Extreme Networks Security Vulnerability Manager User Guide

9034870

Published September 2015

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/

Support

For product support, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

Introduction to Extreme Networks Security Vulnerability Manager

This information is intended for use with Extreme Networks Security Vulnerability Manager. Vulnerability Manager is a scanning platform that is used to identify, manage, and prioritize the vulnerabilities on your network assets.

This guide contains instructions for configuring and using Vulnerability Manager on an Extreme SIEM or Extreme Networks Security Log Manager console.

Intended audience

System administrators responsible for configuring Extreme Networks Security Vulnerability Manager must have administrative access to Extreme SIEM and to your network devices and firewalls. The system administrator must have knowledge of your 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...
👉	General Notice	Helpful tips, tricks, notices 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	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 **enter** and **type**	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 italicized type	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.

Getting Help

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

Web	www.extremenetworks.com/support
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: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com 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

- *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 Downloads*
- *Extreme Security Threat Protection*

1 What's new for users in Extreme Security Vulnerability Manager V7.7.2.5

Extreme Networks Security Vulnerability Manager V7.7.2.5 introduces support for overlapping IP addresses in networks that have multiple domains. It also includes enhancements to vulnerability data retention and removal, a new RSS feed dashboard item, and more.

Overlapping IP and domain support

Use Extreme Security Vulnerability Manager domain-aware features to ensure that assets that have the same IP address in different networks are not confused when scanning.

Set vulnerability and scan result retention periods

Set the retention period for vulnerability trend data and scan results so unneeded data is removed regularly from your system.

Remove unwanted vulnerability data

Use Extreme Security Vulnerability Manager vulnerability cleansing features to remove stale vulnerability data from the asset model.

RSS feeds

Use the RSS Feeds dashboard item to see the latest security news, advisories, and information about scan progress and completion.

Extend Extreme Security Vulnerability Manager temporary license period

When the temporary Vulnerability Manager license expires, use the Vulnerability Manager icon on the Admin tab to extend it for a further four weeks.

2 Vulnerability Manager installations and deployments

You access Extreme Networks Security Vulnerability Manager by using the **Vulnerabilities** tab.

Access to the vulnerabilities tab

Depending on the product that you install and whether you upgrade Extreme Security or install a new system, the **Vulnerabilities** tab might not be displayed.

- If you install Extreme SIEM, the **Vulnerabilities** tab is enabled by default with a temporary license key.
- If you install Log Manager, the **Vulnerabilities** tab is not enabled.
- Depending on how you upgrade Extreme Security, the **Vulnerabilities** tab might not be enabled.

To use Vulnerability Manager after an install or upgrade you must upload and allocate a valid license key. For more information, see the *Administration Guide* for your product.

For more information about upgrading, see the *Extreme Networks Security Upgrade Guide*.

Vulnerability processing and scanning deployments

When you install and license Vulnerability Manager, a vulnerability processor is automatically deployed on your Extreme Security console. A processor is not automatically deployed if you use a software activation key on your Extreme Security console.

The vulnerability processor provides a scanning component by default. If required, you can deploy more scanners, either on dedicated Vulnerability Manager managed host scanner appliances or Extreme Security managed hosts. For example, you can deploy a vulnerability scanner on an Event Collector or QFlow Collector. You cannot deploy a vulnerability scanner on a high availability managed host.

If required, you can move the vulnerability processor to a different managed host in your deployment. You might move the processor to preserve disk space on your Extreme Security console.

Note
You can have only one vulnerability processor in your deployment. You can move the vulnerability processor only to a dedicated Vulnerability Manager processor appliance.

Important
After you change your vulnerability processor deployment, you must wait for your deployment to fully configure. In the Scan Profiles page, the following message is displayed: QVM is in the process of being deployed.

Ensure that following applications are installed on all desktop systems that you use to access the Extreme Security product user interface:

- Java™ Runtime Environment (JRE) version 1.7 or 64-bit Runtime Environment for Java™ V7.0
- Adobe™ Flash version 10.x

Related Links

Options for adding scanners to your Vulnerability Manager deployment on page 14

Options for moving the vulnerability processor in your Vulnerability Manager deployment on page 12

Vulnerability processor and scanner appliance activation keys

You can scan and process your vulnerabilities by using dedicated Vulnerability Manager managed host appliances.

When you install a processor or scanner managed host appliance, you must type a valid activation key.

For more information about installing a managed host appliance, see the *Installation Guide* for your product.

The activation key is a 24-digit, four part, alphanumeric string that you receive from Extreme Networks®. The activation key specifies which software modules apply for each appliance type:

- The Vulnerability Manager processor appliance includes vulnerability processing and scanning components.
- The Vulnerability Manager scanner appliance includes only a vulnerability scanning component.

You can obtain the activation key from the following locations:

- If you purchased a Vulnerability Manager software or virtual appliance download, a list of activation keys are included in the *Getting Started* document that is attached in a confirmation email. You can use this document to cross-reference the part number for the appliance that you are supplied with.
- If you purchased an appliance that is preinstalled with Vulnerability Manager software, the activation key is included in your shipping box or CD.

Vulnerability backup and recovery

You can back up and recover your vulnerability data including vulnerability configurations. For example, you can back up scan profiles.

Vulnerability Manager back up and recovery is managed by using the **Admin** tab.

For more information about vulnerability backup and recovery, see the *Administration Guide* for your product.

Options for moving the vulnerability processor in your Vulnerability Manager deployment

If required, you can move the vulnerability processor from your Extreme Security console to a dedicated Vulnerability Manager managed host appliance.

For example, you might move your vulnerability processing capability to a managed host to minimize disk space impact on your Extreme Security console.

> Note
>
> You can have only one vulnerability processor in your deployment. Also, you must deploy the vulnerability processor only on a Extreme Security console or Vulnerability Manager managed host processor appliance.

To move the vulnerability processor, choose one of the following options:

Option 1: Deploy a dedicated Vulnerability Manager processor appliance

To deploy a processor appliance you must complete the followings tasks:

1 Install a dedicated Vulnerability Manager processor appliance.

2 Add the managed host processor appliance to your Extreme Security Console by using the **System and License Management** tool on the **Admin** tab.

When you select the managed host option, the processor is automatically removed from the Extreme Security console.

Option 2: Move the vulnerability processor from your console to your managed host

If the vulnerability processor is on your Extreme Security console, then later you can move your vulnerability processor to a previously installed Vulnerability Manager managed host processor appliance.

At any time, you can move the vulnerability processor back to your Extreme Security console.

Deploying a dedicated Vulnerability Manager processor appliance

You can deploy a dedicated Vulnerability Manager processor appliance as a managed host.

When you deploy your vulnerability processor to a managed host, all vulnerabilities are processed on the managed host.

Note
After you deploy processing to a dedicated Vulnerability Manager managed host, any scan profiles or scan results that are associated with a Extreme Security console processor are not displayed. You can continue to search and view vulnerability data on the Manage Vulnerabilities pages.

Ensure that a dedicated Vulnerability Manager managed host is installed and a valid processor appliance activation key is applied. For more information, see the *Installation Guide* for your product.

1 Log in to Extreme Security Console as an administrator:

   `https://`*`IP_Address_QRadar`*

   The default user name is **`admin`**. The password is the password of the root user account that was entered during the installation.
2 Click the Admin tab.
3 In the System Configuration pane, click System and License Management.
4 From the host table, click the Extreme Security Console host, and click > Deployment Actions > Add Host.
5 Enter the Host IP address and password.
6 Click Add.
7 Close the System and License Management window.
8 On the Admin tab toolbar, click Advanced > Deploy Full Configuration.
9 Click OK.

Related Links

Verifying that a vulnerability processor is deployed on page 14

Vulnerability processor and scanner appliance activation keys on page 11

Moving your vulnerability processor to a managed host or console

If required, you can move your vulnerability processor between a Vulnerability Manager managed host appliance and your Extreme Security console.

Ensure that a dedicated Vulnerability Manager managed host is installed and a valid processor appliance activation key is applied.

1 On the Admin tab, click System and License Management > Deployment Actions > Manage Vulnerability Deployment.
2 Click Enable Processor.
3 Select the a managed host or console from the Processor list.
   If your processor is on the managed host, you can select only the Extreme Security console.
4 Click Save.
5 On the Admin tab toolbar, select Advanced > Deploy Full Configuration.
6 Click OK.

Related Links

Vulnerability processor and scanner appliance activation keys on page 11

Verifying that a vulnerability processor is deployed

In Extreme Networks Security Vulnerability Manager, you can verify that your vulnerability processor is deployed on a Extreme Security console or Vulnerability Manager managed host.

1. Log in to the Extreme Security console.
2. On the Admin tab, click System and License Management > Deployment Actions > Manage Vulnerability Deployment.
3. Verify that the processor is displayed on Processor list.

Removing a vulnerability processor from your console or managed host

If required, you can remove the vulnerability processor from a Extreme Security console or Vulnerability Manager managed host.

1. Log in to the Extreme Security console.
2. On the Admin tab, click System and License Management > Deployment Actions > Vulnerability Deployment Management.
3. Click the Enable Processor check box to deselect it.
4. Click Remove.
5. Click Save.
6. Close the System and License Management window.
7. On the Admin tab toolbar, select Advanced > Deploy Full Configuration.
8. Click OK.

Options for adding scanners to your Vulnerability Manager deployment

If you have a large network and require flexible scanning options, you can add more scanners to your Extreme Networks Security Vulnerability Manager deployment.

Your Vulnerability Manager processor is automatically deployed with a scanning component. By deploying more scanners you can increase the flexibility of your scanning operations. For example, you can scan specific areas of your network with different scanners and at different scheduled times.

Dynamic vulnerability scans

The vulnerability scanners that you deploy might not have access to all areas of your network. In Vulnerability Manager you can assign different scanners to network CIDR ranges. During a scan, each asset in the CIDR range that you want to scan is dynamically associated with the correct scanner.

To add more vulnerability scanners, choose any of the following options:

Deploy a dedicated Vulnerability Manager	You can scan for vulnerabilities by using a dedicated Vulnerability Manager managed host scanner appliance.

managed host scanner appliance	To deploy a scanner appliance, you must complete the followings tasks: 1 Install a dedicated Vulnerability Manager managed host scanner appliance. 2 Add the managed host scanner appliance to your Extreme Security Console by using the System and License Management tool on the Admin tab.
Deploy a Vulnerability Manager scanner to your Extreme Security console or managed host	If you move your vulnerability processor from your Extreme Security console to a Vulnerability Manager managed host, you can add a scanner to your console. You can also add a vulnerability scanner to any preexisting Extreme Security managed hosts in your deployment. For example, you can add a scanner to an event collector, flow collector, or event processor. Note You cannot add a vulnerability scanner to a high availability managed host.
Configure access to an Extreme Networks® hosted scanner and scan your DMZ	You can configure access to an Extreme Networks® hosted scanner and scan the assets in your DMZ.

Related Links

Associating vulnerability scanners with CIDR ranges on page 53
In Extreme Networks Security Vulnerability Manager, to do dynamic scanning, you must associate vulnerability scanners with different segments of your network.

Scanning CIDR ranges with different vulnerability scanners on page 53
In Extreme Networks Security Vulnerability Manager, you can scan areas of your network with different vulnerability scanners.

Dynamic vulnerability scans on page 52
In Extreme Networks Security Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Deploying a dedicated Vulnerability Manager scanner appliance

You can deploy a dedicated Vulnerability Manager managed host scanner appliance.

Ensure that a dedicated Vulnerability Manager managed host scanner appliance is installed and a valid appliance activation key is applied.

1 On the Admin tab, click System and License Management > Deployment Actions > Add Managed Host.
2 Enter the Host IP address and password of the Vulnerability Manager managed host scanner appliance.
3 Click Add.

   You must wait several minutes while the managed host is added.
4 Close the System and License Management window.
5 On the Admin tab toolbar, select Advanced > Deploy Full Configuration.
6 Click OK.

Related Links

Vulnerability processor and scanner appliance activation keys on page 11

Deploying a vulnerability scanner to a Extreme Security console or managed host

You can deploy a Vulnerability Manager scanner to a Extreme Security console or Extreme Security managed host. For example, you can deploy a scanner to a flow collector, flow processor, event collector, or event processor.

To deploy a scanner on your Extreme Security console, ensure that the vulnerability processor is moved to a dedicated Vulnerability Manager managed host appliance.

To deploy scanners on Extreme Security managed hosts, ensure that you have existing managed hosts in your deployment. For more information, see the *Installation Guide* for your product.

1 On the Admin tab, click System and License Management > Deployment Actions > Manage Vulnerability Deployment.

2 Click Add Additional Vulnerability Scanners.

3 Click the + icon.

4 From the Host list, select the Extreme Security managed host or console.

Note
You cannot add a scanner to a Extreme Security console when the vulnerability processor is on the console. You must move the vulnerability processor to a Vulnerability Manager managed host.

5 Click Save.

6 Close the System and License Management window.

7 On the Admin tab toolbar, select Advanced > Deploy Full Configuration..

8 Click OK.

9 Check the Scan Server list on the Scan Profiles Configuration page to ensure that the scanner has been added.

For more information, see Creating a scan profile on page 29.

Run an automatic update after you add the scanner or other managed host with scanning capabilities. Alternatively, you can scan after the default daily scheduled automatic update runs.

Related Links

Moving your vulnerability processor to a managed host or console on page 13

Scanning the assets in your DMZ

In Extreme Networks Security Vulnerability Manager, you can connect to an external scanner and scan the assets in your DMZ for vulnerabilities.

If you want to scan the assets in the DMZ for vulnerabilities, you do not need to deploy a scanner in your DMZ. You must configure Vulnerability Manager with a hosted Extreme Networks® scanner that is located outside your network.

Detected vulnerabilities are processed by the processor on either your Extreme Security console or Vulnerability Manager managed host.

1. Configure your network and assets for external scans.
2. Configure Vulnerability Manager to scan your external assets.

Configuring Vulnerability Manager to scan your external assets

To scan the assets in your DMZ, you must configure Vulnerability Manager, by using the System and License Management tool on the Admin tab.

1. On the Admin tab, click System and License Management > Deployment Actions > Manage Vulnerability Deployment.
2. Click Use External Scanner.
3. In the Gateway IP field, enter an external IP address.

   Note
   You cannot scan external assets until your external IP address is configured. Ensure that you email details of your external IP address to Extreme Networks®.

4. If your network is configured to use a proxy server, click Enable Proxy Server and enter the details of your server.
5. Click Save and then click Close.
6. On the Admin tab toolbar, click Advanced > Deploy Full Configuration.
7. Click OK.

Extending the Vulnerability Manager temporary license period

By default, when you install Extreme SIEM, you can see the Vulnerabilities tab because a temporary license key is also installed. When the temporary license expires, you can extend it for an extra four weeks.

1. On the Admin tab, click the Vulnerability Manager icon in the Try it out area.
2. To accept the end-user license agreement, click OK.

   When the extended license period is finished, you must wait six months before you can activate the temporary license again. To have permanent access to Extreme Security Vulnerability Manager, you must purchase a license.

3 Extreme Networks Security Vulnerability Manager

Extreme Networks Security Vulnerability Manager is a network scanning platform that detects vulnerabilities within the applications, systems, and devices on your network or within your DMZ.

Vulnerability Manager uses security intelligence to help you manage and prioritize your network vulnerabilities. For example, you can use Vulnerability Manager to continuously monitor vulnerabilities, improve resource configuration, and identify software patches. You can also, prioritize security gaps by correlating vulnerability data with network flows, log data, firewall, and intrusion prevention system (IPS) data.

You can maintain real-time visibility of the vulnerabilities that are detected by the built-in Vulnerability Manager scanner and other third-party scanners. Third-party scanners are integrated with Extreme Security and include IBM® Security Endpoint Manager, Guardium®, AppScan®, Nessus, nCircle, and Rapid 7.

Unless otherwise noted, all references to Vulnerability Manager refer to Extreme Networks Security Vulnerability Manager. All references to Extreme Security refer to Extreme SIEM and Extreme Networks Security Log Manager and all references to SiteProtector™ refer to Security SiteProtector.

Vulnerability scanning

In Extreme Networks Security Vulnerability Manager, vulnerability scanning is controlled by configuring scan profiles. Each scan profile specifies the assets that you want to scan and the scan schedule.

Vulnerability processor

When you license Vulnerability Manager, a vulnerability processor is automatically deployed on your Extreme Security console. The processor contains a Vulnerability Manager scanning component.

Deployment options

Vulnerability scanning can be deployed in different ways. For example, you can deploy your scanning capability to a Vulnerability Manager managed host scanner appliance or a Extreme Security managed host.

Configuration options

Administrators can configure scans in the following ways:

- Schedule scans to run at times convenient for your network assets.
- Specify the times during which scans are not allowed to run.
- Specify the assets that you want to exclude from scans, either globally or for each scan.
- Configure authenticated patch scans for Linux™, UNIX™, or Windows™ operating systems.
- Configure different scanning protocols or specify the port ranges that you want to scan.

Related Links

Options for adding scanners to your Vulnerability Manager deployment on page 14

Options for moving the vulnerability processor in your Vulnerability Manager deployment on page 12

Getting started with vulnerability scanning

Initial configuration of Extreme Networks Security Vulnerability Manager system for network and vulnerability management requires systematic planning.

There are three key areas to consider when you use Extreme Security Vulnerability Manager for vulnerability scanning :

- The type of scan to run and how often to run it.
- The number of scanners to deploy and the number of assets to scan at any one time.
- How to manage the vulnerabilities that are discovered.

Scan types

Extreme Networks Security Vulnerability Manager provides several default scan policy types. You can also define your own scans from templates.

The following are the most commonly used templates:

Discovery scan Discovers network assets. Then scans ports to identify key asset characteristics such as operating system, device type, and services that are provided by the asset. Vulnerabilities are not scanned.

Full scan Discovers network assets that use a fast scan port range. Performs a user-configurable port scan and unauthenticated scan of discovered services like FTP, web, SSH, and database. If credentials are provided, an authenticated scan is performed.

Patch scan Scouts the network to discover assets and then performs a fast port scan and credential scan of the assets.

Discovery scans

A discovery scan is a lightweight uncredentialed scan. It searches an address space for active IP addresses, and then scans their ports. It performs DNS and NetBIOS look-ups to discover what operating system the assets run, what open services they provide, and any network names that are assigned to them.

Generally, you run discovery scans frequently. They are often run weekly to ensure good visibility of network assets and asset information, such as asset names, operating system and open services, to SIEM and SOC users.

Full scans

A full scan runs the full suite of Extreme Security Vulnerability Manager tests.

A full scan has these phases:

1. A discovery scan
2. Uncredentialed checks. Checks services that do not require credentials, for example, reading banners and responses for version information, SSL certificate expiry, testing default accounts, testing responses for vulnerabilities.
3. Credentialed checks. Extreme Security Vulnerability Manager logs on to the asset and gathers installed application inventory and required configuration, and raises (or suppresses) vulnerabilities as appropriate. Credential scans are preferable to uncredentialed scans. Uncredentialed scans provide a useful overview of the vulnerability posture of the network. Credentialed scanning, however, is essential to a comprehensive and effective vulnerability management program.

Note
Full scans can sometimes lock some administration accounts, for example, SQL Server, when Extreme Security Vulnerability Manager tests multiple default credentials on those accounts.

Patch scans

You use patch scans to determine which patches and products are installed or missing on the network.

A patch scan has two main phases:

- A discovery scan
- Uncredentialed checks

Patch scans run more quickly and have a lesser impact on the network and assets being scanned because they do not perform uncredentialed checks.

When to scan

The following is a typical timetable for each type of scan:

- Discovery scan – Run weekly
- Patch Scan – Run every 1–4 weeks
- Full scan – Run every 2-3 months

Related Links

Creating a scan profile on page 29
Scan scheduling on page 34
Vulnerability scanning on page 29
Scan policies on page 54

Remote scanner deployments

You can deploy an unlimited number of remote scanners in a network.

When you design a remote scanner deployment, you must consider the following factors:

- The number of assets that you need to scan.
- Network connectivity between the Extreme Networks Security Vulnerability Manager and the assets it scans.
- The network bandwidth that is required.
- Whether to use dynamic scanning.
- How many Networks Interface Cards (NICs) to use on a scanner.

Scanners and assets

There is no limited to the number of assets that a scanner can scan, in principle. Each scanner has a bandwidth and scan requests are queued when that bandwidth is full.

The more assets that you ask a scanner to scan the longer the scan takes. For example, deploying scanners to scan up to 4000-5000 assets results in acceptable scan times (2-3 days maximum).

Scanner and asset connectivity

In general, avoid scanning through firewalls, and over low-bandwidth WAN connections.

The following guidelines are useful:

- Keep the load on your firewalls low.
- Reduce the risk of firewall interference with the scan. For example, do not permit the firewall to block ports that are required to complete the scan.
- Ensure your scans run as quickly as possible.
- Ensure that poor WAN connectivity does not negatively affect your scans.

Bandwidth limit settings

You can configure network bandwidth per scan profile in Extreme Networks Security Vulnerability Manager.

When you increase the network bandwidth per scan profile, Extreme Security Vulnerability Manager scans more vulnerability tools in parallel and therefore scans run more quickly. You can set the bandwidth limit on the Scan Profile Configuration page. The following options are available:

Option	Bandwidth limit setting
Low	100 Kbps
Medium	1000 Kbps (default)
High	5000 Kbps
Full	network maximum

If you are scanning over limited network bandwidth links, do not increase network bandwidth to more than 1000 Kbps. As a rule, when patch scanning with a setting of Medium, Extreme Security Vulnerability Manager patch scan 10 assets in parallel. With a setting of High, it scans 50 assets in parallel.

Related Links

Creating a scan profile on page 29

Scan profile details on page 33

Dynamic scanning

In dynamic scanning, Extreme Networks Security Vulnerability Manager selects a scanner based on the IP address to scan.

Dynamic scanning reduces the number of scan jobs that you need to configure. For example, if you deploy 10 Extreme Security Vulnerability Manager scanners and do not use dynamic scanning, you must configure 10 individual scan jobs. You must select one scanner per scan job. If you use dynamic scanning, you can configure a single scan job to use all 10 scanners by associating CIDR ranges with each scanner. Extreme Security Vulnerability Manager selects the appropriate scanner for each IP address that is being scanned.

Dynamic scanning is most useful when you deploy many scanners. If you have, for example, more than 5 scanners, dynamic scanning might save you time. As a rule, do not enable dynamic scanning when you do your initial set of test scans. You can switch to dynamic scanning when you are satisfied with scan times and results.

Related Links

Dynamic vulnerability scans on page 52

In Extreme Networks Security Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Creating a scan profile on page 29

Network Interface Cards on scanners

In Extreme Networks Security Vulnerability Manager scanning is not dependent on the Network Interface Cards (NICs) that are configured on the scanner appliance.

You can configure many NICs, although 4-5 NICs is a typical configuration. Extreme Security Vulnerability Manager uses standard TCP/IP protocols to scan any device that has an IP address. If multiple NICs are defined, scanning follows the standard networking configuration on an appliance.

Vulnerability management overview

Extreme Networks Security Vulnerability Manager provides a process for managing vulnerabilities that are based on assignment of asset owners.

You can configure Asset owners on the **Vulnerability Assignment** page of the **Vulnerabilities** tab or by using an API. After assets are assigned, any vulnerabilities discovered on the assets are assigned to those users or groups with a due date based on the risk level of the vulnerabilities in question. You also configure due dates and risk level on the **Vulnerability Assignment** page. You can then configure remediation reports to send to those users on a periodic basis. Use remediation reports to highlight the following actions:

- The patches that you need to install.
- The steps that you need to take to remediate the vulnerability.
- The assets that have overdue vulnerabilities.
- New vulnerabilities that were discovered since the last scan.

The standard remediation reports are available on the Email tab of the Scan Profile Configuration page. You can create extra customer reports by using Extreme Security Vulnerability Manager searches. Use a wide range of search criteria to ensure that your reports focus on the vulnerability remediation activities that you require to meet your specific business and compliance needs.

To make remediation report creation easier, Extreme Security Vulnerability Manager can automatically create Asset vulnerabilities and Vulnerability reports for each asset owner from a single report definition.

When assets are rescanned, any remediated vulnerabilities are automatically detected and flagged as fixed. They are removed from reports and views, unless explicitly configured otherwise. Any vulnerabilities that were previously fixed and are detected again are automatically reopened.

Related Links

Assigning a technical user as the owner of asset groups on page 77

Configuring remediation times for the vulnerabilities on assigned assets on page 79

Emailing asset owners when vulnerability scans start and stop on page 60

Email the configured asset technical owners to alert them of the scan schedule. You can also email reports to asset owners.

Vulnerability reports on page 80

Searching vulnerability data on page 63

Vulnerability management dashboard

You can display vulnerability information on your Extreme Security dashboard.

Extreme Networks Security Vulnerability Manager is distributed with a default vulnerability dashboard so that you can quickly review the risk to your organization.

You can create a new dashboard, manage your existing dashboards, and modify the display settings of each vulnerability dashboard item.

For more information about dashboards, see the *Users Guide* for your product.

Reviewing vulnerability data on the default vulnerability management dashboard

You can display default vulnerability management information on the Extreme Security dashboard.

The default vulnerability management dashboard contains risk, vulnerability, and scanning information.

You can configure your own dashboard to contain different elements like saved searches.

1 Click the Dashboard tab.
2 On the toolbar, in the Show Dashboard list, select Vulnerability Management.

Creating a customized vulnerability management dashboard

In Extreme Security you can create a vulnerability management **dashboard** that is customized to your requirements.

1 Click the Dashboard tab.

2 On the toolbar, click New Dashboard.

3 Type a name and description for your vulnerability dashboard.

4 Click OK.

5 On the toolbar select Add Item > Vulnerability Management and choose from the following options:

- If you want to show default saved searches on your dashboard, select Vulnerability Searches.
- If you want to show website links to security and vulnerability information, select Security News, Security Advisories, or Latest Published Vulnerabilities.
- If you want show information that is about completed or running scans, select Scans Completed or Scans In Progress.

Related Links

Saving your vulnerability search criteria on page 66

Creating a dashboard for patch compliance

Create a **dashboard** that shows the most effective patch to use to remediate vulnerabilities that are found on the network.

1 Click the Dashboard tab.

2 On the toolbar, click New Dashboard.

3 Type a name and description for your vulnerability dashboard.

4 Click OK.

5 On the toolbar, select Add Item > Vulnerability Management > Vulnerability Searches and choose the default saved search that you want to show on your dashboard.

6 On the header of the new dashboard item, click the yellow Settings icon.

7 Select Patch from the Group By list and then select one of the following options from the Graph By list:

- If you want to see how many assets need to a have the patch applied, select Asset Count.
- If you want to see the cumulative risk score by patch, select Risk Score.
- If you want to see the number of vulnerabilities that are covered by a patch, select Vulnerability Count.

8 Click Save.

9 To view vulnerability details on the Manage Vulnerabilities > By Vulnerability page on the Vulnerabilities tab, click the View in By Vulnerability link at the bottom of the dashboard item.

4 Security software integrations

Extreme Networks Security Vulnerability Manager integrates with other security products to help you manage and prioritize your security risks.

Extreme Networks Security Risk Manager and Extreme Networks Security Vulnerability Manager integration

Extreme Networks Security Vulnerability Manager integrates with Risk Manager to help you prioritize the risks and vulnerabilities in your network.

Risk Manager is installed as a separate appliance and then and added to your Extreme SIEM console as a managed host by using the System and License Management tool on the Admin tab.

For more information about installing Risk Manager, see the *Extreme Networks Security Risk Manager Installation Guide*.

Risk policies and vulnerability prioritization

You can integrate Vulnerability Manager with Risk Manager by defining and monitoring asset or vulnerability risk policies.

When the risk policies that you define in Risk Manager either pass or fail, then the vulnerability risk scores in Vulnerability Manager are adjusted. The adjustment levels depend on the risk policies in your organization.

When the vulnerability risk scores are adjusted in Vulnerability Manager, administrators can do the following tasks:

- Gain immediate visibility of the vulnerabilities that failed a risk policy.

  For example, new information might be displayed on the Extreme Security dashboard or sent by using email.
- Re-prioritize the vulnerabilities that require immediate attention.

  For example, an administrator can use the Risk Score to quickly identify high risk vulnerabilities.

If you apply risk policies at an asset level in Risk Manager, then all the vulnerabilities on that asset have their risk scores adjusted.

For more information about creating and monitoring risk policies, see the *Extreme Networks Security Risk Manager User Guide*.

Related Links

Prioritizing high risk vulnerabilities by applying risk policies on page 70

IBM® Security Endpoint Manager integration

Extreme Networks Security Vulnerability Manager integrates with IBM® Security Endpoint Manager to help you filter and prioritize the vulnerabilities that can be fixed.

Integration components

A typical Vulnerability Manager IBM® Security Endpoint Manager integration consists of the following components:

- An Extreme Networks Security Analytics console.
- A licensed installation of Vulnerability Manager.
- An IBM® Security Endpoint Manager server installation.
- An IBM® Security Endpoint Manager agent installation on each of the scan targets in your network.

Vulnerability remediation

Depending on whether you installed and integrated IBM® Security Endpoint Manager, Vulnerability Manager provides different information to help you remediate your vulnerabilities.

- If IBM® Security Endpoint Manager is not installed, then Vulnerability Manager provides information about vulnerabilities for which a fix is available.

  Vulnerability Manager maintains a list of vulnerability fix information. Fix information is correlated against the known vulnerability catalog.

  Using the Vulnerability Manager search feature, you can identify vulnerabilities that have an available fix.
- If IBM® Security Endpoint Manager is installed, then Vulnerability Manager also provides specific details about the vulnerability fix process. For example, a fix might be scheduled or an asset might be already fixed.

  The IBM® Security Endpoint Manager server gathers fix information from each of the IBM® Security Endpoint Manager agents. Fix status information is transmitted to Vulnerability Manager at pre-configured time intervals.

  Using the Vulnerability Manager search feature, you can quickly identify those vulnerabilities that are scheduled to be fixed or are already fixed.

Related Links

Identifying the patch status of your vulnerabilities on page 72

Configuring SSL for IBM® Security Endpoint Manager integration

You can configure secure socket layer (SSL) encryption to integrate Vulnerability Manager with IBM® Security Endpoint Manager.

1. To download the public key certificate, open your web browser and type `https://IP address/webreports`.

> Remember
> The *`IP address`* is the IP address of your IBM® Security Endpoint Manager server.

2. Click Add Exception.
3. In the Add Security Exception window, click View.
4. Click the Details tab and click Export.
5. In the File name field, type `iemserver_cert.der`
6. In the Save as type field, select X.509 Certificate (DER).
7. Click Save.
8. Copy the public key certificate to your Extreme Security console.
9. To create a Vulnerability Manager truststore.
   a. Using SSH, log in to the Extreme SIEM console as the root user.
   b. Type the following command:

      ```
      keytool -keystore /opt/qvm/iem/truststore.jks -genkey -alias iem.
      ```

   c. At the prompts, type the appropriate information to create the truststore.
10. To import the public key certificate to your truststore, type the following command:

    ```
    keytool -importcert -file iemserver_cert.der -keystore truststore.jks
    -storepass <your truststore password> -alias iem_crt_der
    ```

11. At the Trust this certificate? prompt, type Yes.

Integrating Extreme Networks Security Vulnerability Manager with IBM® Security Endpoint Manager

You can integrate Extreme Networks Security Vulnerability Manager, with IBM® Security Endpoint Manager.

The following components must be installed on your network:

- An IBM® Security Endpoint Manager server.
- An IBM® Security Endpoint Manager agent on each asset in your network that you scan.

If you use secure socket layer (SSL) encryption, ensure that you configure secure socket layer (SSL) for IBM® Security Endpoint Manager integration.

1. Using SSH, log in to the Extreme SIEM console as the root user.
2. Change directory to following location:

   ```
   /opt/qvm/iem
   ```

3 To configure the IBM® Security Endpoint Manager adapter for Vulnerability Manager, type the following commands:

   a Type `./iem-setup-webreports.pl`

   b Type the ***`IP address`*** of the IBM® Security Endpoint Manager server.

   c Type the ***`User name`*** of the IBM® Security Endpoint Manager server.

   d Type the ***`Password`*** of the IBM® Security Endpoint Manager server.

4 At the Use SSL encryption? prompt, type the appropriate response.

> Important
> If you type `Yes`, then ensure that the prerequisite conditions are met.

5 Type the location of your truststore.

6 Type your truststore password.

Security SiteProtector integration

Vulnerability Manager integrates with Security SiteProtector to help direct intrusion prevention system (IPS) policy.

When you configureSecurity SiteProtector, the vulnerabilities that are detected by scans are automatically forwarded to SiteProtector™.

Security SiteProtector receives vulnerability data from Vulnerability Manager scans that are performed only after the integration is configured.

Connecting to Security SiteProtector

You can forward vulnerability data to Security SiteProtector to help direct intrusion prevention system (IPS) policy.

1 On the Admin tab, click System and License Management > Deployment Actions > Manage Vulnerability Deployment.

2 Click Use SiteProtector.

3 In the SiteProtector IP Address field, type the IP address of the Security SiteProtector agent manager server.

4 Click Save and then click Close.

5 On the Admin tab toolbar, click Advanced > Deploy Full Configuration.

6 Click OK.

Scan your network assets to determine if the vulnerability data is displayed in your Security SiteProtector installation.

5 Vulnerability scanning

In Extreme Networks Security Vulnerability Manager, all network scanning is controlled by the scan profiles that you create. You can create multiple scan profiles and configure each profile differently depending on the specific requirements of your network.

Scan profiles

Use scan profiles to do the following tasks:

- Specify the network nodes, domains, or virtual domains that you want to scan.
- Specify the network assets that you want to exclude from scans.
- Create operational windows, which define the times at which scans can run.
- Manually run scan profiles or schedule a scan to run at a future date.
- Run, pause, resume, cancel or delete a single or multiple scans.
- Use centralized credentials to run Windows™, UNIX™, or Linux™ operating systems.
- Scan the assets from a saved asset search.

Related Links

Centralized credential sets on page 41

Creating a scan profile

In Extreme Networks Security Vulnerability Manager, you configure scan profiles to specify how and when your network assets are scanned for vulnerabilities.

1 Click the **Vulnerabilities** tab.

2 In the navigation pane, click **Administrative** > **Scan Profiles**.

3 On the toolbar, click **Add**.

When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. In addition, you can also configure the following optional settings.

- If you added more scanners to your Vulnerability Manager deployment, select a scanner from the **Scan Server** list. This step is unnecessary if you want to use dynamic scanning.
- To enable this profile for on-demand scanning, click the **On Demand Scanning Enabled** check box.

  By selecting this option, you make the profile available to use if you want to trigger a scan in response to a custom rule event. It also enables on-demand vulnerability scanning by using the right-click menu on the **Assets** page.
- To specify which scanner to use for each CIDR range, click the **Dynamic server selection** check box.

  If you configured domains in the **Admin** > **Domain Management** window, you can select one from the **Domain** list. Only assets within the domain you selected are scanned.
- To scan your network by using a predefined set of scanning criteria, select a scan type from the **Scan Policies** list.
- If you configured centralized credentials for assets, click the **Use Centralized Credentials** check box. For more information, see the .

4 Click **Save**.

Related Links

Options for adding scanners to your Vulnerability Manager deployment on page 14

Associating vulnerability scanners with CIDR ranges on page 53

In Extreme Networks Security Vulnerability Manager, to do dynamic scanning, you must associate vulnerability scanners with different segments of your network.

Rescanning an asset by using the right-click menu option on page 32

Scan policies on page 54

Dynamic vulnerability scans on page 52

In Extreme Networks Security Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Configuring a scan policy to manage your vulnerability scans on page 55

In Extreme Networks Security Vulnerability Manager, you can configure a scan policy to control your vulnerability scans.

Creating an external scanner scan profile

In Extreme Networks Security Vulnerability Manager, you can configure scan profiles to use a hosted scanner to scan assets in your DMZ.

Vulnerability Manager must be configured with a hosted scanner. For more information, see Scanning the assets in your DMZ on page 16.

1 Click the **Vulnerabilities** tab.

2 In the navigation pane, click **Administrative** > **Scan Profiles**.

3 On the toolbar, click **Add**.

When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To create an external scanner profile, you must also follow the remaining steps in this procedure.

4 Select an external scanner from the **Scan Server** list.

5 Select **Full Scan** or **Web Scan** from the **Scan Policies** list.

6 Click the **Domain and Web App** tab. In the **Virtual Webs** pane, enter the domain and IP address information for the websites and applications that you want to scan.

7 Click **Save**.

Creating a benchmark profile

To create Center for Internet Security compliance scans, you must configure benchmark profiles. You use CIS compliance scans to test for Windows™ and Red Hat Enterprise Linux™ CIS benchmark compliance.

1 Click the **Vulnerabilities** tab.

2 In the navigation pane, click **Administrative** > **Scan Profiles**.

3 On the toolbar, click **Add Benchmark**.

4 If you want to use pre-defined centralized credentials, select the **Use Centralized Credentials** check box.

Credentials that are used to scan Linux™ operating systems must have root privileges. Credentials that are used to scan Windows™ operating systems must have administrator privileges.

5 If you are not using dynamic scanning, select a Vulnerability Manager scanner from the **Scan Server** list.

6 To enable dynamic scanning, click the **Dynamic server selection** check box.

If you configured domains in the **Admin** > **Domain Management** window, you can select a domain from the **Domain** list. Only assets within the CIDR ranges and domains that are configured for your scanners are scanned.

7 In the **When To Scan** tab, set the run schedule, scan start time, and any pre-defined operational windows.

8 In the **Email** tab, define what information to send about this scan and to whom to send it.

9 If you are not using centralized credentials, add the credentials that the scan requires in the **Additional Credentials** tab.

Credentials that are used to scan Linux™ operating systems must have root privileges. Credentials that are used to scan Windows™ operating systems must have administrator privileges.

10 Click **Save**.

Related Links

Centralized credential sets on page 41

Running scan profiles manually

In Extreme Networks Security Vulnerability Manager you can run one or more scan profile manually.

You can also schedule scans to run at a future date and time. For more information, see Scan scheduling on page 34.

Ensure that a vulnerability processor is deployed. For more information, see Verifying that a vulnerability processor is deployed on page 14.

1 Click the **Vulnerabilities** tab.
2 In the navigation pane, select **Administrative** > **Scan Profiles**.
3 On the **Scan Profiles** page, select the check box on the row assigned to the scan profiles that you want to run.

> Note
> To find the scan profiles you want to run, use the toolbar **Name** field to filter scan profiles by name.

4 On the toolbar, click **Run**.

By default, scans complete a fast scan by using the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocol. A fast scan includes most ports in the range 1 - 1024.

Related Links

Managing scan results on page 57

Scan profile details on page 33

Rescanning an asset by using the right-click menu option

In Extreme Networks Security Vulnerability Manager, you can quickly rescan an asset by using the right-click option.

The right-click scan option is also available on the Extreme Security **Offenses** tab, and the Risk Manager sub-net asset view.

1 Click the **Vulnerabilities** tab.
2 In the navigation pane, select **Manage Vulnerabilities** > **By Asset**.
3 On the **By Asset** page, identify the asset that you want to rescan.
4 Right-click the **IP Address** and select **Run Vulnerability Scan**.
5 In the **Run Vulnerability Scan** window, select the scan profile that you want use when the asset is rescanned.

The scanning process requires a scan profile. The scan profile determines the scanning configuration options that are used when the scan runs.

To view a scan profile in the **Run Vulnerability Scan** window, you must select the **On Demand Scanning Enabled** check box in the **Details** tab on the **Scan Profile Configuration** page.

> Important
> The scan profile that you select might be associated with multiple scan targets or IP address ranges. However, when you use the right-click option, only the asset that you select is scanned.

6 Click **Scan Now**.

7 Click **Close Window**.

8 To review the progress of your right-click scan, in the navigation pane, click **Scan Results**.

Right-click scans are identified by the prefix **RC:**.

Related Links

Asset vulnerabilities on page 67

Scan profile details

In Extreme Networks Security Vulnerability Manager, you can describe your scan, select the scanner that you want to use, and choose from a number of scan policy options.

Scan profile details are specified in the **Details** tab, in the **Scan Profile Configuration** page.

See especially the following options:

Table 3: Scan profile details configuration options

Options	Description
Use Centralized Credentials	Specifies that the profile uses pre-defined credentials. Centralized credentials are defined in the **Admin** > **System Configuration** > **Centralized Credentials** window.
Scan Server	The scanner that you select depends on your network configuration. For example, to scan DMZ assets, then select a scanner that has access to that area of your network. The **Controller** scan server is deployed with the vulnerability processor on your Extreme Security console or Vulnerability Manager managed host. Note You can have only 1 vulnerability processor in your deployment. However, you can deploy multiple scanners either on dedicated Vulnerability Manager managed host scanner appliances or Extreme Security managed hosts.
On Demand Scanning	Enables on-demand asset scanning for the profile. Use the right-click menu on the **Assets** page to run on-demand vulnerability scanning. By selecting this option, you also make the profile available to use if you want to trigger a scan in response to a custom rule event. By enabling on-demand scanning, you also enable dynamic scanning.
Dynamic server selection	Specifies whether you want to use a separate vulnerability scanner for each CIDR range that you scan. During a scan, Vulnerability Manager automatically distributes the scanning activity to the correct scanner for each CIDR range that you specify. If you configured domains in the **Domain Management** window of the **Admin** tab, you can also select the domain that you want to scan.
Bandwidth Limit	The scanning bandwidth. The default setting is medium. Important If you select a value greater than 1000 kbps, you can affect network performance.
Scan Policies	The pre-configured scanning criteria about ports and protocols. For more information, see Scan policies on page 54.

Related Links

Dynamic vulnerability scans on page 52

In Extreme Networks Security Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

Scan policies on page 54

Scan scheduling

In Extreme Networks Security Vulnerability Manager, you can schedule the dates and times that it is convenient to scan your network assets for known vulnerabilities.

Scan scheduling is controlled by using the When To Scan pane, in the Scan Profile Configuration page.

A scan profile that is configured with a manual setting must be run manually. However, scan profiles that are not configured as manual scans, can also be run manually.

When you select a scan schedule, you can further refine your schedule by configuring a permitted scan interval.

Related Links

Configuring a permitted scan interval on page 50

Reviewing your scheduled scans in calendar format on page 35

Scanning domains monthly

In Extreme Networks Security Vulnerability Manager, you can configure a scan profile to scan the domains on your network each month.

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.
   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To set up monthly scans, you must also follow the remaining steps in this procedure.
4. Click the **When To Scan** pane.
5. In the **Run Schedule** list, select **Monthly**.
6. In the **Start Time** field, select a start date and time for your scan.
7. In the **Day of the month** field, select a day each month that your scan runs.
8. Click the **Domain and Web App** tab.
9. In the **Domains** field, type the URL of the asset that you want to scan and click (**>**).
10. Click **Save**.
11. During and after the scan, you can monitor scan progress and review completed scans.

Scheduling scans of new unscanned assets

In Extreme Networks Security Vulnerability Manager, you can configure scheduled scans of newly discovered, unscanned network assets.

1. Click the Assets tab.
2. In the navigation pane, click Asset Profiles, then on the toolbar click Search > New Search.
3. To specify your newly discovered, unscanned assets, complete the following steps in the Search Parameters pane:

   a. Select Days Since Asset Found, Less than 2 then click Add Filter.
   b. Select Days Since Asset Scanned Greater than 2 then click Add Filter.
   c. Click Search.
4. On the toolbar, click Save Criteria and complete the following steps:

   a. In the Enter the name of this search field, type the name of your asset search.
   b. Click Include in my Quick Searches.
   c. Click Share with Everyone.
   d. Click OK.
5. Click the Vulnerabilities tab.
6. In the navigation pane, select Administrative > Scan Profiles.
7. On the toolbar, click Add.

   When you create a scan profile, the only mandatory fields are Name and IP Addresses on the Details tab of the Scan Profile Configuration page. To schedule scans for unscanned assets, you must also follow the remaining steps in this procedure.
8. In the Include Saved Searches pane, select your saved asset search from the Available Saved Searches list and click (>).
9. Click the When To Scan pane and in the Run Schedule list, select Weekly.
10. In the Start Time fields, type or select the date and time that you want your scan to run on each selected day of the week.
11. Select the check boxes for the days of the week that you want your scan to run.
12. Click Save.

    For more information about using the Assets tab and saving asset searches, see the *Users Guide* for your product.

Related Links

Searching vulnerability data on page 63

Reviewing your scheduled scans in calendar format

In Extreme Networks Security Vulnerability Manager, the scheduled scan calendar provides a central location where you can review information about scheduled scans.

1. Click the Vulnerabilities tab.
2. In the navigation pane, click Administrative > Scheduled Scans.
3. Hover your mouse on the scheduled scan to display information about the scheduled scan.

   For example, you can show the time that a scan took to complete.
4. Double-click a scheduled scan to edit the scan profile.

Network scan targets and exclusions

In Extreme Networks Security Vulnerability Manager, you can provide information about the assets, domains, or virtual webs on your network that you want to scan.

Use the **Details** tab on the **Scan Profile Configuration** page to specify the network assets that you want to scan.

You can exclude a specific host or range of hosts that must never be scanned. For example, you might restrict a scan from running on critical servers that are hosting your production applications. You might also want to configure your scan to target only specific areas of your network.

Vulnerability Manager integrates with Extreme Security by providing the option to scan the assets that form part of a saved asset search.

Scan targets

You can specify your scan targets by defining a CIDR range, IP address, IP address range, or a combination of all three.

Domain scanning

You can add domains to your scan profile to test for DNS zone transfers on each of the domains that you specify.

A host can use the DNS zone transfer to request and receive a full zone transfer for a domain. Zone transfer is a security issue because DNS data is used to decipher the topology of your network. The data that is contained in a DNS zone transfer is sensitive and therefore any exposure of the data might be perceived as a vulnerability. The information that is obtained might be used for malicious exploitation such as DNS poisoning or spoofing.

Scans that used saved asset searches

You can scan the assets and IP addresses that are associated with a Extreme Security saved asset search.

Any saved searches are displayed in the **Asset Saved Search** section of the **Details** tab.

For more information about saving an asset search, see the *Users Guide* for your product.

Exclude network scan targets

In **Excluded Assets** section of the **Domain and Web App** tab, you can specify the IP addresses, IP address ranges, or CIDR ranges for assets that must not be scanned. For example, if you want to avoid scanning a highly loaded, unstable, or sensitive server, exclude these assets.

When you configure a scan exclusion in a scan profile configuration, the exclusion applies only to the scan profile.

Virtual webs

You can configure a scan profile to scan different URLs that are hosted on the same IP address.

When you scan a virtual web, Vulnerability Manager checks each web page for SQL injection and cross site scripting vulnerabilities.

Related Links

Scanning CIDR ranges with different vulnerability scanners on page 53

In Extreme Networks Security Vulnerability Manager, you can scan areas of your network with different vulnerability scanners.

Excluding assets from all scans on page 37

In Extreme Networks Security Vulnerability Manager, scan exclusions specify the assets in your network that are not scanned.

Scheduling scans of new unscanned assets on page 34

Scanning domains monthly on page 34

Excluding assets from all scans

In Extreme Networks Security Vulnerability Manager, scan exclusions specify the assets in your network that are not scanned.

Scan exclusions apply to all scan profile configurations and might be used to exclude scanning activity from unstable or sensitive servers. Use the IP Addresses field on the Scan Exclusion page to enter the IP addresses, IP address ranges, or CIDR ranges that you want to exclude from all scanning. To access the Scan Exclusion page:

1. Click the Vulnerabilities tab.
2. In the navigation pane, click Administrative > Scan Exclusions.
3. On the toolbar, select Actions > Add.

Note

You can also use the Excluded Assets section of the Vulnerabilities > Administrative > Scan Profiles > Add > Domain and Web App tab to exclude assets from an individual scan profile.

Managing scan exclusions

In Extreme Networks Security Vulnerability Manager you can update, delete, or print scan exclusions.

1. Click the Vulnerabilities tab.
2. In the navigation pane, click Administrative > Scan Exclusions.
3. From the list on the Scan Exclusions page, click the Scan Exclusion that you want to modify.
4. On the toolbar, select an option from the Actions menu.
5. Depending on your selection, follow the on-screen instructions to complete this task.

Scan protocols and ports

In Extreme Networks Security Vulnerability Manager, you can choose different scan protocols and scan various port ranges.

Use the How To Scan pane on the Scan Profile Configuration page to specify scanning protocols and the ports that you want to scan.

You can configure your scan profile port protocols by using the following options:

Table 4: scan protocol and port options

Protocol	Description
TCP and UDP	The default scan protocol that scans common ports in the range 1 - 1024. Remember Compared with other scanning protocols, TCP and UDP might generate more network activity.
TCP	The most common scanning protocol. When TCP scanning is combined with IP range scanning, you can locate a host that is running services that are prone to vulnerabilities. The default port range is 1 - 65535.
SYN	Sends a packet to all specified ports. If the target is listening, it responds with a SYN and Acknowledgement (ACK). If the target is not listening, it responds with an RST (reset). Normally, the destination port is closed and an RST is returned. The default port range is 1 - 65535.
ACK	Similar to SYN, but in this case an ACK flag is set. The ACK scan does not determine whether the port is open or closed, but tests if the port is filtered or unfiltered. Testing the port is useful when you probe for the existence of a firewall and its rule sets. Simple packet filtering enables established connections (packets with the ACK bit set), whereas a more sophisticated stateful firewall might not. The default port range is 1-65535.
FIN	A TCP packet that is used to terminate a connection, or it can be used as a method to identify open ports. FIN sends erroneous packets to a port and expects open listening ports to send back different error messages than closed ports. The scanner sends a FIN packet, which might close a connection that is open. Closed ports reply to a FIN packet with an RST. Open ports ignore the packet in question. The default port range is 1 - 65535.

Scanning a full port range

In Extreme Networks Security Vulnerability Manager, you can scan the full port range on the assets that you specify.

1 Click the Vulnerabilities tab.

2 In the navigation pane, select Administrative > Scan Profiles.

3 On the toolbar, click Add.

When you create a scan profile, the only mandatory fields are Name and IP Addresses on the Details tab of the Scan Profile Configuration page. To scan a full port range, you must also follow the remaining steps in this procedure.

4 Click the How To Scan tab.

5 In the Protocol field, accept the default values of TCP & UDP.

6 In the Range field, type 1-65535.

Note

Port ranges must be configured in dash-separated, comma-delimited, consecutive, ascending, and non-overlapping order. Multiple port ranges must be separated by a comma. For example, the following examples show the delimiters that are used to enter port ranges:(1-1024, 1055, 2000-65535).

7 In the Timeout (m) field, type the time in minutes after which you want the scan to cancel if no scan results are discovered.

Important

You can type any value in the range 1 - 500. Ensure that you do not enter too short a time, otherwise the port scan cannot detect all running ports. Scan results that are discovered before the timeout period are displayed.

8 Click Save.

9 In the Scan Profiles page, click Run.

Scanning assets with open ports

In Extreme Networks Security Vulnerability Manager, you can configure a scan profile to scan assets with open ports.

1 Click the Assets tab.

2 In the navigation pane, click Asset Profiles then on the toolbar, click Search > New Search.

3 To specify assets with open ports, configure the following options in the Search Parameters pane:

a Select Assets With Open Port, Equals any of 80 and click Add Filter.

b Select Assets With Open Port, Equals any of 8080 and click Add Filter.

c Click Search.

4 On the toolbar, click Save Criteria and configure the following options:

a In the Enter the name of this search field, type the name of your asset search.

b Click Include in my Quick Searches.

c Click Share with Everyone and click OK.

5 Click the Vulnerabilities tab.

6 In the navigation pane, select Administrative > Scan Profiles.

7 On the toolbar, click Add.

When you create a scan profile, the only mandatory fields are Name and IP Addresses on the Details tab of the Scan Profile Configuration page. To scan assets with open ports, you must also follow the remaining steps in this procedure.

8 On the Details tab, select your saved asset search from the Available Saved Searches list and click >.

When you include a saved asset search in your scan profile, the assets and IP addresses associated with the saved search are scanned.

9 Click the When To Scan pane and in the Run Schedule list, select Manual.

10 Click the What To Scan pane.

11 Click **Save**.

For more information about saving an asset search, see the *Users Guide* for your product.

Perform the steps in the procedure, Running scan profiles manually on page 31.

Authenticated patch scans

In Extreme Networks Security Vulnerability Manager, you can scan for community names and run authenticated patch scans for Windows™, Linux™, and UNIX™ operating systems.

SNMP community names

You can scan your network assets by using SNMP community names.

When you scan assets, Vulnerability Manager authenticates by using the SNMP services that are found and completes a more detailed vulnerability scan.

Windows™ patch scans

To scan Windows™ operating systems for missing patches, remote registry access and Windows™ management interface (WMI) must be enabled. If your Windows™ patch scan returns WMI connectivity issues, you must configure your windows systems.

To read WMI data on a remote server, you must enable the connections between your Extreme Security console and the server that you are monitoring. If the server is using a Windows™ firewall, then you must configure the system to enable remote WMI requests.

If you are use a non-administrator account to monitor the Windows™ server, then you must enable the account to interact with Distributed Component Object Model (DCOM).

If the patch scan tool cannot connect to a Windows™ asset, a yellow triangular warning icon is displayed next to the asset in the scan results. The following vulnerability is raised: `Local Checks Error`.

Secure Linux™ operating system authenticated scanning

To scan Linux™ operating systems by using secure authentication, you can configure public key encryption between your console or managed host and your scan targets.

When secure authentication is configured, you do not need to specify a Linux™ operating system password in your scan profile.

You must configure public key authentication on every Linux™ operating system that you want to scan.

If you move your vulnerability processor to a dedicated vulnerability processor appliance, you must reconfigure the secure authentication between the dedicated vulnerability processor appliance and the scan target.

If the patch scan tool cannot connect to a Linux™ asset, a yellow triangular warning icon is displayed next to the asset in the scan results. The following vulnerability is raised: `SSH Patch Scanning - Failed Logon`.

Related Links

Configuring Linux operating system public key authentication on page 41

Configuring an authenticated scan of the Linux or UNIX operating systems on page 42

Configuring an authenticated scan of the Windows operating system on page 44

Centralized credential sets

When you run authenticated scans, you can use a central list that stores the login credentials for your Linux™, UNIX™, or Windows™ operating systems. Your system administrator must configure the list of credentials.

An administrator can specify credentials for SNMP network devices and Linux™, UNIX™, or Windows™ operating systems. Therefore, a user who is responsible for configuring a scan profile does not need to know the credentials of each asset that is scanned. Also, if the credentials of an asset change, the credentials can be modified centrally rather than updating the scan profile.

Related Links

Configuring an authenticated scan of the Linux or UNIX operating systems on page 42

Configuring an authenticated scan of the Windows operating system on page 44

Creating a benchmark profile on page 31

To create Center for Internet Security compliance scans, you must configure benchmark profiles. You use CIS compliance scans to test for Windows™ and Red Hat Enterprise Linux™ CIS benchmark compliance.

Configuring a credential set

In Extreme Networks Security Vulnerability Manager, you can create a credential set for the assets in your network. During a scan, if a scan tool requires the credentials for a Linux™, UNIX™, or Windows™ operating system, the credentials are automatically passed to the scan tool from the credential set.

1 Click the **Admin** tab.
2 In the **System Configuration** pane, click **Centralized Credentials**.
3 In the **Centralized Credentials** window, on the toolbar, click **Add**.

   To configure a credential set, the only mandatory field in the **Credential Set** window is the **Name** field.
4 In the **Credential Set** window, click the **Assets** tab.
5 Type a CIDR range for the assets that you want to specify credentials for and click **Add**.
6 Click the **Linux/Unix, Windows, or Network Devices (SNMP)** tabs, then type your credentials.
7 Click **Save**.

Configuring Linux™ operating system public key authentication

To scan Linux™ operating systems by using secure public key authentication, you must configure your Extreme Networks Security Analytics console or managed host and the asset that you want to scan. When authentication is configured you can do authenticated scanning by specifying a Linux™ operating system user name, and not specifying a password. Extreme Security supports both `rsa` and `dsa` for SSH key generation.

You must configure your public key on the device where your vulnerability processor is installed. For more information, see Verifying that a vulnerability processor is deployed on page 14.

1. Using SSH, log in to the Extreme Security console or managed host as the root user.
2. Generate a public DSA key pair by typing the following command:

   ```
   su -m -c 'ssh-keygen -t dsa' qvmuser
   ```
3. Accept the default file by pressing Enter.
4. Accept the default passphrase for the DSA key by pressing the Enter key.
5. Press the Enter key again to confirm.
6. Copy the public key to the scan target by typing the following command:

   ```
   ssh-copy-id -i /home/qvmuser/.ssh/id_dsa.pub root@<IP address>
   ```

   Change *`<IP address>`* to the IP address of the scan target.
7. Type the passphrase for the scan target.
8. Check that the ***`qvmuser`*** account on the console can SSH to the scan target without a passphrase by typing the following command:

   ```
   su -m -c 'ssh -o StrictHostKeyChecking=no root@<IP address> ls'
   qvmuser
   ```

   Change *`<IP address>`* to the IP address of the scan target.

   A list of the files in the root user's home directory on the scan target is displayed.

Create a scan profile in Vulnerability Manager with user name ***`root`*** without specifying a password and run a patch scan.

Related Links

Configuring an authenticated scan of the Linux or UNIX operating systems on page 42

Configuring an authenticated scan of the Linux™ or UNIX™ operating systems

In Extreme Networks Security Vulnerability Manager, you can configure an authentication scan of the Linux™ or UNIX™ operating systems that are on your network. You can manually specify the credentials in the scan profile or use a credential set.

To scan by using a credential list, you must first define a central list of the credentials that are required by your operating systems. For more information, see Configuring a credential set on page 41.

1. Click the Vulnerabilities tab.
2. In the navigation pane, select Administrative > Scan Profiles.
3. On the toolbar, click Add.

   When you create a scan profile, the only mandatory fields are Name and IP Addresses on the Details tab of the Scan Profile Configuration page. To configure an authenticated scan, you must also follow the remaining steps in this procedure.

4. Click **Use Centralized Credentials** to scan your Linux™ or UNIX™ operating systems.

   If a credential set is not configured and you do not manually specify the credentials, the scan tools run but no credentials are passed in.

   If a credential set exists for the hosts that you are scanning, any credentials that you manually specify in the **Additional Credentials** tab, override your credential set.
5. Click the **When To Scan** tab.
6. In the **Run Schedule** list, select **Manual**.
7. Click the **Additional Credentials** tab.
8. In the **Linux/Unix Patch Scanning** area, type the user name and password for the Linux™ or UNIX™ hosts that you want to scan and click **>**.

   A password is not required, if you configured secure public key authentication between your console and your scan target.
9. Click **Save**.
10. In the **Scan Profiles** page, click **Run**.

Related Links

Centralized credential sets on page 41

Configuring a credential set on page 41

> In Extreme Networks Security Vulnerability Manager, you can create a credential set for the assets in your network. During a scan, if a scan tool requires the credentials for a Linux™, UNIX™, or Windows™ operating system, the credentials are automatically passed to the scan tool from the credential set.

Configuring Linux operating system public key authentication on page 41

Enabling permissions for Linux™ or UNIX™ patch scans

Non-root user accounts must have the permissions to run the commands that Vulnerability Manager requires to scan for patches on Linux™ and UNIX™ computers.

To assign the relevant permissions for Linux™ or UNIX™ patch scanning, use the following procedure:

1. SSH to the asset.
2. Run the following `uname` commands:

```
uname -m
uname -n
uname -s
uname -r
uname -v
uname -p
uname -a
```

3. Depending on your operating system, run the following commands:

Operating System	Commands
Linux™	Read the contents of the following files that are relevant for your distribution:

Operating System	Commands

	• /etc/redhat-release
	• /etc/SuSE-release
	• /etc/debian-version
	• /etc/slackware-version
	• /etc/mandrake-version
	• /etc/gentoo-version
	For example, on Red Hat Enterprise Linux™, use the commands:
	`ls /etc/redhat-releasecat`
	`/etc/redhat-release`
	`rpm -qa --qf '%{NAME}--%{VERSION}---%{RELEASE}`
	`\\|%{EPOCH}--%{ARCH}---%{FILENAMES}--%{SIGPGP}---%{SIGGPG}\n'`
	`rpm -qa --qf '%{NAME}-%{VERSION}-%{RELEASE}|%{EPOCH}\n'`

Solaris	`/usr/bin/svcs -a`
	`/usr/bin/pkginfo -x \\| awk '{ if ( NR % 2 ) { prev = \$1 }`
	` else  { print prev\" \"\$0  } }'`
	`/usr/bin/showrev -p`
	`/usr/sbin/patchadd -p`
	`/usr/bin/isainfo -b`
	`/usr/bin/isainfo -k`
	`/usr/bin/isainfo -n`
	`/usr/bin/isainfo -v`

HP-UX	`/usr/sbin/swlist -l fileset -a revision`
	`/usr/sbin/swlist -l patch`

AIX®	`oslevel -r`
	`lslpp -Lc`

ESX	`vmware -vesxupdate query --all`
	`. /etc/profile ;  /sbin/esxupdate query –all`

Configuring an authenticated scan of the Windows™ operating system

In Extreme Networks Security Vulnerability Manager, you can configure a scan of the Windows™ operating systems that are installed on your network. You can manually specify the credentials in the scan profile or use a credential set.

If scanning is performed without administrative privileges, then Vulnerability Manager scans the remote registry for each installation on the Windows™ operating system.

Scanning without administrative privileges is incomplete, prone to false positives, and does not cover many third-party applications.

Vulnerability Manager uses standard Windows™ operating system remote access protocols that are enabled by default in most windows deployments.

If your Windows™ scan results return a local checks error vulnerability, that indicates Windows™ management interface (WMI) connectivity issues, then you must configure your Windows™ systems.

For more information about Windows™ connectivity, see:

- Enabling remote registry access to assets on the Windows operating system on page 46.
- Configuring Windows Management Instrumentation on page 47.

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add**.

   When you create a scan profile, the only mandatory fields are **Name** and **IP Addresses** on the **Details** tab of the **Scan Profile Configuration** page. To configure an authenticated scan of the Windows™ operating system, you must also follow the remaining steps in this procedure.
4. Click **Use Centralized Credentials** to scan your Windows™ operating systems.

   You must configure a credential set or manually specify credentials for hosts before scan tools that require credentials can run.

   If a credential set exists for the hosts that you are scanning, any credentials that you manually specify in the **Additional Credentials** tab, override your credential set.
5. Click the **When To Scan** pane.
6. In the **Run Schedule** list, select **Manual**.
7. Click the **Additional Credentials** area.
8. In the **Windows Patch Scanning** area, type the **Domain**, **Username**, and **Password** for the Windows™ hosts that you want to scan and click (**>**).
9. Click **Save**.
10. In the **Scan Profiles** page, click **Run**.

Related Links

Centralized credential sets on page 41

Authenticated patch scans on page 40

Windows™ patch scanning

Windows™ patch scanning is an authenticated network-based method that is used to interrogate the target computer for missing security-related patches and updates.

Windows™ patch scanning requires access to 3 key Windows™ services:

- Remote Registry
- WMI
- Administrative Shares

It is possible scan computers for Windows™ patches without using WMI and Administrative Shares but the results are not complete and are prone to false positives.

Use complex passwords. However, some special characters can cause issues. Limit the special characters to numbers, periods, colons, semi-colons, quotation marks, percentage signs, and spaces.

Remote Registry

The Remote Registry service must be enabled and started and accessible from both the Vulnerability Manager scanner appliance and the configured scanning user used in the scan profile.

If the remote registry cannot be accessed, windows patch scanning fails completely.

If Vulnerability Manager cannot access the remote registry, the scan results record the following error:

```
Local Checks Error – Remote Registry Service Not Running
```

In Vulnerability Manager V7.7.2.3 and later, a yellow triangle icon is displayed next to the asset in the scan results.

The status of the remote registry service can be verified from the **Administrative Control Panel** under **Services**. Ensure that the following dependent services are started:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC EndPoint Manager

Vulnerability Manager can access the remote registry over the classic NetBIOS (ports 135, 137, 139) or the newer NetBIOS over TCP (on port 445). Network or personal firewalls that block access to either of these protocols prevents access to Windows™ patch scans.

Administrative user accounts have access to the remote registry by default. Non-administrative user accounts do not have access to the remote registry. You must configure access.

Enabling remote registry access to assets on the Windows™ operating system

To scan Windows-based systems, you must configure your registry.

1 Log in to your Windows-based system.
2 Click **Start**.
3 In the **Search programs and files** field, type **services** and press Enter.
4 In the **Services** window, locate the **Remote Registry** service.
5 Right-click the **Remote Registry** service and click **Start**.
6 Close the **Services** window.

Assigning minimum remote registry permissions

Administrative user accounts have access to the remote registry by default. Non-administrative user accounts do not have access to the remote registry. You must configure access.

1 On the target Windows™ computer, create or designate a Local or Global User (example, "QVM_scan_user") and assign read-only Registry access to the non-administrative user account.
2 Log on to your Windows™ computer by using an account that has administrator privileges. Click **Start** > **Run**.
3 Type `regedit`.
4 Click **OK**.

5 Go to the key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers \winreg.

The permissions that are associated with this registry key control which users or group can access the registry remotely from the network.

6 Highlight the winreg key and do one of the following steps:

- On Windows™ XP or later, click Edit > Permissions.
- On Windows™ 2000, click Security > Permissions.

7 Give read-only access to the designated "QVM_scan_user" account.

On Windows™ XP, the *ForceGuest* setting is enabled by default when in workgroup mode. This setting might cause access problems for WMI connections and shares access, other DCOM services, and RPC services. You cannot disable the *ForceGuest* setting on Windows™ XP Home computers.

Configuring Windows™ Management Instrumentation

Vulnerability Manager uses Windows™ Management Instrumentation (WMI) to locate and identify versions of the installed .exe and .dll files on the target assets that are scanned.

Without the information that is provided by WMI, many third-party applications are missed. False positives that are detected during registry scanning (by using the remote registry service) cannot be identified or removed by Vulnerability Manager.

WMI is installed on all of modern Windows™ operating systems, such as Windows™ Vista, Windows™ 2008, Windows™ 2012, Windows™ 7, Windows™ 8, and Windows™ 8.1).

Remote WMI requests must be enabled and accessible by the scanning user on assets that are scanned. If WMI is not available, the following error is reported in the scan results:

```
Local Checks Error – Unable to Query WMI serviceMount Remote Filesystem
```

In Vulnerability Manager V7.7.2.3 and above, a yellow triangle warning icon appears next to the asset in the scan results.

If your patch scan is not successful, do the following steps.

1 On the target server, go to Control Panel > Administrative Tools > Computer Management.

2 Expand Services and Applications.

3 Right-click WMI Control and click Properties.

4 Click the Security tab.

5 Click Security.

6 If necessary, add the monitoring user, and click the Remote Enable check box for the user or group that requests WMI data. To add a monitoring user or group:

a Click Add.

b In the Enter the object names to select field, type the name of your group or user name.

c Click OK.

7 Click Advanced and apply to the root and sub name spaces.

> Note
>
> In some cases, you might also need to configure the Windows™ firewall and DCOM settings.
>
> If you experience WMI issues, you can install the WMI Administrative tools from the Microsoft™ website.
>
> The tools include a WMI browser that helps you connect to a remote machine and browse through the WMI information. These tools help you to isolate any connectivity issues in a more direct and simpler environment.

Allow WMI requests through a Windows™ firewall

To read WMI data on a remote server, a connection must be made from your management computer (where the monitoring software is installed) to the server that you are monitoring. If the target server is running the Windows™ Firewall (also called Internet Connection Firewall) which is installed on Windows™ XP and Windows™ 2003computers, you must configure the firewall to allow remote WMI requests through.

To configure Windows™ Firewall to allow remote WMI requests, open a command prompt and enter the following command:

```
netsh firewall set service RemoteAdmin enable
```

Setting minimum DCOM permissions

To connect to a remote computer by using WMI, you must ensure that the correct DCOM settings and WMI namespace security settings are enabled for the connection.

To grant DCOM remote launch and activation permissions for a user or group, do these steps.

1 Click Start > Run, type `DCOMCNFG`, and then click OK.
2 In the Component Services dialog box, expand Component Services, expand Computers, and then right-click My Computer and click Properties.
3 In the My Computer Properties dialog box, click the COM Security tab.
4 Under Launch and Activation Permissions, click Edit Limits.
5 In the Launch Permission dialog box, if your name or your group does not appear in the Groups or user names list, follow these steps:
   a In the Launch Permission dialog box, click Add.
   b In the Select Users, Computers, or Groups dialog box, add your name and the group in the Enter the object names to select box, and then click OK.
6 In the Launch Permission dialog box, select your user and group in the Group or user names box.
7 In the Allow column under Permissions for User, select Remote Launch and select Remote Activation, and then click OK.

Setting DCOM remote access permissions

You must grant DCOM remote access permissions for certain users and groups.

If Computer A is connecting remotely to Computer B, you can set these permissions on Computer B to allow a user or group that is not part of the Administrators group on Computer B to connect to Computer B.

1. Click Start > Run, type `DCOMCNFG`, and then click OK.
2. In the Component Services dialog box, expand Component Services, expand Computers, and then right-click My Computer and click Properties.
3. In the My Computer Properties dialog box, click the COM Security tab.
4. Under Access Permissions, click Edit Limits.
5. In the Access Permission dialog box, select the ANONYMOUS LOGON name in the Group or user names box. In the Allow column under Permissions for User, select Remote Access, and then click OK.

Administrative shares

All Windows™ computers have administrative shares, `\\machinename\driveletter$` enabled, especially when they are part of a domain.

Extreme Security Vulnerability Manager uses administrative shares to detect vulnerabilities on the following limited set of applications:

- Mozilla Firefox
- Mozilla Thunderbird
- Java™ FX
- Apache Archiva
- Apache Continuum
- Google ChromePreferences

Administrative shares are not visible to non-administrative users, and some organizations disable administrative shares or use non-administrative user accounts to scan. If administrative shares are not accessible, Extreme Security Vulnerability Manager might miss vulnerabilities in the products in the preceding list or produce false positives. In general, Extreme Security Vulnerability Manager vulnerability tests use only administrative shares as a last resort, and use registry scans and WMI.

Enabling administrative shares

On Windows™ Vista or later, administrative shares are disabled by default when in “workgroup” mode.

Enable administrative shares by using these steps:

1. Click Start > Run and type `regedit`.
2. Go to the key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. Right-click WMI Control and click Properties.
4. Add a new DWORD named: `LocalAccountTokenFilterPolicy`
5. Set the value to `1`.

Disabling administrative shares

Some organizations do not want to enable administrative shares. However, when enable the remote registry service, the server service is started and administrative shares are enabled.

To disable administrative shares, modify the following registry key:

1. Click Start > Run and type `regedit`.
2. Go to the key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\
3. Set the ***`AutoShareWks`*** parameter to `0`.

Note

This action does not disable the IPC$ share. Although this share is not used to access files directly, ensure that anonymous access to this share is disabled. Alternatively, you can remove the IPC$ share completely by deleting it at start-up by using the following command:

```
net share IPC$ /delete
```

Use this method to remove the C$ and D$ shares also.

Configuring a permitted scan interval

In Extreme Networks Security Vulnerability Manager, you can create an operational window to specify the times that a scan can run.

If a scan does not complete within the operational window, it is paused and continues when the operational window reopens. To configure an operational window:

1. Click the Vulnerabilities tab.
2. In the navigation pane, click Administrative > Operational Window.
3. On the toolbar, click Actions > Add.
4. Enter a name for the operational window in the Name field.
5. Choose an operational window schedule from the Schedule list.
6. Select the times when scanning is permitted.
7. Select your timezone.
8. If you selected Weekly from the Schedule list, then click the desired days of the week check boxes in the Weekly area.
9. If you selected Monthly from the Schedule list, then select a day from the Day of the month list.
10. Click Save.

Operational windows can be associated with scan profiles by using the When To Scan tab on the Scan Profile Configuration page.

If you assign two operational windows to a scan profile, the scan profile runs at the time intersection of the operational windows. For example, if you configure two daily operational windows for the periods 1 a.m. to 6 a.m. and 5 a.m. to 9 a.m., the scan runs only between 5 a.m. and 6 a.m. If the operational windows are not configured with an overlapping time schedule, then the scans do not run.

Scanning during permitted times

In Extreme Networks Security Vulnerability Manager, you can schedule a scan of your network assets at permitted times, by using an operational window.

1. Click the Vulnerabilities tab.
2. In the navigation pane, select Administrative > Operational Window.
3. On the toolbar, select Actions > Add.
4. Type a name for your operational window, then configure a permitted time interval and click Save.
5. In the navigation pane, select Administrative > Scan Profiles.
6. On the toolbar, click Add.

   When you create a scan profile, the only mandatory fields are Name and IP Addresses on the Details tab of the Scan Profile Configuration page. To configure scanning during permitted times, you must also follow the remaining steps in this procedure.
7. Click the When To Scan tab.
8. In the Run Schedule list, select Daily.
9. In the Start Time fields, type or select the date and time that you want your scan to run each day.
10. In the Operational Windows pane, select your operational window from the list and click (>).
11. Click Save.

Managing operational windows

In Extreme Networks Security Vulnerability Manager, you can edit, delete, and print operational windows.

Remember
You can edit an operational window while it is associated with a scan profile.

1. Click the Vulnerabilities tab.
2. In the navigation pane, select Administrative > Operational Window.
3. Select the operational window that you want to edit.
4. On the toolbar, select an option from the Actions menu.
5. Follow the instructions in the user interface.

Note
You cannot delete an operational window that is associated with a scan profile. You must first disconnect the operational window from the scan profile.

Disconnecting an operational window

If you want to delete an operational window that is associated with a scan profile, you must disconnect the operational window from the scan profile.

1. Click the Vulnerabilities tab.
2. In the navigation pane, select Administrative > Scan Profiles.
3. Select the scan profile that you want to edit.

4 On the toolbar, click **Edit**.
5 Click the **When To Scan** pane.
6 Select the relevant option from the **Run Schedule** list as required.
7 In the **Name** field, select the operational window that you want to disconnect and click (**<**).
8 Click **Save**.

Dynamic vulnerability scans

In Extreme Networks Security Vulnerability Manager, you can configure a scan to use certain vulnerability scanners for specific CIDR ranges in your network. For example, your scanners might have access only to certain areas of your network.

During a scan, Vulnerability Manager determines which scanner to use for each CIDR, IP address, or IP range that you specify in your scan profile.

Dynamic scanning and domains

If you configured domains in the **Domain Management** window on the **Admin** tab, you can associate scanners with the domains that you added.

For example, you might associate different scanners each with a different domain, or with different CIDR ranges within the same domain. Extreme Security dynamically scans the configured CIDR ranges that contain the IP addresses you specify on all domains that are associated with the scanners on your system. Assets with the same IP address on different domains are scanned individually if the CIDR range for each domain includes that IP address. If an IP address is not within a configured CIDR range for a scanner domain, Extreme Security scans the domain that is configured for the Controller scanner for the asset.

Setting up dynamic scanning

To use *dynamic scanning*, you must do the following actions:

1 Add vulnerability scanners to your Vulnerability Manager deployment. For more information, see Options for adding scanners to your Vulnerability Manager deployment on page 14.
2 Associate vulnerability scanners with CIDR ranges and domains.
3 Configure a scan of multiple CIDR ranges and enable **Dynamic server selection** in the **Details** tab of the **Scan Profile Configuration** page.

Related Links

Dynamic scanning on page 22
In dynamic scanning, Extreme Networks Security Vulnerability Manager selects a scanner based on the IP address to scan.

Options for adding scanners to your Vulnerability Manager deployment on page 14
Scan profile details on page 33
Scan profile details on page 33

Associating vulnerability scanners with CIDR ranges

In Extreme Networks Security Vulnerability Manager, to do dynamic scanning, you must associate vulnerability scanners with different segments of your network.

You must add extra vulnerability scanners to your deployment. For more information, see Options for adding scanners to your Vulnerability Manager deployment on page 14.

1 Click the **Vulnerabilities** tab.
2 In the navigation pane, select **Administrative** > **Scanners**.

Caution
By default, the Controller scanner is displayed. The Controller scanner is part of the Vulnerability Manager processor that is deployed on either your Extreme Security Console or on a dedicated Vulnerability Manager processing appliance. You can assign a CIDR range to the Controller scanner, but you must deploy extra scanners to use dynamic scanning.

3 Click a scanner on the **Scanners** page.
4 On the toolbar, click **Edit**.

Note
You cannot edit the name of the scanner. To edit a scanner name, click **Admin** > **System and License Management** > **Deployment Actions** > **Manage Vulnerability Deployment**.

5 In the **CIDR** field, type a CIDR range or multiple CIDR ranges that are separated by commas.
6 Click **Save**.

Related Links

Options for adding scanners to your Vulnerability Manager deployment on page 14

Scanning CIDR ranges with different vulnerability scanners

In Extreme Networks Security Vulnerability Manager, you can scan areas of your network with different vulnerability scanners.

You must configure your network CIDR ranges to use the different vulnerability scanners in your Vulnerability Manager deployment. For more information, see Options for adding scanners to your Vulnerability Manager deployment on page 14.

1 Click the **Vulnerabilities** tab.
2 In the navigation pane, select **Administrative** > **Scan Profiles**.
3 On the toolbar, click **Add**.
4 Click the **Dynamic server selection** check box.

   If you configured domains in the **Admin** > **Domain Management** window, you can select a domain from the **Domain** list. Only assets within the domain you selected are scanned.
5 Add more CIDR ranges.
6 Click **Save**.
7 Click the check box on the row that is assigned to your scan on the **Scan Profiles** page and click **Run**.

Scan policies

A scan policy provides you with a central location to configure specific scanning requirements.

You can use scan policies to specify scan types, ports to be scanned, vulnerabilities to scan for and scanning tools to use. In Extreme Networks Security Vulnerability Manager, a *scan policy* is associated with a scan profile and is used to control a vulnerability scan. You use the Scan Policies list on the Details tab of the Scan Profile Configuration page to associate a scan policy with a scan profile.

You can create a new scan policy or copy and modify a pre-configured policy that is distributed with Vulnerability Manager.

Pre-configured scan policies

The following pre-configured scan policies are distributed with Vulnerability Manager:

- Full scan
- Discovery scan
- Database scan
- Patch scan
- PCI scan
- Web scan

A description of each pre-configured scan policy is displayed on the Scan Policies page.

Related Links

Modifying a pre-configured scan policy on page 54

In Extreme Networks Security Vulnerability Manager, you can copy a pre-configured scan policy and modify the policy to your exact scanning requirements.

Configuring a scan policy to manage your vulnerability scans on page 55

In Extreme Networks Security Vulnerability Manager, you can configure a scan policy to control your vulnerability scans.

Modifying a pre-configured scan policy

In Extreme Networks Security Vulnerability Manager, you can copy a pre-configured scan policy and modify the policy to your exact scanning requirements.

1. Click the Vulnerabilities tab.
2. In the navigation pane, select Administrative > Scan Policies.
3. On the Scan Policies page, click a pre-configured scan policy.
4. On the toolbar, click Edit.
5. Click Copy.
6. In the Copy scan policy window, type a new name in the Name field and click OK.
7. Click the copy of your scan policy and on the toolbar, click Edit.

8 In the **Description** field, type new information about the scan policy.

> Important
> If you modify the new scan policy, you must update the information in the description.

9 To modify your scan policy, use the **Port Scan**, **Vulnerabilities**, **Tool Groups**, or **Tools** tabs.

> Note
> Depending on the **Scan Type** that you select, you cannot use all the tabs on the **Scan Policy** window.

Configuring a scan policy to manage your vulnerability scans

In Extreme Networks Security Vulnerability Manager, you can configure a scan policy to control your vulnerability scans.

1 Click the **Vulnerabilities** tab.

2 In the navigation pane, select **Administrative** > **Scan Policies**.

3 On the toolbar, click **Add**.

4 Type the name and description of your scan policy.

To configure a scan policy, the only mandatory fields in the **New Scan Policy** window are the **Name** and **Description** fields.

5 From the **Scan Type** list, select the scan type to base your scan policy on.

6 To include specific vulnerabilities in your scan policy, do the following steps:

a In the **New Scan Policy** window, click the **Patch** check box.

b Click the **Vulnerabilities** tab.

c Click **Add**.

By default, all vulnerabilities discovered in the last year are displayed.

d Filter the list of vulnerabilities.

e Click the vulnerabilities that you want to include in your scan policy and click **Submit** on the toolbar.

7 To include or exclude tool groups from a zero-credentialed or full scan policy, click the **Tool Group** tab.

8 To include or exclude tools from a zero-credentialed or full scan policy, click the **Tools** tab.

> Important
> If you do not modify the tools or tool groups, and you selected the **Full** option as your scan type, then all the tools and tool groups that are associated with a full scan are included in your scan policy.

9 Click **Save**.

6 Vulnerability scan investigations

In Extreme Networks Security Vulnerability Manager, you can investigate summary asset and vulnerability data for each scan.

To investigate vulnerability scans, do the following tasks:

- Build and save complex vulnerability search criteria.
- Investigate exploitation risk levels at a network, asset, and vulnerability level.
- Prioritize your vulnerability remediation processes.

Scan results

You can use the Scan Results page to investigate the following information:

- The progress of a scan and the scanning tools that are queued and running.
- The status of a scan. For example, a scan with a status of Stopped indicates that the scan completed successfully or was canceled.
- The degree of risk that is associated with each completed scan profile. Risk is indicated by the Score column and shows the total Common Vulnerability Scoring System (CVSS) score for the completed scan profile.
- The total number of assets that were found by the scan.
- The total number of vulnerabilities that were discovered by the completed scan profile.
- The total number of open services that were discovered by the completed scan profile.

Vulnerability counts

The Scan Results page shows Vulnerabilities and Vulnerabilities Instances.

- The Vulnerabilities column shows the total number of unique vulnerabilities that were discovered on all the scanned assets.
- When you scan multiple assets, the same vulnerability might be present on different assets. Therefore, the Vulnerability Instances column shows the total number of vulnerabilities that were discovered on all the scanned assets.

Searching scan results

In Extreme Networks Security Vulnerability Manager, you can search and filter your scan results.

For example, you might want to identify recent scans, scans on a specific IP address, or scans that identified a specific vulnerability.

Use the **Name** field on the **Vulnerabilities** tab to search results by scan profile name. To use more advanced criteria in your search, do the following:

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Scan Results**.
3. On the toolbar, select **Search** > **New Search**.
   To search your scan results, there are no mandatory fields. All parameters are optional.
4. To show scan results for scans that completed within a recent number of days, type a value in the **Scan Run in the last days** field.
5. To show scan results for a specific vulnerability, click **Browse** in the **Contains Vulnerability** field.
6. To show scan results for scans that were only scheduled, click **Exclude on demand scan**.
7. Click **Search**.

Related Links

Scan scheduling on page 34

Including column headings in asset searches

Limit asset searches with filters that include custom asset profiles, name, vulnerability count, and risk score.

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**, then on the toolbar click **Search** > **New Search**.
3. In the field containing column names, in the field on the left, click the column headings you want to include in your search, and click the arrow button to move the selected headings to field on the right.
4. Click the up and down buttons to change the priority of the selected column headings.
5. When the field on the right contains all the column heading that you want to search on, click **Search**.

Managing scan results

In Extreme Networks Security Vulnerability Manager, on the **Scan Results** page, you can manage your scan results and manage the scans that are running.

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Scan Results**.
3. If you want to rerun completed scans, select the check box in the rows assigned to the scans and click **Run**.
   A completed scan has a status of **Stopped**.
4. To delete completed scan results:
   a. On the **Scan Results** page, select the check box in the rows assigned to the scans results you want to delete.

b. On the toolbar, click **Delete**.

If you delete a set of scan results, no warning is displayed. The scan results are immediately deleted.

> Remember
> When you delete a set of scan results, neither the scan data in the Extreme Security asset model or the scan profile are deleted.

5. To cancel a scan that is running:

   a. On the **Scan Results** page, select the check box in the rows assigned to the scans you want to cancel.

   b. On the toolbar, click **Cancel**.

   You can cancel a scan that has a status of **Running** or **Paused**.

   After you cancel a scan, the status of the scan is **Stopped**.

Asset risk levels and vulnerability categories

In Extreme Networks Security Vulnerability Manager, you can investigate the exploitation risk level of your scanned assets on the **Scan Results Assets** page.

The **Scan Results Assets** page provides a risk and vulnerability summary for each of the assets that you scanned by running a scan profile.

Risk score

Each vulnerability that is detected on your network has a risk score that is calculated by using the Common Vulnerability Scoring System (CVSS) base score. A high risk score provides an indication of the potential for a vulnerability exploitation.

On the **Scan Results Assets** page the **Score** column is an accumulation of the risk score for each vulnerability on an asset. The accumulated value provides an indication of the level of risk that is associated with each asset.

To quickly identify the assets that are most at risk to vulnerability exploitation, click the **Score** column heading to sort your assets by the risk level.

Vulnerability counts and categories

The **Scan Results Assets** page shows the total number of vulnerabilities and open services that were discovered on every scanned asset.

To identify the assets with the highest number of vulnerabilities, click the **Vulnerability Instances** column heading to order your assets.

The **High**, **Medium**, **Low**, and **Warning** columns group all vulnerabilities according to their risk.

The **Policy Check Passed %** and **Policy Check Failed %** columns display the percentage of policy checks that the asset passed or failed in the benchmark scan. Click the values in these columns to see more information on policy checks that passed or failed on the **Scan Results Policy Checks** page.

Asset, vulnerability, and open services data

In Extreme Networks Security Vulnerability Manager, the Scan Results Asset Details page shows asset, vulnerability, and open services data.

By using the options on the toolbar, you can switch between viewing vulnerabilities and open services.

The Scan Results Asset Details page provides the following information:

- Summary information about the asset that you scanned, including the operating system and network group.
- A list of the vulnerabilities or open services that were discovered on the scanned asset.
- Various ways of categorizing and ordering your list of vulnerabilities or open services for example, Risk, Severity, and Score.
- A quick way to view open service or vulnerability information. On the toolbar, click Vulnerabilities or Open Services.
- An easy way to view detailed information about the asset that you scanned. On the toolbar, click the Asset Details.
- An alternative method of creating a vulnerability exception. On the toolbar, click Actions > Exception.

The caution icon indicates that the scan failed. Hover over the icon for additional details.

For more information about the Asset Details window, see the *Users Guide* for your product.

Related Links

Vulnerability exception rules on page 75

In Extreme Networks Security Vulnerability Manager, you can configure exception rules to minimize the number of false positive vulnerabilities.

Viewing the status of asset patch downloads

View whether an asset has a pending patch download. If there are no pending downloads, the asset has all available patches.

1. Search for the asset that you want to confirm the patch status for.
2. Click the Asset IP address to open the Asset Details window.
3. Click Details > Properties to open the Asset Properties window.
4. Click the Windows Patches arrow.
5. View the patch status in the Pending column.
   - True - the asset has pending patches to download.
   - False - the asset has no pending patch downloads.

Vulnerability risk and PCI severity

In Extreme Networks Security Vulnerability Manager, you can review the risk and payment card industry (PCI) severity for each vulnerability that is found by a scan.

You can review the following information:

- The risk level that is associated with each vulnerability.
- The number of assets in your network on which the specific vulnerability was found.

To investigate a vulnerability, you can click a vulnerability link in the Vulnerability column.

Emailing asset owners when vulnerability scans start and stop

Email the configured asset technical owners to alert them of the scan schedule. You can also email reports to asset owners.

Configure the system mail server and technical owners for assets. For more information, see the .

1. Click the Vulnerabilities tab.
2. Click Administrative > Scan Profiles.
3. On the row assigned to the scan you want to edit, select the check box and click Edit on the toolbar.
4. In the What To Email area of the Email tab, select the appropriate check boxes.
5. If you selected the Reports check box, in the Available Reports field, select the reports that you want to email and click the arrow to move reports into the Selected Reports field.

   Reports can be large. Confirm that the sent reports are not rejected by the recipient's email provider.
6. In the Who to Email area, select the recipients that you want to receive the emails:
   - To email the configured technical owners of the scanned assets, select the Technical Owners check box. Technical owners receive emails about their assets only.
   - To enter or select email addresses in the field, select the To Addresses check box. Select emails and click Add Me to email the selected email recipients. Entered email addresses receive emails and reports regarding all scanned assets.
7. Click Save.

7 Management of your vulnerabilities

In Extreme Networks Security Vulnerability Manager, you can manage, search, and filter your vulnerability data to help you focus on the vulnerabilities that pose the greatest risk to your organization.

The vulnerability data that is displayed is based on the vulnerability status information that is maintained in the Extreme Security asset model. This information includes vulnerabilities that are found by the Extreme Security Vulnerability Manager scanner and the vulnerabilities that are imported from external scanning products.

Manage your vulnerabilities to provide the following information:

- A network view of your current vulnerability posture.
- Identify vulnerabilities that pose the greatest risk to your organization and assign vulnerabilities to Extreme Security users for remediation.
- Establish how widely your network is impacted by vulnerabilities and display detailed information about the network assets that contain vulnerabilities.
- Decide which vulnerabilities pose less risk to your organization and create vulnerability exceptions.
- Display historical information about the vulnerabilities on your network.
- Display vulnerability data by network, asset, vulnerability, open service, or vulnerability instance.

Investigating vulnerability risk scores

In Extreme Networks Security Vulnerability Manager, you can investigate vulnerability risk scores and understand how each score is calculated.

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. Click the **Risk Score** column to sort your vulnerabilities by risk.
4. To investigate the risk score, hover you mouse on a vulnerability risk score.

Risk score details

In Extreme Networks Security Vulnerability Manager, vulnerability risk scores provide an indication of the risk that a vulnerability poses to your organization.

Using Extreme Networks Security Risk Manager, you can configure policies that adjust vulnerability risk scores and draw attention to important remediation tasks.

Risk Score

The **Risk Score** provides specific network context by using the Common Vulnerability Scoring System (CVSS) base, temporal, and environmental metrics.

When Risk Manager is not licensed the **Risk Score** column shows the CVSS environmental metric score with a maximum value of 10.

Exploitability subscore

Exploitability is calculated as a subset of the CVSS base score by using the following elements:

- Access Vector provides an indication of risk that is based on the remoteness for example, local, adjacent network, or network, of an attacker.
- Access Complexity provides an indication of risk that is based on attack complexity. The lower the complexity the higher the risk.
- Authentication provides an indication of risk that is based on authentication attempts. The fewer the attempts the higher the risk.

Risk adjustments

If Extreme Networks Security Risk Manager is installed and you configured vulnerability risk policies, then the risk adjustments are listed. The adjustments either increase or decrease the overall risk that is associated with a vulnerability.

Related Links

Extreme Networks Security Risk Manager and Extreme Networks Security Vulnerability Manager integration on page 25

Prioritizing high risk vulnerabilities by applying risk policies on page 70

Prioritizing high risk vulnerabilities by applying risk policies on page 70

Searching vulnerability data

In Extreme Networks Security Vulnerability Manager, you can identify important vulnerabilities by searching your vulnerability data.

Vulnerability Manager provides various methods to search your data. You can search by network, by asset, by open service, or by vulnerability.

Default saved searches provide a fast method of identifying the risk to your organization. Saved searches are displayed in the Available Saved Searches field on the Vulnerability Manager Search page.

You must create a scan profile and scan your network assets.

1 Click the Vulnerabilities tab.
2 In the navigation pane, click Manage Vulnerabilities.
3 On the toolbar, select Search > New Search.
4 If you want to load a saved search, do the following steps:
   a Select a group from the Group list.
   b In the Type Saved Search field, type the saved search that you want to load.
   c From the Available Saved Searches list, select a saved search, and then click Load.
   d Click Search.
5 If you want to create a new search, do the following steps in the Search Parameters pane:
   a In the first list, select the parameter that you want to use.
   b In the second list, select a search modifier. The modifiers that are available depend on the search parameter that you select.
   c In the third list, type or select the specific information that is related to your search parameter.
   d Click Add Filter.

   For example, to email the vulnerabilities that are assigned to a technical user, select Technical Owner Contact and provide an email address that is configured on the Vulnerability Assignment page.
6 Click Search.
7 On the toolbar, click Save Search Criteria.

> Important
> Vulnerability reports use saved search information. If you want to create a report that emails a technical user, you must save your search criteria.

Related Links

Vulnerability search parameters on page 64

In Extreme Networks Security Vulnerability Manager, you can search your vulnerability data and save the searches for later use.

Vulnerability quick searches

Search vulnerabilities by typing a text search string that uses simple words or phrases.

In Extreme Networks Security Vulnerability Manager, you can use quick searches to filter vulnerabilities on the My Assigned Vulnerabilities and Manage Vulnerabilities pages.

Use the Quick Searches list to do a pre-configured vulnerability search.

Use the Quick Filter field to create your own vulnerability filters. Click Save Search Criteria to add your vulnerability quick filters to the Quick Searches list.

Table 5: Vulnerability quick filter syntax guidelines

Description	Example

Include any plain text that you expect to find in vulnerability title, description, solution, concern, reference ID type, or reference ID value.	`2012-3764`
	`MS203`
	`java`

To search only the text in the vulnerability title, add ***:A*** to the search text string	`PHP:A`
To search only the text in the vulnerability description, add ***:B*** to the search text string	`cross-site scripting:B`
To search only the text in the vulnerability external reference type, add ***:C*** to the search text string	`RedHat RHSA:C`
Include wildcard characters. The search term cannot start with a wildcard.	`SSLv*`

Group terms with logical operators: ***AND***, ***OR***, and ***NOT*** (or ***!***). To be recognized as logical operators and not as search terms, the operators must be uppercase.	`PHP AND Traversal`
	`XSS:A OR cross-site scripting:A`
	`!MySQL`
	`NOT MySQL`

Related Links

Saving your vulnerability search criteria on page 66

Vulnerability search parameters

In Extreme Networks Security Vulnerability Manager, you can search your vulnerability data and save the searches for later use.

The following table is not a complete list of vulnerability search parameters, but a subset of the available options.

Select any of the parameters to search and display vulnerability data.

Table 6: Vulnerability search parameters

Option	Description
Access Complexity	The complexity of the attack that is required to exploit a vulnerability.
Access Vector	The network location from where a vulnerability can be exploited.
Asset saved search	The host, IP address, or range of IP addresses associated with a saved asset search. For more information about saving asset searches, see the *Users Guide* for your product.
Assets with Open Service	Assets that have specific open services. For example, HTTP, FTP, and SMTP.

Table 6: Vulnerability search parameters (continued)

Option	Description
Authentication	The number of times an attacker must authenticate against a target to exploit a vulnerability.
Availability Impact	The level that resource availability can be compromised if a vulnerability is exploited.
Confidentiality Impact	The level of confidential information that can be obtained if a vulnerability is exploited.
Days since asset found	The elapsed number of days since the asset with the vulnerability was discovered on your network. Assets can be discovered either by an active scan or passively by using log or flow analysis.
Days since associated vulnerability service traffic	Displays vulnerabilities on assets with associated layer 7 traffic to or from an asset, based on the elapsed number of days since the traffic was detected.
Domain	If you configured Extreme Networks Security Analytics for multi-domain systems, use this option to specify the domain you want to search for vulnerabilities.
By Open Service	Use this parameter to search for vulnerabilities that are associated with particular open services such as, HTTP, FTP, and SMTP.
External Reference of type	Vulnerabilities that have an associated Endpoint Manager fixlet. By using this parameter, you can show only those vulnerabilities without an available patch.
Impact	The potential impact to your organization. For example, access control loss, downtime, and reputation loss.
Include early warnings	Newly published vulnerabilities that are detected on your network without extra scanning.
Include vulnerability exceptions	Those vulnerabilities with an exception rule applied.
Integrity Impact	The level to which system integrity might be compromised if a vulnerability is exploited.
Only include assets with risk	Vulnerabilities that pass or fail specific risk policies that are defined and monitored in Extreme Networks Security Risk Manager. Note You must monitor at least one question in the **Policy Monitor** page on the **Risks** tab to use this search parameter.
Only include assets with risk passed	Vulnerabilities that pass specific risk policies that are defined and monitored in Risk Manager.
Only include early warnings	Use this parameter to include only newly published vulnerabilities that are detected on your network without extra scanning in your search.
Only include Vulnerability Exceptions	Use this parameter to include only vulnerabilities with an exception rule applied in your search.
Overdue by Days	Use this parameter to look for vulnerabilities that are overdue for remediation by a specified number of days.
Patch Status	Use this parameter to filter vulnerabilities by patch status. For more information, see Identifying the patch status of your vulnerabilities on page 72.
PCI Severity	Use this parameter to search for vulnerabilities by the PCI Severity level (High, Medium, or Low) assigned by the PCI compliance service. Vulnerabilities assigned a High or Medium PCI Severity level fail PCI compliance.

Table 6: Vulnerability search parameters (continued)

Option	Description
Quick Search	You can search for a vulnerabilities title, description, solution, and external reference ID. In the Quick Search field, you can use AND, OR, and NOT operators, and brackets.
Risk	Use this parameter to search for vulnerabilities by risk level (High, Medium, Low, Warning).
Unassigned	Use this parameter to search for vulnerabilities with no assigned user to remediate them.
Vulnerability External Reference	Vulnerabilities that are based on an imported list of vulnerability IDs, for example CVE ID. For more information about Reference Sets, see the *Administration Guide* for your product.
Vulnerability has a virtual patch from vendor	Vulnerabilities that can be patched by an intrusion prevention system.
Vulnerability state	The status of the vulnerability since the last scan of your network or specific network assets. For example, when you scan assets, the vulnerabilities that are discovered are either New, Pre-existing, Fixed, or Existing.
Vulnerability with risk	Use this parameter to filter vulnerabilities by risk policy results. You must monitor at least one question in the Policy Monitor page on the Risks tab to use this search parameter.

Saving your vulnerability search criteria

In Extreme Networks Security Vulnerability Manager, you can save your vulnerability search criteria for future use.

1. Click the Vulnerabilities tab.
2. In the navigation pane, click Manage Vulnerabilities.
3. On the toolbar, select Search > New Search and complete the search of your data.
4. On the toolbar, click Save Search Criteria.
5. In the Save Search Criteria window, type a recognizable name for your saved search.
6. To include your saved search in the Quick Searches list on the toolbar, then click Include in my Quick Searches.
7. To share your saved search criteria with all Extreme Security users, then click Share with Everyone.
8. To place your saved search is a group, then click a group or click Manage Groups to create a new group.

   For more information about managing search groups, see the *Administration Guide* for your product.
9. If you want to show the results of your saved search when you click any of the Manage Vulnerabilities pages in the navigation pane, then click Set As Default.
10. Click OK.

Deleting saved vulnerability search criteria

In Extreme Networks Security Vulnerability Manager, you can delete your saved vulnerability search criteria.

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities** > **By Network**
3. On the toolbar, select **Search** > **New Search**.
4. On the **Vulnerability Manager Search** page, in the **Available Saved Searches** list, select the saved search that you want to delete.
5. Click **Delete**.
6. Click **OK**.

Vulnerability instances

In Extreme Networks Security Vulnerability Manager, you can display the vulnerabilities on each of the scanned assets in your network. Each vulnerability might be listed multiple times because the vulnerability exists on several of your assets.

If you configure third-party vulnerability assessment (VA) scanners, by using the Extreme Security **Admin** tab, then the vulnerabilities that are detected are automatically displayed in the **By Vulnerability Instances** page.

For more information about VA scanners, see the *Administration Guide* for your product.

The **By Vulnerability Instances** page provides the following information:

- A view of every vulnerability that was detected by scanning your network assets.
- The risk that each vulnerability poses to the Payment Card Industry (PCI).
- The risk that a vulnerability poses to your organization. Click the **Risk Score** column to identify the highest risk vulnerabilities.
- The name or email address of the user that is assigned to remediate the vulnerability.
- The numbers of days in which a vulnerability must be remediated.

Related Links

Risk score details on page 62

Network vulnerabilities

In Extreme Networks Security Vulnerability Manager, you can review vulnerability data that is grouped by network.

The **By Network** page provides the following information:

- An accumulated risk score that is based on the vulnerabilities that are detected on each of your networks.
- The number of the assets, vulnerabilities, and open services for each network.
- The number of vulnerabilities that are assigned to a technical user and are overdue for remediation.

Asset vulnerabilities

In Extreme Networks Security Vulnerability Manager, you can display summary vulnerability data that is grouped by each scanned asset.

You can use the By Asset page to prioritize the remediation tasks for assets in your organization that pose the greatest risk.

The By Asset page provides the following information:

- An accumulated risk score that is based on the vulnerabilities that are detected on each of your assets.

  Click the Risk Score column to sort your assets by their risk.
- The number of asset vulnerabilities that are assigned to a technical user and are overdue for remediation.

Open service vulnerabilities

In Extreme Networks Security Vulnerability Manager, you can display vulnerability data that is grouped by open service.

The By Open Service page shows an accumulated risk score and vulnerability count for each service in your entire network.

Investigating the history of a vulnerability

In Extreme Networks Security Vulnerability Manager, you can display useful information about the history of a vulnerability.

For example, you can investigate information about how the risk score of a vulnerability was calculated. You can also review information about when a vulnerability was first discovered and the scan that was used to discover the vulnerability.

1. Click the Vulnerabilities tab.
2. In the navigation pane, click Manage Vulnerabilities.
3. Search your vulnerability data.
4. Click the vulnerability that you want to investigate.
5. On the toolbar, select Actions > History.

Related Links

Searching vulnerability data on page 63

Reducing the number of false positive vulnerabilities

In Extreme Networks Security Vulnerability Manager, you can automatically create exception rules for vulnerabilities that are associated with a specific type of server.

When you configure server types, Extreme Security Vulnerability Manager creates exception rules and automatically reduces the vulnerabilities that are returned by searching your data.

1. Click the Assets tab.
2. In the navigation pane, select Server Discovery.

3 To automatically create false positive exception rules for vulnerabilities on specific server types, from the **Server Type** list, select one of the following options:

   - FTP Servers
   - DNS Servers
   - Mail Servers
   - Web Servers

   It might take a few minutes for the **Ports** field to refresh.

4 From the **Network** list, select the network for your servers.

5 Click **Discover Servers**.

6 In the **Matching Servers** pane, select the servers where the vulnerability exception rules are created.

7 Click **Approve Selected Servers**.

Depending on your server type selection the following vulnerabilities are automatically set as false positive exception rules:

Table 7: Server type vulnerabilities

Server Type	Vulnerability
FTP Servers	FTP Server Present
DNS Servers	DNS Server is Running
Mail Servers	SMTP Server Detected
Web Servers	Web Service is Running

Investigating high risk assets and vulnerabilities

In Extreme Networks Security Vulnerability Manager, you can investigate high risk vulnerabilities that might be susceptible to exploitation.

1 Click the **Vulnerabilities** tab.

2 In the navigation pane, click **Manage Vulnerabilities**.

3 On the **By Vulnerability Instances** page, click the **Risk Score** column heading to sort the vulnerabilities by risk score.

4 To investigate the CVSS metrics that are used to derive the risk score, hover your mouse on the **Risk Score** field.

5 Identify the vulnerability that has the highest score and click the **Vulnerability** link.

6 In the **Vulnerability Details** window, investigate the vulnerability:

   a To view the Extreme Networks® Security Systems website, click the **X-Force** link.

   b To view the National Vulnerability Database website, click the **CVE** link.

   The Extreme Networks® Security Systems website and National Vulnerability Database provide remediation information and details on how a vulnerability might affect your organization.

c. To open the Patching window for the vulnerability, click the Plugin Details link. Use the tabs to discover Oval Definition, Windows™ Knowledge Base, or UNIX™ advisory information about the vulnerability. This feature provides information on how Extreme Security Vulnerability Manager checks for vulnerability details during a patch scan. You can use it to identify why a vulnerability was raised on an asset or why it was not.

d. The Solution text box contains detailed information about how to remediate a vulnerability.

Related Links

Risk score details on page 62

Prioritizing high risk vulnerabilities by applying risk policies

In Extreme Networks Security Vulnerability Manager, you can alert administrators to higher risk vulnerabilities by applying risk policies to your vulnerabilities.

When you apply a risk policy, the risk score of a vulnerability is adjusted, allowing administrators to prioritize more accurately the vulnerabilities that require immediate attention.

In this example, the vulnerability risk score is automatically increased by a percentage factor for any vulnerability that remains active on your network after 40 days.

1. Click the Vulnerabilities tab.
2. In the navigation pane, click Manage Vulnerabilities.
3. On the toolbar click Search > New Search.
4. In the Search Parameters pane, configure the following filters:
   a. Risk Equals High
   b. Days since vulnerabilities discovered Greater than or equal to 40
5. Click Search and then on the toolbar click Save Search Criteria.

   Type a saved search name that is identifiable in Risk Manager.
6. Click the Risks tab.
7. In the navigation pane, click Policy Monitor.
8. On the toolbar click Actions > New.
9. In the What do you want to name this question field, type a name.
10. In the Which tests do you want to include in your question field, click are susceptible to vulnerabilities contained in vulnerability saved searches.
11. In the Find Assets that field, click the underlined parameter on the are susceptible to vulnerabilities contained in vulnerability saved searches.
12. Identify your Vulnerability Manager high risk vulnerability saved search, click Add, then click OK.
13. Click Save Question.
14. In the Questions pane, select your question from the list and on the toolbar click Monitor.

    Note
    The Event Description field is mandatory.
15. Click Dispatch question passed events.
16. In the Vulnerability Score Adjustments field, type a risk adjustment percentage value in the Percentage vulnerability score adjustment on question fail field.

17 Click **Apply adjustment to all vulnerabilities on an asset** then click **Save Monitor**.

On the **Vulnerabilities** tab, you can search your high risk vulnerabilities and prioritize your vulnerabilities

Related Links

Saving your vulnerability search criteria on page 66

Extreme Networks Security Risk Manager and Extreme Networks Security Vulnerability Manager integration on page 25

Configuring custom display colors for risk scores

Configure custom color coding for Extreme Networks Security Vulnerability Manager risk scores to view color-coded risk scores in Extreme Security Vulnerability Manager interfaces.

1 In Extreme Networks Security Analytics, select **Vulnerabilities** > **Vulnerability Assignment** > **Risk Preferences**.

2 In the **Greater than or equal to** column, enter the minimum risk score value for High, Medium, Low, and Warning.

3 In the **Color** column, select or define a color to represent High, Medium, Low, and Warning risk scores.

Identifying vulnerabilities with an IBM® Security Endpoint Manager patch

In Extreme Networks Security Vulnerability Manager, you can identify the vulnerabilities that have an available fix.

After you identify your vulnerabilities that have an available fix, you can investigate detailed fix information in the **Vulnerability Details** window.

1 Click the **Vulnerabilities** tab.

2 In the navigation pane, click **Manage Vulnerabilities**.

3 On the toolbar, select **Search** > **New Search**

4 In the **Search Parameters** pane configure the following options:

   a In the **first list** select **External Reference of type**.

   b In the **second list** select **Equals**.

   c In the **third list** select **IBM Endpoint Manager Patch**.

   d Click **Add Filter**.

   e Click **Search**.

   The **By Vulnerability Instances** page shows the vulnerabilities that have an available fix.

5 Order your vulnerabilities according to their importance by clicking the **Risk Score** column heading.

6 To investigate patch information for a vulnerability, click a vulnerability link in the **Vulnerability** column.

7 In the **Vulnerability Details** window, scroll to the bottom of the window to view the vulnerability patch information.

   The **Site ID** and **Fixlet ID** are unique identifiers that you use to apply vulnerability patches by using IBM® Security Endpoint Manager.

   The **Base** column indicates a unique reference that you can use to access more information on a knowledge base.

Identifying the patch status of your vulnerabilities

In Extreme Networks Security Vulnerability Manager, you can identify the patch status of your vulnerabilities.

By filtering patched vulnerabilities, you can prioritize your remediation efforts on the most critical vulnerabilities in your organization.

1 Click the **Vulnerabilities** tab.
2 In the navigation pane, click **Manage Vulnerabilities**.
3 On the toolbar, select **Search** > **New Search**.
4 In the **first list** in the **Search Parameters** pane, select **Patch Status**.
5 In the **second list**, select a search modifier.
6 To filter your vulnerabilities according to their patch status, select one of the following options from the third list:

Option	Description
Pending Downloads	Select this option to show vulnerabilities that are scheduled to be patched
Pending Restart	Select this option to shows vulnerabilities that are patched after the scanned asset is restarted
Fixed	Select this option to show vulnerabilities that are patched by IBM® Security Endpoint Manager

7 Click **Add Filter**.
8 Click **Search**.

Related Links

IBM Security Endpoint Manager integration on page 26

Removing unwanted vulnerability data

Use Extreme Security Vulnerability Manager vulnerability cleansing functionality to remove stale vulnerability data from the asset model.

Any one of the following scenarios might leave you with unwanted vulnerability data:

- Change of scanner type
- Decommissioned assets

- Change of IP address
- Inaccurate or test scans

Important
After you remove vulnerability data for an asset or scanner type, it cannot be recovered.

To remove unwanted vulnerability data, you have two options:

- Use the Actions > Clean Vulnerabilities (All) option on the Assets page to remove all vulnerability data for a selected scanner type.
- Use the Actions > Clean Vulnerabilities (Asset) option on the Asset Details page to remove all vulnerability data for a particular asset with a selected scanner type.

Configuring vulnerability data retention periods

You can set the retention period for vulnerability trend data and scan results in the Asset Profiler Configuration window.

Use the configuration rules in the QVM Vulnerability Retention section of the Asset Profiler Configuration window to define how long Extreme Networks Security Vulnerability Manager retains vulnerability trend data and scan results.

1 Click Admin > Asset Profiler Configuration.

2 In the QVM Vulnerability Retention section of the Asset Profiler Configuration window, enter a value in the following fields:

Rule	Description	Default Value
Vulnerability Trend Reporting Data (In Days)	Sets how many days Extreme Security Vulnerability Manager retains vulnerability trend data for use in daily vulnerabilities reports.	14 days
Vulnerability Trend Reporting Data (In Weeks)	Sets how many weeks Extreme Security Vulnerability Manager retains vulnerability trend data for use in weekly vulnerabilities reports.	14 weeks
Vulnerability Trend Reporting Data (In Months)	Sets how many months Extreme Security Vulnerability Manager retains vulnerability trend data for use in monthly vulnerabilities reports.	14 months

Rule	Description	Default Value
Purge Scan Results After Period (In Days)	Use this rule with Purge Scan Results After Period (In Execution Cycles) to set the retention limits for scan results data. Sets the number of days that Extreme Security Vulnerability Manager retains data after it applies the Purge Scan Results After Period (In Execution Cycles) limiting rule.	30 days
Purge Scan Results After Period (In Execution Cycles)	Use this rule with Purge Scan Results After Period (In Days) to set the retention limits for scan results data. Sets how many versions of scan result data Extreme Security Vulnerability Manager retains. This rule has precedence over the value you set in Purge Scan Results After Period (In Days). For the default values for the Purge Scan Results After Period (In Days) and Purge Scan Results After Period (In Execution Cycles) rules: • Extreme Security Vulnerability Manager retains scan results data for the 3 most recent execution cycles. It also retains any other versions of results for scans that you run within the 30 days limit. • If any of the 3 most recent execution cycles occurred beyond the 30 days limit, Extreme Security Vulnerability Manager retains scan results data for those execution cycles.	3 execution cycles

3 Click Save.

8 Vulnerability exception rules

In Extreme Networks Security Vulnerability Manager, you can configure exception rules to minimize the number of false positive vulnerabilities.

When you apply exception rules to vulnerabilities, you reduce the number of vulnerabilities that are displayed in search results.

If you create a vulnerability exception, the vulnerability is not removed from Extreme Security Vulnerability Manager.

Viewing exception rules

To display vulnerability exceptions, you can search your vulnerability data by using search filters.

To view exception rules, click the Vulnerabilities tab, then click Vulnerability Exception in the navigation pane.

Related Links

Reducing the number of false positive vulnerabilities on page 68

Applying a vulnerability exception rule

In Extreme Networks Security Vulnerability Manager, you can manually apply a vulnerability exception rule to a vulnerability that you decide does not pose a significant threat.

If you apply an exception rule, the vulnerability is no longer displayed in Extreme Security Vulnerability Manager search results. However, the vulnerability is not removed from Vulnerability Manager.

1. Click the Vulnerabilities tab.
2. In the navigation pane, click Manage Vulnerabilities > By Network.
3. Search your vulnerability data. On the toolbar, click Search > New Search.
4. Click the Vulnerability Instances column link.
5. Select the vulnerability that you want to create an exception rule for.
6. On the toolbar, select Actions > Exception.

   To apply a vulnerability exception rule, the only mandatory field is the Comment text box. All other parameters are optional.

7 In the **Maintain Exception Rule** window, choose one of the following options:
   - Type a date when your vulnerability exception must expire.
   - If the vulnerability exception must never expire, click **Never Expires**.

8 In the **Notes** section of the **Maintain Exception Rule** window, type text in the **Comments** text box.

9 Click **Save**.

Related Links

Searching vulnerability data on page 63

Managing a vulnerability exception rule

If you receive new information about a vulnerability, you can update or remove an existing vulnerability exception rule.

1 Click the **Vulnerabilities** tab.

2 In the navigation pane, click **Vulnerability Exception**.

3 Click the vulnerability that you want to manage.

4 On the toolbar, select an option from the **Actions** menu.

Important

If you delete a vulnerability exception rule, no warning is displayed. The vulnerability is immediately deleted.

5 Click **Save**.

Searching vulnerability exceptions

In Extreme Networks Security Vulnerability Manager, you can search your vulnerability data and filter the search results to display vulnerability exceptions.

1 Click the **Vulnerabilities** tab.

2 In the navigation pane, select **Manage Vulnerabilities** > **By Asset**.

3 On the toolbar, select **Search** > **New Search**.

4 To filter your vulnerability data to include vulnerability exceptions, from the **Search Parameters** pane, select one of the following options:
   - Include vulnerability exceptions

     Displays all vulnerabilities, including vulnerabilities with an exception rule applied to them.
   - Only include vulnerability exceptions

     Displays vulnerabilities only with an exception rule applied to them.

5 Click **Add Filter**.

6 Click **Search**.

9 Vulnerability remediation

In Vulnerability Manager, you can assign vulnerabilities to a technical user for remediation.

You can assign vulnerabilities to your technical user by using two methods.

- Assign individual vulnerabilities to a technical user for remediation.
- Assign a technical user as the owner of asset groups

Related Links

Configuring remediation times for the vulnerabilities on assigned assets on page 79

Assigning individual vulnerabilities to a technical user for remediation

In Extreme Networks Security Vulnerability Manager, you can assign individual vulnerabilities to a Extreme Security user for remediation.

1. Click the Vulnerabilities tab.
2. In the navigation pane, select Manage Vulnerabilities.
3. Search your vulnerability data.
4. Select the vulnerability that you want to assign for remediation.
5. On the toolbar, click Actions > Assign/Edit.
6. Select a technical user from the Assigned User list.

   You assign technical users on the Vulnerability Assignment page. For more information, see Assigning a technical user as the owner of asset groups on page 77.
7. In the Due Date list, select a future date when the vulnerability must be remediated.

   If you do not select a date, the Due Data is set as the current date.
8. In the Notes field, type useful information about the reason for the vulnerability assignment.
9. Click Save.

Assigning a technical user as the owner of asset groups

In Extreme Networks Security Vulnerability Manager, you can configure groups of assets and automatically assign their vulnerabilities to technical users.

After you assign a technical user and scan the assets, all vulnerabilities on the assets are assigned to the technical user for remediation.

The remediation times for vulnerabilities can be configured, depending on their risk or severity. If you add new asset to your network, and it is contained in a technical user's asset group, vulnerabilities on the asset are automatically assigned to the technical user. You can automatically email reports to your technical users with the details of vulnerabilities that they are responsible for fixing.

If you want to configure a group of assets that are identified by a saved asset search, you must search your assets and save the results.

For more information about searching assets and saving the results, see the *User Guide* for your product.

1 Click the Vulnerabilities tab.
2 In the navigation pane, click Vulnerability Assignment.
3 On the toolbar, click Add.
4 Type a name, email address, and CIDR range.

   To automatically assign a technical user in the New Asset Owner window, the only mandatory fields are Name, Email, and CIDR.
5 If you configured Extreme Networks Security Analytics for multiple domains, select the relevant domain from the Domain list.
6 To filter the list of assets in your CIDR range by asset name, type a text string in the Asset Name Filter field.
7 To filter the list of assets in your CIDR range by operating system, type a text string in the OS Filter field.
8 Click Asset Search to assign the technical user to the assets associated with a saved asset search.
9 Click Save.
10 On the toolbar, click Remediation Times.

   You can configure the remediation time for each type of vulnerability, depending on their risk and severity.

   For example, you might need high risk vulnerabilities to be fixed within 5 days.
11 On the toolbar, click Schedule.

   By default, the technical user contact for your assets is updated every 24 hours.

   New assets added to your deployment and falling within the CIDR range that you specified are automatically updated with the technical contact that you specified.

   Important
   The schedule applies to the associations you made between technical users and groups of assets.
12 Click Update Now, to immediately set the owner of your assets.

   Depending on the size of your deployment, it might take an extended time to update your assets.
13 Click Save.

   Any vulnerabilities that are already assigned to a technical user for remediation are updated with the new technical user.

14 If vulnerabilities were not previously assigned to a technical user, you must scan the assets that you assigned to the technical user.

> Important
> Scanning the assets ensures that any vulnerabilities assigned to a technical user exist on the asset.

Configuring remediation times for the vulnerabilities on assigned assets

In Extreme Networks Security Vulnerability Manager you can configure the remediation times for different types of vulnerabilities.

1 Click the Vulnerabilities tab.

2 In the navigation pane, click Vulnerability Assignment.

3 Select an assignment from the Asset Owners list.

4 On the toolbar, click Remediation Times.

5 Update the remediation times for vulnerabilities that are based on their risk and severity.

6 Click Save.

10 Vulnerability reports

In Extreme Networks Security Vulnerability Manager, you can generate or edit an existing report, or use the report wizard to create, schedule, and distribute a new report.

Vulnerability Manager contains several default reports. The report wizard provides a step-by-step guide on how to design, schedule, and generate reports. For more information, see the *Extreme Networks SIEM Users Guide*

.

Emailing technical users with their assigned vulnerabilities that require remediation

When you assign vulnerabilities to a technical user for remediation, you can generate a report that emails the technical user.

The email contains information about the vulnerabilities that the technical user must remediate.

Generating PCI compliance reports

You can generate a compliance report for your PCI (payment card industry) assets.

The compliance report demonstrates that you took all the security precautions necessary to protect your critical assets.

Running a default Vulnerability Manager report

In Extreme Networks Security Vulnerability Manager, you can run a default vulnerability management report.

1 Click the Reports tab.
2 From the list of reports, click the report that you want to run.

   For example, you might want to show a report of your vulnerability overview for the last seven days.
3 On the toolbar, select Actions > Run Report, then click OK.
4 To view the completed report in a PDF format, click the icon in the Formats column.

Emailing assigned vulnerability reports to technical users

In Extreme Networks Security Vulnerability Manager, you can send an assigned vulnerabilities report to the technical contact for each asset.

An emailed report reminds your administrators that vulnerabilities are assigned to them and require remediation. Reports can be scheduled monthly, weekly, daily, or hourly.

You must complete the following tasks:

1. Assign a technical user as the owner of asset groups. For more information, see Assigning a technical user as the owner of asset groups on page 77
2. Scan the assets that you assigned the technical owner to.
3. Create and save a vulnerability search that uses the **Technical Owner Contact** parameter as an input. For more information, see Searching vulnerability data on page 63

1. Click the **Reports** tab.
2. On the toolbar, select **Actions** > **Create**.
3. Click **Weekly** and then click **Next**.
4. Click the undivided report layout that is displayed on the upper left section of the report wizard and click **Next**.
5. Type a **Report Title**.
6. In the **Chart Type** list, select **Asset Vulnerabilities** and type a **Chart Title**.
7. If a technical contact owner is responsible for more than five assets and you want to email all asset information, increase the value in the **Limit Assets To Top** list.

   > Remember
   > By using the **Assets** tab, you must ensure that the same technical contact owner is assigned to each asset that they are responsible for.

8. In the **Graph Type** field, select **AggregateTable**.

   If you select any value other than **AggregateTable**, the report does not generate a vulnerability sub-report.
9. In the **Graph Content** pane, click **Search to Use** and select your saved technical contact vulnerability search then click **Save Container Details**.
10. Click **Next** and select your report output type.
11. In the report distribution section of the report wizard, click **Multiple Reports**.
12. Click **All Asset Owners**.
13. Click **Load asset owners** to display all list of the technical users contact details.

    You can remove any technical users that you do not want to email with a list of assigned vulnerabilities.
14. On the Reports list, select the report that you created and on the toolbar, select **Actions** > **Run Report**.

Related Links

Assigning a technical user as the owner of asset groups on page 77

Searching vulnerability data on page 63

Generating PCI compliance reports

In Extreme Networks Security Vulnerability Manager, you can generate a compliance report for your PCI (payment card industry) assets. For example, generate a report for assets that store credit card or other sensitive financial information.

The compliance report demonstrates that you took all the security precautions necessary to protect your assets.

1. Run a PCI scan for the assets in your network that store or process PCI information.

   For more information, see Creating a scan profile on page 29.
2. Update your asset compliance plans and software declarations.

   Your compliance plan and software declarations are displayed in the special notes section of the executive summary.

   For more information, see the PCI security standards for approved software vendors.
3. Create and run a PCI compliance report for the assets that you scanned.

Related Links

Creating a scan profile on page 29

Updating your asset compliance plans and software declarations

In Extreme Networks Security Vulnerability Manager, if you want to generate a PCI compliance report for your assets, you must complete your attestations for each asset.

Your attestation of compliance is displayed on your PCI compliance report.

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**.
3. On the **Assets** page, select the asset that you want to provide an attestation for.
4. On the toolbar, click **Edit Asset**.
5. In the **Edit Asset Profile** window, click the **CVSS, Weight & Compliance** pane.
6. Complete the following fields. Use the hover help if you need assistance:
   - Compliance Plan
   - Compliance Notes
   - Compliance Notes Declaration
   - Compliance Notes Description
   - Compliance Out Of Scope Reason
7. Click **Save**.

Creating a PCI compliance report

In Extreme Networks Security Vulnerability Manager, you can create and run a PCI compliance report.

The PCI compliance report demonstrates that your assets involved in PCI activities comply with security precautions that prevent outside attack.

Ensure that you ran a PCI compliance scan.

1. Click the Reports tab.
2. On the toolbar, select Actions > Create.
3. Click Weekly and then click Next.
4. Click the undivided report layout that is displayed on the upper left section of the report wizard and click Next.
5. Type a Report Title.
6. In the Chart Type list, select Vulnerability Compliance and type a Chart Title.
7. In the Scan Profile list, select the scan profile for the assets that you scanned.

   > Attention
   > If no scan profile is displayed, you must create and run a PCI scan of the assets in your network that store or process PCI information.

8. In the Scan Result list, select the version of the scan profile that you want to use.

   > Remember
   > To provide evidence of your compliance, you must select the Latest option in the Scan Result list. You can also generate a compliance report by using a scan profile that was run at an earlier date.

9. In the Report Type list, select a report type.

   If you select Executive Summary, Vulnerability Details, or a combination of both, the attestation is automatically attached to your PCI compliance report.
10. Complete the information in the Scan Customer Information and Approved Scanning Vendor Information panes.

    > Important
    > You must add a name in the Company field for both panes, as this information is displayed in the attestation section of the report.

11. Click Save Container Details and then click Next.
12. Use the Report Wizard to complete your PCI compliance report.

The report is displayed in the reports list and is automatically generated.

Including column headings in asset searches

Limit asset searches with filters that include custom asset profiles, name, vulnerability count, and risk score.

1. Click the Assets tab.
2. In the navigation pane, click Asset Profiles, then on the toolbar click Search > New Search.
3. In the field containing column names, in the field on the left, click the column headings you want to include in your search, and click the arrow button to move the selected headings to field on the right.
4. Click the up and down buttons to change the priority of the selected column headings.
5. When the field on the right contains all the column heading that you want to search on, click Search.

11 Vulnerability research, news, and advisories

You can use Extreme Networks Security Vulnerability Manager to remain aware of the vulnerability threat level and manage security in your organization.

A vulnerability library contains common vulnerabilities that are gathered from a list of external sources. The most significant external resource is the National Vulnerability Database (NVD). You can research specific vulnerabilities by using a number of criteria for example, vendor, product, and date range. You might be interested in specific vulnerabilities that exist in products or services that you use in your enterprise.

Vulnerability Manager also provides a list of security-related news articles and advisories, gathered from an external list of resources and vendors. Articles and advisories are a useful source of security information from around the world. Articles also help you to keep up-to-date with current security risks.

Viewing detailed information about published vulnerabilities

In Extreme Networks Security Vulnerability Manager, you can display detailed vulnerability information.

Using the Research Vulnerabilities page, you can investigate CVSS metrics and access information from Extreme Networks® X-Force research and development.

1. Click the Vulnerabilities tab.
2. In the navigation pane, select Research > Vulnerabilities.
3. If no vulnerabilities are displayed, select an alternative time range from the Viewing vulnerabilities from list.
4. To search the vulnerabilities, on the toolbar, select Search > New Search.
5. Identify the vulnerability that you want to investigate.
6. Click the vulnerability link in the Vulnerability Name column.

Remaining aware of global security developments

In Extreme Networks Security Vulnerability Manager, you can view security news from across the world to help keep you updated about current security developments.

1 Click the Vulnerabilities tab.
2 In the navigation pane, click Research > News.
3 If no news articles are displayed, select an alternative time range from the Viewing news from list.
4 To search the news articles, on the toolbar, select Search > New Search.
5 Identify the news article that you want to find out more about.
6 Click the news article link in the Article Title column.

Viewing security advisories from vulnerability vendors

In Extreme Networks Security Vulnerability Manager, you can view the vulnerability advisories that are issued by software vendors. Use advisory information to help you identify the risks in your technology, and understand the implications of the risk.

1 Click the Vulnerabilities tab.
2 In the navigation pane, click Research > Advisories.
3 If no advisories are displayed, select an alternative time range from the Viewing advisories from list.
4 If you want to search the security advisories, on the toolbar, select Search > New Search.
5 Click the advisory link in the Advisory column.

  Each security advisory might include vulnerability references, solutions, and workarounds.

Searching vulnerabilities, news, and advisories

In Extreme Networks Security Vulnerability Manager, you can search the latest vulnerability news and advisories that are issued by software vendors.

1 Click the Vulnerabilities tab.
2 In the navigation pane, click one of the following options:
  - Research > Vulnerabilities.
  - Research > News.
  - Research > Advisories.
3 On the toolbar, select Search > New Search.
4 Type a search phrase in the Phrase field.
5 If you are searching news items, select a news source from the Source list.
6 In the By Date Range area, specify the date period for the news or advisory that you are interested in.
7 If you are searching a published vulnerability, specify a vendor, product and product version in the By Product area.
8 If you are searching a published vulnerability, specify a CVE, Vulnerability, or OSVDB ID in the By ID area.

News feeds

Use the RSS Feeds dashboard items to see the latest Extreme Networks® security news, advisories, published vulnerability information, and updates on scans that are completed or in progress.

The RSS Feeds dashboard items rotates the latest 10 news and scan results so that you don't need to search the Research or Scan Results pages on the Vulnerabilities tab for information.

On the Dashboard tab, use the Add Item > Reports > RSS Feeds menu to add RSS feeds to your dashboard.

Index