON API to start a pre-configured scan that is based on a scan name and optional policy name on the Nessus server.

To start a live scan from Extreme Security, 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 point your mouse over the Nessus scanner in the **Scan Scheduling** window to view the percentage of the live scan that is complete. After the live scan reaches completion, Extreme Security uses the JSON API to retrieve the scan data and update the vulnerability information for your assets.

The Nessus JSON API is only available on Nessus servers and clients with software v6.0 and higher.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Nessus scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Nessus Scanner**.
- 7 From the **Collection Type** list, select **Scheduled Live Scan - JSON API**.

- 8 Configure the following parameters:

Parameter	Description
Hostname	The IP address or host name of the Nessus server.
Port	The port number the Nessus server.
Username	The user name that is required to access Nessus server
Password	Your Nessus server password must not contain the exclamation mark (!) character or authentication failures can occur.
Scan Name	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 Extreme Security Scan. This field does not support by using the ampersand (&) character in this field.
Policy Name	The name of a policy on your Nessus server to start a live scan.  The policy must exist on the Nessus server when the system attempts to start the scan. If the policy does not exist, an error is displayed in the <b>Status</b> column. Systems can have custom policy names, but several default policy names are included. <b>External Network Scan</b> , <b>Internal Network Scan</b> , <b>Web App Tests</b> , <b>Prepare for PCI DSS audits</b> are default policy names.
Scanner Name	If there is more than one Nessus scanner in your deployment, specify the name of the scanner that you want to run scans on.

- 9 To configure a CIDR range for your scanner:
- In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - Click **Add**.
- 10 Click **Save**.

## Adding a Nessus completed report import with the JSON API

A scheduled results import retrieves completed Nessus scan reports from an external location by using the JSON API.

A completed scan report can be stored on a Nessus server or a file repository. Extreme Networks Security Analytics connects to the Nessus server or file repository by using the JSON API and then imports completed scan report files. The reports are filtered by a defined expression or maximum report age.

The Nessus JSON API is only available on Nessus servers and clients with software v6.0 and higher.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Nessus scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Nessus Scanner**.
- 7 From the **Collection Type** list, select **Scheduled Completed Report Import - JSON API**.
- 8 Configure the following parameters:

Parameter	Description
<b>Hostname</b>	The IP address or host name of the Nessus server.
<b>Port</b>	The port number the Nessus server.
<b>Username</b>	The user name that is required to access Nessus server
<b>Password</b>	Your Nessus server password.
<b>Report Name Filter</b>	Filters the list of files that are specified in the Remote Directory. All matching files are included in the processing. By default, the Report Name Pattern field contains <code>.*</code> as the filter.
<b>Report Max Age (days)</b>	The maximum file age for your scan results file. Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts. The default value is 7 days.

- 9 To configure a CIDR range for your scanner:
  - a In the text field, type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 10 Click **Save**.

# 18 netVigilance SecureScout scanner overview

---

## Adding a netVigilance SecureScout scan

Extreme Security can collect vulnerability data from an SQL database on the SecureScout scanner by polling for data with JDBC.

netVigilance SecureScout NX and SecureScout SP store scan results in an SQL database. This database can be a Microsoft MSDE or SQL Server database. To collect vulnerabilities, Extreme Security connects to the remote database to locate the latest scan results for a given IP address. The data returned updates the asset profile in Extreme Security with the asset IP address, discovered services, and vulnerabilities. Extreme Security supports SecureScout scanner software version 2.6.

We suggest that administrators create a special user in your SecureScout database for Extreme Security to poll for vulnerability data.

The database user you create must have select permissions to the following tables:

- HOST
- JOB
- JOB\_HOST
- SERVICE
- TCRESULT
- TESTCASE
- PROPERTY
- PROP\_VALUE
- WKS
- IPSORT - The database user must have execute permission for this table.

To add a scanner configuration, see [Adding a netVigilance SecureScout scan](#) on page 55.

## Adding a netVigilance SecureScout scan

---

Administrators can add a SecureScout scanner to query for vulnerability data with JDBC.

To query for vulnerability data, Extreme Security you must have appropriate administrative access to poll the SecureScout scanner with JDBC. Administrators must also ensure that firewalls, including the firewall on the SecureScout host permits a connection from the managed host responsible for the scan to the SecureScout scanner.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.

- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your SecureScout server.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **SecureScout Scanner**.
- 7 In the **Database Hostname** field, type the IP address or hostname of the SecureScout database server that contains the SQL server.
- 8 In the **Login Name** field, type the username required to access the SQL database of the SecureScout scanner.
- 9 Optional. In the **Login Password** field, type the password required to access the SQL database of the SecureScout scanner.
- 10 In the **Database Name** field, type `scs`.
- 11 In the **Database Port** field, type the TCP port you want the SQL server to monitor for connections. The default value is 1433.
- 12 To configure a CIDR range for your scanner:
  - a In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 13 Click **Save**.
- 14 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.



# 19 Nmap scanner overview

## Adding a Nmap remote result import Adding a Nmap remote live scan

Extreme Security uses SSH to communicate with the Nmap server to either start remote Nmap scans or download the completed Nmap scan results.

When administrators configure an Nmap scan, a specific Nmap user account can be created for the Extreme Security system. A unique user account ensures that Extreme Security possesses the credentials required to log in and communicate with the Nmap server. After the user account creation is complete, administrators can test the connection from Extreme Security to the Nmap client with SSH to verify the user credentials. This ensures that each system can communicate before the system attempt to download vulnerability scan data or start a live scan.

The following options are available for data collection of vulnerability information from Nmap scanners:

- Remote live scan. Live scans use the Nmap binary file to remotely start scans. After the live scan completes, the data is imported over SSH. See [Adding a Nmap remote live scan](#) on page 58.
- Remote results import. The result data from a previously completed scan is imported over SSH. See [Adding a Nmap remote result import](#) on page 57

## Adding a Nmap remote result import

A remote results import retrieves completed Nmap scan reports over SSH.

Scans must be generated in XML format using the `-oX` option on your Nmap scanner. After you add your Nmap scanner, you must assign a scan schedule to specify the frequency that the vulnerability data is imported from scanner.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Nmap scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Nessus Scanner**.
- 7 From the **Collection Type** list, select **Remote Results Import**.
- 8 In the **Server Hostname** field, type the hostname or IP address of the remote system that hosts the Nmap client. We suggest that administrators host Nmap on a UNIX™-based system with SSH enabled.

- 9 Choose one of the following authentication options:

Option	Description
<b>Login Username</b>	<p>To authenticate with a user name and password:</p> <ol style="list-style-type: none"> <li>1 In the <b>Server Username</b> field, type the username required to access the remote system hosting the Nmap client.</li> <li>2 In the <b>Login Password</b> field, type the password associated with the user name.</li> </ol> <p>The password must not contain the ! character. This character could cause authentication failures over SSH.</p> <p>If the scanner is configured to use a password, the SSH scanner server to that connects to Extreme Security must support password authentication.</p> <p>If it does not, SSH authentication for the scanner fails. Ensure the following line is displayed in your <code>/etc/ssh/sshd_config</code> file: <code>PasswordAuthentication yes</code>.</p> <p>If your scanner server does not use OpenSSH, see the vendor documentation for the scanner configuration information.</p>
<b>Enable Key Authorization</b>	<p>To authenticate with a key-based authentication file:</p> <ol style="list-style-type: none"> <li>1 Select the <b>Enable Key Authentication</b> check box.</li> <li>2 In the <b>Private Key File</b> field, type the directory path to the key file.</li> </ol> <p>The default is directory for the key file is <code>/opt/gradar/conf/vis.ssh.key</code>. If a key file does not exist, you must create the <code>vis.ssh.key</code> file.</p>

- 10 In the **Remote Folder** field, type the directory location of the scan result files.
- 11 In the **Remote File Pattern** field, type a regular expression (regex) required to filter the list of files specified in the remote folder. All matching files are included in the processing.
- The default regex pattern to retrieve Nmap results is `.*\.*xml`. The `.*\.*xml` pattern imports all xml result files in the remote folder.
- Scan reports imported and processed are not deleted from the remote folder. We suggest that you schedule a cron job to delete previously processed scan reports.
- 12 To configure a CIDR range for your scanner:
- a In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 13 Click **Save**.
- 14 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81

## Adding a Nmap remote live scan

monitors the status of the live scan in progress and waits for the Nmap server to complete the scan. After the scan completes, the vulnerability results are downloaded over SSH.

Several types of Nmap port scans require Nmap to run as a root user. Therefore, Extreme Security 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 root access credentials to Extreme Security when you add the

scanner. Alternately, you can have your administrator configure the Nmap binary with `setuid root`. See your Nmap administrator for more information.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Nmap scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Nmap Scanner**.
- 7 From the **Scan Type** list, select **Remote Live Scan**.
- 8 In the **Server Hostname** field, type the IP address or hostname of the Nmap server.
- 9 Choose one of the following authentication options:

Option	Description
<b>Server Username</b>	<p>To authenticate with a user name and password:</p> <ol style="list-style-type: none"> <li>1 In the <b>Server Username</b> field, type the username required to access the remote system hosting the Nmap client using SSH.</li> <li>2 In the <b>Login Password</b> field, type the password associated with the user name.</li> </ol> <p>If the <b>OS Detection</b> check box is selected, the username must have root privileges.</p>
<b>Enable Key Authorization</b>	<p>To authenticate with a key-based authentication file:</p> <ol style="list-style-type: none"> <li>1 Select the <b>Enable Key Authentication</b> check box.</li> <li>2 In the <b>Private Key File</b> field, type the directory path to the key file.</li> </ol> <p>The default is directory for the key file is <code>/opt/gradar/conf/vis.ssh.key</code>. If a key file does not exist, you must create the <code>vis.ssh.key</code> file.</p> <p>If the scanner is configured to use a password, the SSH scanner server to that connects to Extreme Security must support password authentication.</p> <p>If it does not, SSH authentication for the scanner fails. Ensure the following line is displayed in your <code>/etc/ssh/sshd_config</code> file: <code>PasswordAuthentication yes</code>.</p> <p>If your scanner server does not use OpenSSH, see the vendor documentation for the scanner configuration information.</p>

- 10 In the **Nmap Executable** field, type the full directory path and filename of the Nmap binary file.
 

The default directory path to the binary file is `/usr/bin/Nmap`.
- 11 Select an option for the **Disable Ping** check box.
 

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.
- 12 Select an option for the **OS Detection** check box:
  - Select this check box to enable operating system detection in Nmap. You must provide the scanner with root privileges to use this option.
  - Clear this check box to receive Nmap results without operating system detection.

- 13 From the **Max RTT Timeout** list, select a timeout value.

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). If you specify a timeout period of 50 milliseconds, then we suggest that the devices that are scanned be in the local network. Devices in remote networks can use a timeout value of 1 second.

- 14 Select an option from the **Timing Template** list. The options include:

- Paranoid - This option produces a slow, non-intrusive assessment.
- Sneaky - This option produces a slow, non-intrusive assessment, but waits 15 seconds between scans.
- Polite - This option is slower than normal and intended to ease the load on the network.
- Normal - This option is the standard scan behavior.
- Aggressive - This option is faster than a normal scan and more resource intensive.
- Insane - This option is not as accurate as slower scans and only suitable for very fast networks.
- 

- 15 In the **CIDR Mask** field, type the size of the subnet scanned.

The value specified for the mask represents the largest portion of the subnet the scanner can scan at one time. The mask segments the scan to optimize the scan performance.

- 16 To configure a CIDR range for your scanner:

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

- 17 Click **Save**.

- 18 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81

# 20 Outpost24 Vulnerability Scanner overview

## Creating an Outpost24 API authentication token for Extreme Security

Extreme Networks Security Analytics uses HTTPS to communicate with the Outpost24 vulnerability scanner API to download asset and vulnerability data from previously completed scans.

The following table lists the specifications for the Outpost24 vulnerability scanner:

**Table 5: Outpost24 Vulnerability Scanner specifications**

Specification	Value
Scanner name	Outpost24 Vulnerability Scanner
Supported versions	HIAB V4.1 OutScan V4.1
Connection type	HTTPS
More information	<a href="http://www.outpost24.com/">Outpost24 website</a> (http://www.outpost24.com/)

To configure Extreme Security to download asset and vulnerability data from an Outpost24 vulnerability scanner, complete the following steps:

- 1 If automatic updates are not enabled, download and install the most recent version of the Outpost24 Vulnerability Scanner RPM on your Extreme Security system.
- 2 On the Outpost24 vulnerability scanner, create an application token for Extreme Security.
- 3 On the Extreme Security Console, add the Outpost24 vulnerability scanner. Configure all required parameters and use the following table to identify specific Outpost24 values:

**Table 6: Outpost24 Vulnerability Scanner parameters**

Parameter	Value
Type	Outpost24 Vulnerability Scanner
Server Hostname	The host name of the Outpost24 vulnerability scanner device.
Port	443
API token	Must use the API token that you created on the Outpost24 vulnerability scanner device.

- 4 Schedule a scan.

### Related Links

[Creating an Outpost24 API authentication token for Extreme Security](#) on page 62

To enable Extreme Networks Security Analytics to use the Outpost24 API to download asset and vulnerability data, create an Application Access Token on the Outpost24 vulnerability scanner.

[Scheduling a vulnerability scan](#) on page 81

Scan schedules are intervals assigned to scanners that determine when vulnerability assessment data is imported from external scanning appliances in your network. Scan schedules can also define CIDR ranges or subnets that are included in the data import when the vulnerability data import occurs.

## Creating an Outpost24 API authentication token for Extreme Security

---

To enable Extreme Networks Security Analytics to use the Outpost24 API to download asset and vulnerability data, create an Application Access Token on the Outpost24 vulnerability scanner.

- 1 Log in to Outpost24 vulnerability scanner.
- 2 Select **Settings > Account**.
- 3 Click the **Security Policy** tab.
- 4 In the **Application Access Tokens** pane, click **New**.
- 5 In the **Maintaining App Access Token** window, ensure that the **Active** check box is selected.
- 6 Type a name for the application, for example, Extreme Security.
- 7 Configure the IP restrictions and user access rights.
- 8 Click **Save**.
- 9 Copy the 64 character authentication token to a file.

On your Extreme Security system, add the Outpost24 vulnerability scanner.

# 21 Positive Technologies MaxPatrol

## Integrating Positive Technologies MaxPatrol with Extreme Security Adding a Positive Technologies MaxPatrol scanner

You can add a Positive Technologies MaxPatrol scanner to your Extreme Networks Security Analytics deployment.

At intervals that are determined by a scan schedule, Extreme Security imports XML file results that contain MaxPatrol vulnerabilities. The MaxPatrol scanner imports files from a remote server that contains the exported scan data.

The following table provides Positive Technologies MaxPatrol scanner details:

**Table 7: Positive Technologies MaxPatrol Scanner details**

Vendor	Positive Technologies
Scanner name	MaxPatrol
Supported versions	V8.24.4 and later

Use the following procedures to integrate Positive Technologies MaxPatrol with Extreme Security

- 1 Configure your Positive Technologies MaxPatrol scanner to export scan reports. Enable the Extreme Security compatible XML file vulnerability exports. To obtain the necessary files and configuration procedures, contact Positive Technologies Customer Support.
- 2 On your Extreme Security Console, add a Positive Technologies MaxPatrol scanner.
- 3 On your Extreme Security Console, create a scan schedule to import scan result data.

## Integrating Positive Technologies MaxPatrol with Extreme Security

Procedures that are required to integrate Positive Technologies MaxPatrol with Extreme Security.

- 1 Configure your Positive Technologies MaxPatrol scanner to export scan reports. Enable the Extreme Security compatible XML file vulnerability exports. To obtain the necessary files and configuration procedures, contact Positive Technologies Customer Support.
- 2 On your Extreme Security Console, add a Positive Technologies MaxPatrol scanner.
- 3 On your Extreme Security Console, create a scan schedule to import scan result data.

## Adding a Positive Technologies MaxPatrol scanner

Add a Positive Technologies MaxPatrol scanner to your Extreme Networks Security Analytics deployment.

Ensure that the following prerequisites are met:

- The Positive Technologies MaxPatrol system is configured to export Extreme Security compatible XML vulnerability reports.
- An SFTP or SMB share is set up and contains the exported XML vulnerability reports.

The following table describes Positive Technologies MaxPatrol scanner parameters when you select SFTP as the import method:

**Table 8: Positive Technologies MaxPatrol scanner SFTP properties**

Parameter	Description
Remote Hostname	The IP address or host name of the server that has the scan results file.
Login Username	The user name that Extreme Security uses to log in to the server.
Enable Key Authentication	Specified Extreme Security authenticates with a key-based authentication file.
Remote directory	The location of the scan result files.
Private Key File	The full path to the file that contains the private key. If a key file does not exist, you must create the <code>vis.ssh.key</code> file.
File Name Pattern	The regular expression (regex) required to filter the list of files in the Remote Directory. The <code>.*\.xml</code> pattern imports all XML files in the remote directory.

The following table describes Positive Technologies MaxPatrol scanner parameters when you select SMB Share as the import method:

**Table 9: Positive Technologies MaxPatrol scanner SMB Share properties**

Parameter	Description
Hostname	The IP address or host name of the SMB Share.
Login Username	The user uses Extreme Security to log in to SMB Share.
Domain	The domain that is used to connect to the SMB Share.
SMB Folder Path	The full path to the share from the root of the SMB host. Use forward slashes, for example, <code>/share/logs/</code> .
File Name Pattern	The regular expression (regex) required to filter the list of files in the Remote Directory. The <code>.*\.xml</code> pattern imports all xml files in the remote directory.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.



- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify the Positive Technologies MaxPatrol scanner.
- 5 From the **Managed Host** list, select the managed host that manages the scanner import.
- 6 From the **Type** list, select **Positive Technologies MaxPatrol Scanner**.
- 7 Configure the parameters.
- 8 Configure a CIDR range for the scanner.
- 9 Click **Save**.
- 10 On the **Admin** tab, click **Deploy Changes**.

For more information about how to create a scan schedule, see [Scheduling a vulnerability scan](#) on page 81.

# 22 Qualys scanner overview

---

**Adding a Qualys detection scanner**

**Adding a Qualys scheduled live scan**

**Adding a Qualys scheduled import asset data report**

**Adding a Qualys scheduled import scan report**

Extreme Security can retrieve vulnerability information from the QualysGuard Host Detection List API or download scan reports directly from a QualysGuard appliance. Extreme Security supports integration with QualysGuard appliances that use software version 4.7 through 7.10.

## Qualys Detection Scanners

Add a Qualys Detection Scanner if you want to use the QualysGuard Host Detection List API to query multiple scan reports to collect vulnerability data for assets. The data that the query returns contains the vulnerabilities as identification numbers, which Extreme Security compares against the most recent Qualys Vulnerability Knowledge Base. The Qualys Detection Scanner does not support live scans, but enables the Qualys Detection Scanner to retrieve vulnerability information aggregated across multiple scan reports. Extreme Security supports key search parameters to filter for the information that you want to collect. You can also configure how frequently Extreme Security retrieves and caches the Qualys Vulnerability Knowledge Base.

## Qualys Scanners

Add a Qualys scanner if you want to import specific live or imported reports that include scan or asset data. When you add a Qualys scanner, you can choose from the following collection types:

- Scheduled live - Scan Report
- Scheduled Import - Asset Data Report
- Scheduled Import - Scan Report

## Adding a Qualys detection scanner

---

Add a Qualys detection scanner to use an API to query across multiple scan reports to collect vulnerability data for assets. The Qualys detection scanner uses the QualysGuard Host Detection List API.

Before you add this scanner, a server certificate is required to support HTTPS connections. Download the certificate from the Qualys URL for your region.

### Examples

- [Qualys US API site](http://qualysapi.qualys.com) (<http://qualysapi.qualys.com>)

- [Qualys European site](http://qualysapi.qualys.eu) (http://qualysapi.qualys.eu)

Extreme Security supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Qualys detection scanner.
- 5 From the **Managed Host** list, select the managed host that manages the scanner import.
- 6 From the **Type** list, select **Qualys Detection Scanner**.

- 7 Configure the following parameters:

Parameter	Description
Qualys Server Host Name	The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type <code>qualysapi.qualys.com</code> or <code>qualysapi.qualys.eu</code> .
Qualys Username	The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation.
Operating System Filter	The regular expression (regex) to filter the scan data by the operating system.
Asset Group Names	A comma-separated list to query IP addresses by the asset group name.
Host Scan Time Filter (Days)	Host scan times that are older than the specified number of days are excluded from the results that Qualys returns.
Qualys Vulnerability Retention Period (Days)	The number of days that you want Extreme Security to store the Qualys Vulnerability Knowledge Base. If a scan is scheduled and the retention period expires, the system downloads an update.

#### Attention



After you create this scanner for the first time, subsequent updates to this retention period might not take effect. For this change to take effect after the initial creation, you might need to delete or clear the cache.

- Force Qualys Vulnerability Update** Forces the system to update to the Qualys Vulnerability Knowledge Base for each scheduled scan.
- 8 Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
- 9 Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
- 10 Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.

#### Restriction



The QualysGuard Host Detection List API accepts only CIDR ranges to a maximum of a single class A or /8 and does not accept the local host IP address (127.0.0.1).

- 11 Click **Save**.
- 12 On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

## Adding a Qualys scheduled live scan

Add a scheduled live scan to start preconfigured scans on the Qualys Scanner and then collect the completed scan results.

Before you add this scanner, a server certificate is required to support HTTPS connections. Extreme Security supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Qualys scanner.
- 5 From the **Managed Host** list, select the managed host that manages the scanner import.
- 6 From the **Type** list, select **Qualys Scanner**.
- 7 Configure the following parameters:

Parameter	Description
Qualys Server Host Name	The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type <code>qualysapi.qualys.com</code> or <code>qualysapi.qualys.eu</code> .
Qualys Username	The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation.

- 8 Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
- 9 Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
- 10 From the **Collection Type** list, select **Scheduled Live - Scan Report**.
- 11 Configure the following parameters:

Parameter	Description
Scanner Name	To obtain the scanner name, contact your network administrator. Public scanning appliance must clear the name from this field.
Option Profiles	The name of the option profile that determines which live scan is started. Live scans support only one option profile name for each scanner configuration.

- 12 Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
- 13 Click **Save**.
- 14 On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

## Adding a Qualys scheduled import asset data report

Add an asset report data import to schedule Extreme Security to retrieve a single asset report from your Qualys scanner.

Before you add this scanner, a server certificate is required to support HTTPS connections. Extreme Security supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Qualys scanner.
- 5 From the **Managed Host** list, select the managed host that manages the scanner import.
- 6 From the **Type** list, select **Qualys Scanner**.
- 7 Configure the following parameters:

Parameter	Description
<b>Qualys Server Host Name</b>	The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type <code>qualysapi.qualys.com</code> or <code>qualysapi.qualys.eu</code> .
<b>Qualys Username</b>	The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation.

- 8 Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
- 9 Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
- 10 From the **Collection Type** list, select **Scheduled Import - Asset Data Report**.

- Configure the following parameters:

Parameter	Description
Report Template Title	The report template title to replace the default asset data report title.
Max Reports Age (Days)	Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts.
Import File	The directory path to download and import a single asset report from Qualys. If you specify an import file location, Extreme Security downloads the contents of the asset report from Qualys to a local directory and imports the file. If you leave this field blank or if the file or directory cannot be found, the Qualys scanner uses the API to retrieve the asset report by using the value in the <b>Report Template Title</b> field.

- Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
- Optional: To enable Extreme Security to create custom vulnerabilities from the live scan data, select the **Enable Custom Vulnerability Creation** check box and select options that you want to include.
- Click **Save**.
- On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

## Adding a Qualys scheduled import scan report

Add a scan report data import to schedule Extreme Security to retrieve scan reports from your Qualys scanner.

Before you add this scanner, a server certificate is required to support HTTPS connections. Extreme Security supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
  - SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.
- Click the **Admin** tab.
  - Click the **VA Scanners** icon.
  - Click **Add**.
  - In the **Scanner Name** field, type a name to identify your Qualys scanner.
  - From the **Managed Host** list, select the managed host that manages the scanner import.
  - From the **Type** list, select **Qualys Scanner**.

- 7 Configure the following parameters:

Parameter	Description
Qualys Server Host Name	The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type <code>qualysapi.qualys.com</code> or <code>qualysapi.qualys.eu</code> .
Qualys Username	The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation.

- 8 Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
- 9 Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
- 10 From the **Collection Type** list, select **Scheduled Import - Scan Report**.
- 11 Configure the following parameters:

Parameter	Description
Option Profiles	The name of the option profile to determine which scan to start. Extreme Security retrieves the completed live scan data after the live scan completes. Live scans support only one option profile name per scanner configuration.
Scan Report Name Pattern	The regular expression (regex) to filter the list of scan reports.
Max Reports Age (Days)	Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts.
Import File	The directory path to download and import a single scan report from Qualys, for example, <code>/qualys_logs/test_report.xml</code> . If you specify an import file location, QRadar downloads the contents of the scan report from Qualys to a local directory and imports the file. If you leave this field blank or if the file or directory cannot be found, the Qualys scanner uses the API to retrieve the scan report by using the value in the <b>Options Profile</b> field.

- 12 Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
- 13 Optional: To enable Extreme Security to create custom vulnerabilities from the live scan data, select the **Enable Custom Vulnerability Creation** check box and select options that you want to include.
- 14 Click **Save**.
- 15 On the **Admin** tab, click **Deploy Changes**.

Any changes to the proxy configuration requires a **Deploy Full Configuration**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.



# 23 Rapid7 NeXpose scanners overview

## Adding a Rapid7 NeXpose scanner API site import Adding a Rapid7 NeXpose scanner local file import

Rapid7 NeXpose scanners can provide site data reports to Extreme Security to import vulnerabilities known about your network.

The following options are available to collect vulnerability information from Rapid7 NeXpose scanners:

- Site import of an adhoc reports through the Rapid7 API. See [Adding a Rapid7 NeXpose scanner API site import](#) on page 73.
- Site import of a local file. See [Adding a Rapid7 NeXpose scanner local file import](#) on page 74

## Adding a Rapid7 NeXpose scanner API site import

API imports enable Extreme Security to import ad hoc report data for vulnerabilities on your sites from Rapid7 NeXpose scanners. The site data the scan schedule imports depends on the site name.

Before you add this scanner, a server certificate is required to support HTTPS connections. Extreme Security supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Rapid7 NeXpose scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Rapid7 Nexpose Scanner**.
- 7 From the **Import Type** list, select **Import Site Data - Adhoc Report via API**.
- 8 In the **Remote Hostname** field, type the IP address or host name of the Rapid7 NeXpose scanner.

- 9 In the **Login Username** field, type the user name that to access the Rapid7 NeXpose scanner.  
The login must be a valid user. The user name can be obtained from the Rapid7 NeXpose user interface or from the Rapid7 NeXpose administrator.
- 10 In the **Login Password** field, type the password to access the Rapid7 NeXpose scanner.
- 11 In the **Port** field, type the port that is used to connect to the Rapid7 NeXpose Security Console.  
The port number is the same port to connect to the Rapid7 NeXpose user interface.
- 12 In the **Site Name Pattern** field, type the regular expression (regex) to determine which Rapid7 NeXpose sites to include in the scan. All sites that match the pattern are included when the scan schedule starts.  
The default value regular expression is `. *` to import all site names.
- 13 In the **Port** field, type the port that is used to connect to the Rapid7 NeXpose Security Console.
- 14 In the **Cache Timeout (Minutes)** field, type the length of time the data from the last generated scan report is stored in the cache.  
If the cache timeout limit expires, new vulnerability data is requested from the API when the scheduled scan starts.
- 15 To configure a CIDR range for the scanner:
  - a In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 16 Click **Save**.
- 17 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.

## Adding a Rapid7 NeXpose scanner local file import

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

Before you add this scanner, a server certificate is required to support HTTPS connections. Extreme Security supports certificates with the following file extensions: `.cert`, `.cert`, or `.der`. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Local file imports collect vulnerabilities for a site from a local file that is downloaded. The Rapid7 NeXpose XML file that contains the site and vulnerability information must be copied from your Rapid7 NeXpose appliance to the Console or managed host you specify when the scanner is added to Extreme Security. The directory on the managed host must exist before the system can copy site reports to the

managed host. Administrators can configure the site files to copy to the managed host files can be copied using Secure Copy (SCP) or Secure File Transfer Protocol (SFTP).

**Note**

Site files that are imported are not deleted from the import folder, but renamed to `.processed0`. Administrators can create a cron job to delete previously processed site files, if required.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your Rapid7 NeXpose scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Rapid7 Nexpose Scanner**.
- 7 From the **Import Type** list, select **Import Site Data - Local File**.
- 8 In the **Import Folder** field, type the directory path to the XML vulnerability data.  
If you specify an import folder, you must move the vulnerability data from your Rapid7 NeXpose scanner to Extreme Security.
- 9 In the **Import Name Pattern** field, 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 from the import folder.
- 10 To configure a CIDR range for your scanner:
  - a In the text field, type the CIDR range you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 11 Click **Save**.
- 12 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.

# 24 SAINT scanner overview

## Configuring a SAINTwriter template Adding a SAINT vulnerability scan

Administrators can integrate their Security Administrator's Integrated Network Tool (SAINT) vulnerability scanners with Extreme Security for SAINT appliances with V7.4.x software.

Administrators can add SAINT scanners to Extreme Security to collect SAINT vulnerability data for hosts, including Mac addresses, ports, and service information. The SAINT scanner identifies vulnerabilities based on the specified scan level and uses SAINTwriter to generate custom reports. Therefore, your SAINT system must include a custom SAINTwriter report template and scans that runs regularly to ensure the results are current.

The following data collection types are supported for SAINT scanner configurations:

- Live scan - Start a remote scans on the SAINT scanner. The live scan generates vulnerability report based on the session name, which is imported after the scan completes.
- Report only - Import completed reports from the SAINT scanner based on the session name.

To configure a template for your report, see [Configuring a SAINTwriter template](#) on page 76.

## Configuring a SAINTwriter template

Before administrators can add and import vulnerabilities from a SAINT scanner, a template must be configured in SAINTwriter.

- 1 Log in to the SAINT user interface.
- 2 From the navigation menu, select **Data > SAINTwriter**.
- 3 Click **Report Type**.
- 4 From the **Type** list, select **Custom**.
- 5 In the **File Name** field, type a configuration file name.  
The configuration file name that is created must be used when you add the SAINT scanner to Extreme Security.
- 6 From the **Template Type** list, select **Technical Details**.
- 7 Click **Continue**.
- 8 Select **Lists**.
- 9 From the **Columns to include in host** list, change a None column to **MAC address**.
- 10 From the **Columns to include in vulnerability** list, change a None column to **Port**.
- 11 From the **Columns to include in vulnerability** list, change a None column to **Service**.
- 12 Click **Save**.

You are now ready to add a scan configuration to Extreme Security for the SAINT scanner. See [Adding a SAINT vulnerability scan](#) on page 77.

## Adding a SAINT vulnerability scan

Administrators can add a SAINT scanner configuration to collect specific reports or start scans on the remote scanner.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify your SAINT scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **SAINT Scanner**.
- 7 In the **Remote Hostname** field, type the IP address or host name of the SAINT scanner.
- 8 Choose one of the following authentication options:

Option	Description
<b>Login Username</b>	<p>To authenticate with a user name and password:</p> <ol style="list-style-type: none"> <li>1 In the <b>Login Username</b> field, type a username that has access to access the remote host.</li> <li>2 In the <b>Login Password</b> field, type the password associated with the user name.</li> </ol>
<b>Enable Key Authorization</b>	<p>To authenticate with a key-based authentication file:</p> <ol style="list-style-type: none"> <li>1 Select the <b>Enable Key Authentication</b> check box.</li> <li>2 In the <b>Private Key File</b> field, type the directory path to the key file.</li> </ol> <p>The default is directory for the key file is <code>/opt/gradar/conf/vis.ssh.key</code>.</p> <p>If a key file does not exist, you must create the vis.ssh.key file.</p>

- 9 In the **SAINT Base Directory** field, type the path to the installation directory of the SAINT scanner.
- 10 From the **Scan Type** list, select one of the following options:
  - Live Scan - Starts a vulnerability scan to generate report data based on the session name.
  - Report Only - Generates a scan report based on the session name.
- 11 For **Live Scan** configurations, select an option for the **Ignore Existing Data** check box.
  - Select this check box to force the live scan to gather new vulnerability data from the network. This option removes any data from the session folder before the live scan starts.
  - Clear this check box to enable the live scan to use existing data in the session folder.
- 12 From **Scan Level** list, select a scan level. The options include:
  - Vulnerability Scan - Scan for all vulnerabilities.
  - Port Scan - Scan for TCP or UDP services listening on the network.
  - PCI Compliance Scan - Scan ports and services with emphasis on DSS PCI compliance.
  - SANS Top 20 Scan - Scan for the top 20 most critical security vulnerabilities.
  - FISMA Scan - Scan for all vulnerabilities and including all custom scans and PCI levels.

- 13 In the **Session Name** field, type the session name for the SAINT scanner configuration.
- 14 In the **SAINT Writer Config** field, type the name of the SAINTwriter configuration file.
- 15 To configure a CIDR range for the scanner:
  - a In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 16 Click **Save**.
- 17 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.

# 25 Tenable SecurityCenter scanner overview

## Adding a Tenable SecurityCenter scan

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

To configure a Tenable SecurityCenter scanner, see [Adding a Tenable SecurityCenter scan](#) on page 79.

## Adding a Tenable SecurityCenter scan

You can add a Tenable SecurityCenter scanner to enable Extreme Security to collect host and vulnerability information through the Tenable API.

Verify the location of the `request.php` file on their Tenable SecurityCenter before a scanner is added to Extreme Security.

Before you add this scanner, a server certificate is required to support HTTPS connections. Extreme Security supports certificates with the following file extensions: `.crt`, `.cert`, or `.der`. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

- 1 Click the **Admin** tab.
- 2 Click the **VA Scanners** icon.
- 3 Click **Add**.
- 4 In the **Scanner Name** field, type a name to identify the scanner.
- 5 From the **Managed Host** list, select the managed host from your Extreme Security deployment that manages the scanner import.
- 6 From the **Type** list, select **Tenable SecurityCenter**.
- 7 In the **Server Address** field, type the IP address of the Tenable SecurityCenter.
- 8 In the **API Location** field, type the path to the `request.php` file on the Tenable SecurityCenter. The default path to the API file is `sc4/request.php`.
- 9 In the **User Name** field, type the user name to access the Tenable SecurityCenter API.

- 10 In the **Password** field, type the password to access the Tenable SecurityCenter API.
- 11 To configure a CIDR range for the scanner:
  - a In the text field, type the CIDR range for the scan or click **Browse** to select a CIDR range from the network list.
  - b Click **Add**.
- 12 Click **Save**.
- 13 On the **Admin** tab, click **Deploy Changes**.

You are now ready to create a scan schedule. See [Scheduling a vulnerability scan](#) on page 81.



# 26 Scheduling a vulnerability scan

Scan schedules are intervals assigned to scanners that determine when vulnerability assessment data is imported from external scanning appliances in your network. Scan schedules can also define CIDR ranges or subnets that are included in the data import when the vulnerability data import occurs.

Scan schedules are created for each scanner product in your network and are used to retrieve vulnerability data. There is no limit to the number of scan schedules you can create. It is often helpful to create multiple scans in your network for vulnerabilities in your network. Large vulnerability imports can take a long time to complete and are often very system resource intensive. A scan cannot be scheduled until after the scanner has been added.

- 1 Click the **Admin** tab.
- 2 Click the **Schedule VA Scanners** icon.
- 3 Click **Add**.
- 4 From the **VA Scanners** list, select the scanner that requires a scan schedule.
- 5 Choose one of the following options:

Option	Description
<b>Network CIDR</b>	Select this option to define a CIDR range for the data import.  If a scanner includes multiple CIDR configurations, then the CIDR range can be selected from the list.
<b>Subnet/CIDR</b>	Select this option to define a subnet or CIDR range for the data import.  The subnet/CIDR value that is defined by the administrator must be a Network CIDR that is available to the scanner.

- 6 From the **Priority** list, select the priority level to assign to the scan.

Option	Description
<b>Low</b>	Indicates the scan is of normal priority. Low priority is the default scan value.
<b>High</b>	Indicates the scan is high priority.  High priority scans are always placed above low priority scans in the scan queue.

- 7 In the **Ports** field, type the ports that are included in the scan schedule. Any ports that are not in the schedule are not imported from the vulnerability data. Administrators can specify any port values from 1 - 65536. Individual port values can be included as comma-separated values, along with port ranges. For example, 21,443, 445, 1024-2048.
- 8 Select the start time for the schedule.
- 9 In the **Interval** field, type a time interval to indicate how often you want this scan to repeat. Scans schedules can contain intervals by the hour, day, week, or month.
- 10 Click **Save**.

# 27 viewing the status of a vulnerability scan

The Scan Schedule window provides administrators a status view for when each scanner is scheduled to collect vulnerability assessment data for asset in the network.

The name of each scan is displayed, along with the CIDR range, port or port range, priority, status, and next run time.

**Table 10: Scan schedule status**

Column name	Description
VA Scanner	Displays the name of the schedule scan.
CIDR	Displays the CIDR address ranges that are included in the vulnerability data import when the scan schedule starts.
Ports	Displays the port ranges that are included in the vulnerability data import when the scan schedule starts. Scan schedules are capable of starting a remote scan on a remote vulnerability appliance for specific vendors. For example, NMap or Nessus, or Nessus Scan Results Importer, then the ports listed in the Ports column are the ports contained in the scan. For most 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. Scans schedules with a high priority are queued above in priority and run before low priority scans.
Status	Displays the current status of the scan. Each status field contains unique information about the scan status. <ul style="list-style-type: none"><li>• New scans can be edited until the state changes.</li><li>• Pending scans must wait for another scan to complete.</li><li>• In progress scans provide a percentage complete with tooltip information about the data import.</li><li>• Completed scans provide a summary of the vulnerabilities imported or any partial imports of data that occurred.</li><li>• Failed scans provide an error message on why the vulnerabilities failed to import.</li></ul>
Last Finish Time	Displays the last time the scan successfully imported vulnerability records for the schedule.
Next Run Time	Displays the next time the scan is scheduled to import vulnerability data. Scan schedules that display <i>Never</i> in the user interface are one time scans.

- 1 Click the **Admin** tab.
- 2 Click the **Schedule VA Scanners** icon.

- 3 Review the Status column to determine the status of your log sources.

The status column for each scanner provides a status message about each successful vulnerability import or failure.

# 28 Supported vulnerability scanners

Vulnerability data can be collected from several manufacturers and vendors of security products. If the scanner deployed in your network is not listed in this document, you can contact your sales representative to review support for your appliance.

**Table 11: Supported vulnerability scanners**

Vendor	Scanner name	Supported versions	Configuration name	Connection type
Beyond Security	Automated Vulnerability Detection System (AVDS)	AVDS Management V12 (minor version 129) and above	Beyond Security AVDS Scanner	File import of vulnerability data with SFTP
eEye Digital Security	eEye REM	REM V3.5.6	eEye REM Scanner	SNMP trap listener
	eEye Retina CS	Retina CS V3.0 - V4.0		Database queries over JDBC
Generic	Axis	N/A	Axis Scanner	File import of vulnerability data with SFTP
IBM®	InfoSphere® Guardium®	v9.0 and above	IBM Guardium SCAP Scanner	File import of vulnerability data with SFTP
IBM®	IBM Security AppScan® Enterprise	V8.6	IBM AppScan Scanner	IBM REST web service with HTTP or HTTPS
IBM®	InfoSphere® SiteProtector™	V2.9.x	IBM SiteProtector Scanner	Database queries over JDBC
IBM®	Tivoli Endpoint Manager®	V8.2.x	IBM Tivoli Endpoint Manager	SOAP-based API with HTTP or HTTPS
Juniper Networks	NetScreen Security Manager (NSM) Profiler	2007.1r2	Juniper NSM Profiler Scanner	Database queries over JDBC
		2007.2r2		
		2008.1r2		
		2009r1.1		
		2010.x		
McAfee	Foundstone	V5.0 - V6.5	Foundscan Scanner	SOAP-based API with HTTPS
McAfee	Vulnerability Manager	V6.8	McAfee Vulnerability Manager	SOAP-based API with HTTPS
		V7.0		XML file import
		V7.5		
nCircle	ip360	VnE Manager V6.5.2 - V6.8.28	nCircle ip360 Scanner	File import of vulnerability data with SFTP

**Table 11: Supported vulnerability scanners (continued)**

Vendor	Scanner name	Supported versions	Configuration name	Connection type
Nessus	Nessus	Linux™ V4.0.2 - V4.4.x Microsoft™ Windows™ V4.2 - V4.4.x	Nessus Scanner	File import over SFTP with SSH command execution
Nessus	Nessus	Linux™ V4.2 - V5.x Microsoft™ Windows™ V4.2 - V5.x	Nessus Scanner	Nessus XMLRPC API over HTTPS
netVigilance	SecureScout	V2.6	SecureScout Scanner	Database queries over JDBC
Open source	NMap	V3.7 - V6.0	NMap Scanner	File import of vulnerability data over SFTP with SSH command execution
Qualys	QualysGuard	V4.7 -V7.10	Qualys Scanner	APIv2 over HTTPS
Qualys	QualysGuard	V4.7 -V7.10	Qualys Detection Scanner	API Host Detection List over HTTPS
Rapid7	NeXpose	V4.x - V5.5	Rapid7 NeXpose Scanner	Remote Procedure Call (RPC) over HTTPS Local file import of XML file over SCP or SFTP to a local directory
Saint Corporation	SAINT	V7.4.x	Saint Scanner	File import of vulnerability data over SFTP with SSH command execution
Tenable	SecurityCenter	V4.6.0	Tenable SecurityCenter	JSON request over HTTPS

# Index

---

## A

- adding 15
- adding a MaxPatrol scanner 64
- audience 5
- Axis
  - add 11
- AXISscanner 11

## C

- connection type 84
- conventions, guide
  - notice icons 5
  - text 6

## D

- Digital Defense AVS scanner 15

## E

- eEye CS Retina
  - add JDBC scans 18
  - add SNMP scans 17
  - overview 17
- eEye REM
  - add JDBC scans 18
  - add SNMP scans 17
  - overview 17

## F

- Foundstone Foundscan 20
- Foundstone FoundScan
  - add 20
  - importing certificates 21

## I

- IBM AppScan Enterprise
  - adding 25
  - create user type 23
  - publish reports 25
- IBM InfoSphere Guardium
  - adding 27
- IBM InfoSphere SiteProtector
  - adding 30
- IBM Security SiteProtector 30
- integrating
  - Positive Technologies MaxPatrol 63
- introduction 5

## J

- Java Cryptography Extension 9
- Juniper NSM Profiler 34

## L

- log sources 13

## M

- MaxPatrol 63
- McAfee Vulnerability Manager
  - create certificate 38
  - import certificates 40
  - process certificates 39
- Microsoft SCCM
  - adding 43

## N

- nCircle IP360
  - adding 32, 45
  - exporting data 44
- Nessus
  - adding a live scan 47
  - adding a live scan ( JSON API) 52
  - adding a live scan ( XMLRPC API) 50
  - adding a schedule result import 49, 57
  - completed report import XMLRPC API 51
- netVigilance SecureScout 55
- Nmap
  - adding a remote live scan 58

## O

- overview 11, 13, 20, 23, 27, 30, 32, 34, 36, 41, 44, 46, 47, 55, 57, 66, 73, 76, 79

## P

- Positive Technologies MaxPatrol
  - adding 64

## Q

- Qualys Detection 66

## R

- Rapid7 NeXpose scanner 73

## S

- SAINT
  - add 77
  - configure SAINTwriter 76
- SAINT scanner 76
- scan schedule
  - status 82
  - view 82
- scan schedules 81

## scanner

- Beyond Security AVDS 13
  - Juniper NSM Profiler 34
  - McAfee Vulnerability Manager 36, 37
  - Qualys Detection 66, 69
  - Qualys scheduled import asset report 70
  - Qualys scheduled import scan report 71
  - Rapid7 NeXpose 73, 74
  - Security AppScan 24
  - Tenable SecurityCenter 79
- SecureScout scanner
- adding 55
- Security AppScan Enterprise 23
- Security Tivoli Endpoint Manager 32
- Supported vulnerability scanners 84

**T**

- Tenable SecurityCenter scanner 79

**V**

- vulnerability assessment overview 9