



InsightVM

Installation and Quick-start Guide

Table of contents

Table of contents	2
About this guide	4
Other documents and Help	4
Installing the application	6
Installation requirements	6
Supported platforms	7
Making sure you have necessary items	7
Uninstalling a previously installed copy	7
Creating an account during installation	8
Installation choices	8
Installing in Windows environments	10
Running the Windows installer	10
Running the Windows uninstaller	11
Installing in Linux environments	12
Do I need to disable SELinux?	12
Ensuring that the installer file is not corrupted	12
Installing in Ubuntu	13
Installing in Red Hat	14
Running the Linux installer	14
Running the Linux uninstaller	15
Enabling FIPS mode	17
Getting Started	20
Running the application	21
Manually starting or stopping in Windows	21
Changing the configuration for starting automatically as a service	22

Manually starting or stopping in Linux	22
Working with the daemon	22
Using the Web interface	24
Activating and updating on private networks	24
Logging on	24
Enabling Two Factor Authentication	26
Navigating the Security Console Web interface	29
Using the search feature	35
Accessing operations faster with the Administration page	39
Using configuration panels	40
Extending Web interface sessions	41
Troubleshooting your activation	41
Scanning, viewing results, and reporting	44
Discover	44
Assess	46
Act	51
Glossary	57

About this guide

Use this guide to help you to perform the following tasks:

- install the Windows or Linux version of InsightVM software
- enable FIPS mode (if necessary)
- start InsightVM
- log onto the Security Console Web interface
- get started using InsightVM

Other documents and Help

Click the **Help** link on any page of the Security Console Web interface to find information quickly. You can download any of the following documents from the *Support* page in Help.

User's guide

The user's guide helps you to gather and distribute information about your network assets and vulnerabilities using the application. It covers the following activities:

- logging onto the Security Console and familiarizing yourself with the interface
- managing dynamic discovery
- setting up sites and scans
- running scans manually
- viewing asset and vulnerability data
- creating remediation tickets
- using preset and custom report templates
- using report formats
- reading and interpreting report data
- configuring scan templates
- configuring other settings that affect scans and report

Administrator's guide

The administrator's guide helps you to ensure that InsightVM works effectively and consistently in support of your organization's security objectives. It provides instruction for doing key administrative tasks:

- configuring host systems for maximum performance
- planning a deployment, including determining how to distribute scan engines
- managing users and roles
- maintenance and troubleshooting

API guide

The API guide helps you to automate some InsightVM features and to integrate its functionality with your internal systems.

Installing the application

This section provides the following information about installing InsightVM:

- *Installation requirements* on page 6
- *Installing in Windows environments* on page 10
- *Installing in Linux environments* on page 12
- *Enabling FIPS mode* on page 17

Installation requirements

Make sure that your host hardware and network support InsightVM operations.

Hardware requirements

See the Rapid7 Web site for hardware requirements:

<http://www.rapid7.com/products/insightvm/system-requirements/>.

It is recommended that you install InsightVM on a computer that does not have an Intrusion Detection System (IDS), an Intrusion Prevention System (IPS), or a firewall enabled. These devices block critical operations that are dependent on network communication.

The 64-bit configuration is recommended for enterprise-scale deployments.

Network activities and requirements

The Security Console communicates over the network to perform four major activities:

Activity	Type of communication
manage scan activity on Scan Engines and pull scan data from them	outbound; Scan Engines listen on 40814
download vulnerability checks and feature updates from a server at updates.rapid7.com	outbound; server listens on port 80
upload PGP-encrypted diagnostic information to a server at support.rapid7.com	outbound; server listens on port 443
provide Web interface access to users	inbound; Security Console accepts HTTPS requests over port 3780

Scan Engines contact target assets using TCP, UDP, and ICMP to perform scans. They do not initiate outbound communication with the Security Console.

Ideally there should be no firewalls or similar devices between a Scan Engine and its target assets. Also, scanning may also require some flexibility in security policies. For more information, see the *administrator's guide*.

Supported platforms

See the Rapid7 Web site for supported platforms:

<http://www.rapid7.com/products/insightvm/system-requirements/>.

Making sure you have necessary items

Make sure you have all of the following items before you begin the installation process:

- installers for all supported environments (.bin files for Linux and .exe files for Windows)
- the md5sum, which helps to ensure that installers are not corrupted during download
- documentation, including this guide
- a product key, which you need to activate your license when you log on

If you do not have any of these items, contact your account representative. If you purchased InsightVM or registered for an evaluation, Rapid7 sent you an e-mail that includes links for downloading these items and the product key. It is recommended that you add InsightVM to your e-mail client white list communication to ensure you receive future e-mails about InsightVM.

During the installation, the installer runs a system check and identifies any system components or settings that meet the minimum requirements but not the recommended requirements. If any items are identified, you can continue the installation, but you should consider modifying your system after the installation to ensure optimal performance. For example, if your system does not have the recommended the amount of RAM, you may encounter performance issues with RAM-intensive operations, such as running scans or reports. To prevent this, you should consider adding RAM to your system.

Uninstalling a previously installed copy

Installing and using multiple copies of the software on the same server is not supported. If you install multiple copies on the same server, the application will not function properly.

Each copy of the software must be installed from scratch. This means that if you already have a copy installed, you must uninstall it before you install the new copy you downloaded.

Use the procedure in the section *Running the Windows uninstaller* on page 11 or *Running the Linux uninstaller* on page 15 to uninstall any previously installed copies.

Creating an account during installation

When you install the application, you create a default Global Administrator account. You will use the account to log onto the application after you complete the installation.

Recovery of credentials is not supported. If you forget your user name or password, you will have to reinstall the program. Credentials are case-sensitive.

As you enter credentials, the complexity requirements are displayed to ensure that you create strong (secure) credentials. Even if your password meets the requirements, it is recommended that you make your password as strong as possible for better security. A “heat bar” is displayed that gradually changes color from red to green as you make your password stronger.

A Global Administrator can create and modify accounts after installation. See *Managing users and authentication* in Help or the administrator’s guide.

Installation choices

During the installation, you will make several choices, including the following:

- Select the component(s) you want to install and where to install them.
- Enable the application to initialize during the installation and start automatically after installation.
- If you install only the Scan Engine, you must select a communication direction between an existing Security Console and the new Scan Engine.

Selection of components

You can either install a Security Console with a local Scan Engine or you can install a distributed Scan Engine. If you install the latter, you must have a Security Console running in your environment before you can use the Scan Engine. The Security Console controls all Scan Engine activity.

Application initialization and automatic start option

You can choose to have the application initialize during installation and automatically start once you finish the installation. By default, this option is enabled. If you do not want initialization to

occur during installation, you must disable it.

You can only leave this option enabled if you install both components (the Scan Engine and Security Console). If you choose to install only the Scan Engine, this option is not available.

The benefit to leaving the option enabled is that you can start using the application immediately after the installation is complete. This is because the initialization process prepares the application for use by updating the database of vulnerability checks and performing the initial configuration.

Because the time required for the initialization process ranges from 10 to 30 minutes, leaving the option enabled increases the total installation time by 10 to 30 minutes. Although disabling the option shortens the installation time, it takes longer to start the application because it has to initialize before you can begin using it.

Communication direction between Console and Engine

Which direction is preferred depends on your network configuration:

- Engine to Console: The Scan Engine will actively inform the Security Console that it is available for communication. This configuration allows a console that is behind a firewall and is configured to allow inbound connections to establish a communication channel.
- Console to Engine: The Scan Engine will listen for communication from the Security Console. This configuration is most effective when the engine and console are on the same area of the network.

Tips for using the installation wizard

The pages of the wizard are listed in the left page of the wizard, and the current page is highlighted. You can use the list to check your progress.

Each page of the wizard has a **Previous** button and a **Cancel** button. Use the **Previous** button to go to a previous page if you need to review or change an installation setting. Use the **Cancel** button only if you need to cancel the installation. If you cancel at any point in during the installation process, no files are installed and you need to go back to the beginning of the installation process.

Installing in Windows environments

This section describes how to install InsightVM on a Windows host. It also describes options that are available to you during the installation.

Before you begin

Confirm the following items:

- You are logged onto Windows as an administrator.
- Your system meets the minimum installation requirements. See *Installation requirements* on page 6 for details.
- You have all of the items you need to complete the installation. See *Making sure you have necessary items* on page 7 for details.
- You have uninstalled any previously installed copies of the application. See *Running the Windows uninstaller* on page 11 for details.

Running the Windows installer

To install the application in Windows, take the following steps:

1. Double-click the **installer icon**.

The installer displays a message that it is preparing the wizard to guide you through the installation. Then the *Welcome* page of the wizard is displayed.

Command-line windows open once you begin the installation. Although you do not need to interact with them, do not close them.

Note: The installation will stop if you close the command line interface windows.

Click **Next**. The *Type and destination* page is displayed.

2. Follow the instructions in the installer. If you want to enable FIPS mode, do not select the option to initialize the application after installation. FIPS mode must be enabled before the application runs for the first time.

If you are installing just the Scan Engine, you may need to specify the Shared Secret to pair it with a Security Console. Global Administrators can generate a Shared Secret in the Administration section of the Security Console. Select **manage** next to *Engines*, click **Generate** next to *Shared Secret*, and copy and paste the Shared Secret into the Installation Wizard.

3. See *Getting Started* on page 20 for information on getting started using the application.

Running the Windows uninstaller

Each copy of InsightVM must be installed from scratch. This means that if you already have it installed on your system, you must uninstall it before installing the new copy you downloaded.

Warning: To prevent a loss of sites, configurations, reports, and other data, make sure you back up all of your data before you begin the procedure.

Uninstalling completely removes all components. It also deletes sites, configurations, reports, and any scan data on discovered assets, nodes, and vulnerabilities.

To uninstall the application:

1. Start the program to uninstall by doing one of the following:
 - Click the Windows **Start** button and select the **Control Panel**.
 - Select the **uninstall** option or the **remove a program** option (depends on the version of Windows you are running).
 - (If you have a shortcut folder.) Click the Windows **Start** button, go to the InsightVM folder, and select the **Uninstaller**.
2. Double-click InsightVM in the list of programs.
3. Run the uninstaller program.

The uninstaller displays a *Welcome* page. Read the warning about backing up data.

4. Click **Next**.

The uninstaller displays a status bar with a message that uninstallation is in progress followed by a message that the uninstallation is complete.

Do not close the command line window.

5. Click **Finish**.

Installing in Linux environments

See the instructions for your specific supported Linux distribution.

Do I need to disable SELinux?

SELinux is a security-related feature that must be disabled before you can install the application.

Tip: Later versions of Ubuntu do not include SELinux, or it is automatically set to `permissive`. It is recommended that you check the status before you start the installation.

To disable SELinux, take these steps:

1. Open the SELinux configuration file in your preferred text editor.

Example: `$ vi /etc/selinux/config`

2. Go the line that begins with `SELINUX=`.

If the setting is `enforcing`, change it to `disabled`: `SELINUX=disabled`

3. Save and close the file.
4. Restart the server for the change to take effect: `$ shutdown -r now`

At this point you can check the installer file to make sure it is not corrupted or begin the installation. It is recommended that you check the installer file before you begin the installation.

Ensuring that the installer file is not corrupted

This procedure shows you how to check the installer file you downloaded to make sure it is not corrupted. This helps to prevent installation problems.

Make sure that you downloaded the installation file and the md5sum file. See *Installing the application* on page 6 for details.

To check the installer file, take these steps:

1. Go to the directory that contains the installer and the md5sum file. If you have not changed any settings, this will be `Downloads`.
2. Run the md5sum program with the `-c` option to check the MD5 checksum:

```
$ md5sum -c [installer_file_name].md5sum
```

- If this command returns an `OK` message, the file is valid.
- If it returns a “FAILED” message, download the installer and md5sum file again, and repeat this procedure.

Installing in Ubuntu

Make sure that:

- You have downloaded all items necessary for installation. See *Installing the application* on page 6 for details.
- You have root-level access.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 12.

Manually installing necessary packages in Ubuntu

If `sudo` is active in your environment, and if your account is listed in the `sudoers` file, you can use `sudo -i` to run the commands.

Tip: Rapid7 recommends using `apt-get` to install packages on Ubuntu.

To install the necessary packages:

1. To verify that you have `apt-get`, run:

```
$ apt-get -v
```

2. To determine if you have a required package and install it if necessary, run:

```
$ apt-get install [package_name]
```

The following package should be installed:

- `screen`

Next Steps

Run the Linux installer. See "Running the Linux installer" below.

Installing in Red Hat

You must have root-level access to run the installation. If sudo is active in your environment, and if your account is listed in the sudoers file, you can use `sudo -i` to run the commands.

Make sure that:

- You have downloaded all items necessary for installation. See *Installing the application* on page 6 for details.
- You have yum and RPM, which you need to install packages on Red Hat.
- You have a Red Hat Enterprise Linux license.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 12.

Manually installing necessary packages in Red Hat

You need yum and RPM to install packages on Red Hat.

1. To verify that you have yum and RPM, run: `$ yum --version`
2. To determine if you have a required package and install it as necessary, run:

```
$ yum install [package_name]
```

The following package should be installed: `screen`.

Running the Linux installer

This procedure shows you how to install the application in a Linux environment.

If you are using a graphical user interface

If you are using an interface such as KDE or Gnome, omit the `-c flag` in step 3 of the procedure. The installer opens a wizard to guide you through the installation (similar to the Windows installation wizard (see *Installing in Windows environments* on page 10)). The rest of the steps in this procedure reflect installation using the command line interface.

Before you begin

Make sure that:

- Your system meets the minimum installation requirements.
- You have all of the items you need to complete the installation. See *Installing in Linux environments* on page 1.
- You have disabled SELinux (if necessary). See *Do I need to disable SELinux?* on page 1.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 12.
- You have installed the required packages for your Linux platform.
- You have uninstalled any previously installed copies. See *Running the Linux uninstaller* on page 15.

Warning: The installation will fail if you do not install all necessary packages.

To install the application, take these steps:

1. Go to the directory that contains the installer.
2. Change the permissions for the installation file to make it executable:

```
$ chmod +x [installation_file_name]
```

3. Start the installer:

```
$ ./[installation_file_name] -c
```

The installer displays information about the application.

4. Follow the instructions in the installer. If you want to enable FIPS mode, do not select the option to initialize the application after installation. FIPS mode must be enabled before the application runs for the first time.

If you are installing just the Scan Engine, you may need to specify the Shared Secret to pair it with a Security Console. Global Administrators can generate a Shared Secret in the Administration section of the Security Console. Select **manage** next to *Engines*, click **Generate** next to *Shared Secret*, and copy and paste the Shared Secret into the Installation Wizard.

5. See *Getting Started* on page 20 for information on getting started using the application.

Running the Linux uninstaller

Each copy of InsightVM must be installed from scratch. This means that if you already have it installed on your system, you must uninstall it before you install the new copy you downloaded.

Warning: To prevent a loss of sites, configurations, reports, and other data, make sure you back up all of your data before you begin the procedure.

Uninstalling completely removes all components. It also deletes sites, configurations, reports, and any scan data on discovered assets, nodes, and vulnerabilities.

To uninstall the application, take these steps:

1. Run: `$ cd [installation directory]/.install4j`
`install4j` is a hidden directory. To list hidden directories, run: `ls -a`
2. Run: `$./uninstall`

Enabling FIPS mode

If you are operating the application in an environment where the use of FIPS-enabled products is mandatory, or if you want the security of using a FIPS-certified encryption module, you should enable FIPS mode. The application supports the use of Federal Information Processing Standard (FIPS) 140-2 encryption, which is required by government agencies and companies that have adopted FIPS guidelines.

What is FIPS?

The FIPS publications are a set of standards for best practices in computer security products. FIPS certification is applicable to any part of a product that employs cryptography. A FIPS-certified product has been reviewed by a lab and shown to comply with FIPS 140-2 (Standard for Security Requirements for Cryptographic Modules), and to support at least one FIPS-certified algorithm.

Government agencies in several countries and some private companies are required to use FIPS-certified products.

What is FIPS mode?

FIPS mode is a configuration that uses FIPS-approved algorithms only. When the application is configured to operate in FIPS mode, it implements a FIPS-certified cryptographic library to encrypt communication between the Security Console and Scan Engines, and between the Security Console and the user for both the browser and API interfaces.

FIPS mode considerations

It is important to note that due to encryption key generation considerations, the decision to run in FIPS mode or non-FIPS mode is irrevocable. The application must be configured to run in FIPS mode immediately after installation and before it is started for the first time, or else left to run in the default non-FIPS mode. Once the application has started with the chosen configuration, you will need to reinstall it to change between modes.

Activating FIPS mode

When InsightVM is installed, it is configured to run in non-FIPS mode by default. The application must be configured to run in FIPS mode before being started for the first time. See *Activating FIPS mode in Linux* on page 18.

When FIPS mode is enabled, communication between the application and non-FIPS enabled applications such as Web browsers or API clients cannot be guaranteed to function correctly.

Activating FIPS mode in Linux

You must follow these steps after installation, and BEFORE starting the application for the first time.

To enable FIPS mode:

1. Install rng-utils.

The encryption algorithm requires that the system have a large entropy pool in order to generate random numbers. To ensure that the entropy pool remains full, the rngd daemon must be running while the application is running. The rngd daemon is part of the rng-utils Linux package.

2. Download and install the rng-utils package using the system's package manager.

Tip: Add the rngd command to the system startup files so that it runs each time the server is restarted.

3. Run the command `rngd -b -r /dev/urandom`.

4. Create a properties file for activating FIPS mode.

5. Create a new file using a text editor.

6. Enter the following line in this file:

```
fipsMode=1
```

7. Save the file in the [install_directory]/nsc directory with the following name:

CustomEnvironment.properties

8. Start the Security Console.

Activating FIPS mode in Windows

You must follow these steps after installation, and before starting the application for the first time.

To enable FIPS mode:

1. Create a properties file for activating FIPS mode.

2. Create a new file using a text editor.

3. Enter the following line in this file:

```
fipsMode=1
```

Note: You can disable database consistency checks on startup using the CustomEnvironment.properties file. Do this only if instructed by Technical Support.

4. Save the file in the [install_directory]\nsc directory with the following name:

CustomEnvironment.properties

5. Start the Security Console.

Verifying that FIPS mode is enabled

To ensure that FIPS mode has been successfully enabled, check the Security Console log files for the following messages:

```
FIPS 140-2 mode is enabled. Initializing crypto provider
```

```
Executing FIPS self tests...
```

Getting Started

If you haven't used the application before, this section helps you to become familiar with the Web interface, which you will need for running scans, creating reports, and performing other important operations.

- *Running the application* on page 21: By default, the application is configured to run automatically in the background. If you need to stop and start it automatically, or manage the application service or daemon, this section shows you how.
- *Using the Web interface* on page 24: This section guides you through logging on, navigating the Web interface, using configuration panels, and running searches.

Running the application

This section includes the following topics to help you get started with the application:

- *Manually starting or stopping in Windows* on page 21
- *Changing the configuration for starting automatically as a service* on page 22
- *Manually starting or stopping in Linux* on page 22
- *Working with the daemon* on page 22

Manually starting or stopping in Windows

InsightVM is configured to start automatically when the host system starts. If you disabled the initialize/start option as part of the installation, or if you have configured your system to not start automatically as a service when the host system starts, you will need to start it manually.

Starting the Security Console for the first time will take 10 to 30 minutes because the database of vulnerabilities has to be initialized. You may log on to the Security Console Web interface immediately after the startup process has completed.

If you have disabled automatic startup, use the following procedure to start the application manually:

1. Click the **Windows Start** button
2. Go to the application folder.
3. Select **Start Services**.

Use the following procedure to stop the application manually:

1. Click the **Windows Start** button.
2. Open the application folder.
3. Click the **Stop Services** icon.

Changing the configuration for starting automatically as a service

By default the application starts automatically as a service when Windows starts. You can disable this feature and control when the application starts and stops.

1. Click the **Windows Start** button, and select **Run...**
2. Type `services.msc` in the *Run* dialog box.
3. Click **OK**.
4. Double-click the icon for the Security Console service in the *Services* pane.
5. Select *Manual* from the drop-down list for **Startup type**:
6. Click **OK**.
7. Close *Services*.

Manually starting or stopping in Linux

If you disabled the initialize/start option as part of the installation, you need to start the application manually.

Starting the Security Console for the first time will take 10 to 30 minutes because the database of vulnerabilities is initializing. You can log on to the Security Console Web interface immediately after startup has completed.

To start the application from graphical user interface, double-click the InsightVM in the *Internet* folder of the *Applications* menu.

To start the application from the command line, take the following steps:

1. Go to the directory that contains the script that starts the application:

```
$ cd [installation_directory]/nsc
```

2. Run the script: `./nsc.sh`

Working with the daemon

The installation creates a daemon named *nexposeconsole.rc* in the `/etc/init.d/` directory.

WARNING: Do not use `<CTRL+C>`, it will stop the application.

To detach from a screen session, press `<CTRL +A + D>`.

Manually starting or stopping the daemon

To manually start or stop the application as a daemon, run the following commands:

```
service nexposeconsole start/stop
```

```
systemctl nexpose start/stop
```

Preventing the daemon from automatically starting with the host system

To prevent the application daemon from automatically starting when the host system starts, run the following command:

```
$ update-rc.d [daemon_name] remove
```

Using the Web interface

This section includes the following topics to help you access and navigate the Security Console Web interface:

- *Logging on* on page 24
- *Enabling Two Factor Authentication* on page 26
- *Navigating the Security Console Web interface* on page 29
- *Selecting your language* on page 33
- *Using icons and other controls* on page 33
- *Using the search feature* on page 35
- *Using configuration panels* on page 40
- *Extending Web interface sessions* on page 41

Activating and updating on private networks

If your Security Console is not connected to the Internet, you can find directions on updating and activating on private networks. See the topic *Managing versions, updates, and licenses* in the administrator's guide.

Logging on

The Security Console Web interface supports the following browsers:

- Google Chrome (latest) (RECOMMENDED)
- Mozilla Firefox (latest)
- Mozilla Firefox ESR (latest)
- Microsoft Internet Explorer 11

If you received a product key, via e-mail use the following steps to log on. You will enter the product key during this procedure. You can copy the key from the e-mail and paste it into the text box; or you can enter it with or without hyphens. Whether you choose to include or omit hyphens, do so consistently for all four sets of numerals.

If you do not have a product key, click the link to request one. Doing so will open a page on the Rapid7 Web site, where you can register to receive a key by e-mail. After you receive the product key, log on to the Security Console interface again and follow this procedure.

If you are a first-time user and have not yet activated your license, you will need the product key that was sent to you to activate your license after you log on.

To log on to the Security Console take the following steps:

1. Start a Web browser.

If you are running the browser on the same computer as the console, go to the following URL: `https://localhost:3780`

Indicate HTTPS protocol and to specify port 3780.

If you are running the browser on a separate computer, substitute `localhost` with the correct host name or IP address.

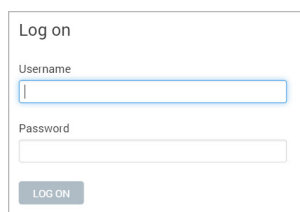
Your browser displays the *Logon* window.

Tip: If there is a usage conflict for port 3780, you can specify another available port in the *httpd.xml* file, located in `[installation_directory]\nsc\conf`. You also can switch the port after you log on. See the topic *Changing the Security Console Web server default settings* in the administrator's guide.

Note: If the logon window indicates that the Security Console is in maintenance mode, then either an error has occurred in the startup process, or a maintenance task is running. See *Running in maintenance mode* in the administrator's guide.

2. Enter your user name and password that you specified during installation.

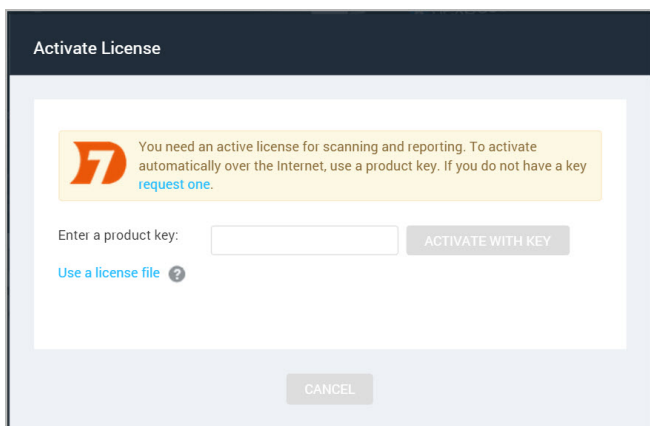
User names and passwords are case-sensitive and non-recoverable.

A screenshot of a web-based logon window. The window has a title bar that says "Log on". Inside the window, there are two text input fields: the first is labeled "Username" and the second is labeled "Password". Below these fields is a button labeled "LOG ON".

Logon window

3. Click the **Logon** icon.

If you are a first-time user and have not yet activated your license, the Security Console displays an activation dialog box. Follow the instructions to enter your product key.



Activate License window

4. Click **Activate** to complete this step.
5. Click the **Home** icon to view the Security Console *Home* page.
6. Click the **Help** icon on any page of the Web interface for information on how to use the application.

The first time you log on, you will see the *News* page, which lists all updates and improvements in the installed system, including new vulnerability checks. If you do not wish to see this page every time you log on after an update, clear the check box for automatically displaying this page after every login. You can view the *News* page by clicking the **News** link that appears under the **Help** icon dropdown. The **Help** icon can be found near the top right corner of every page of the console interface.

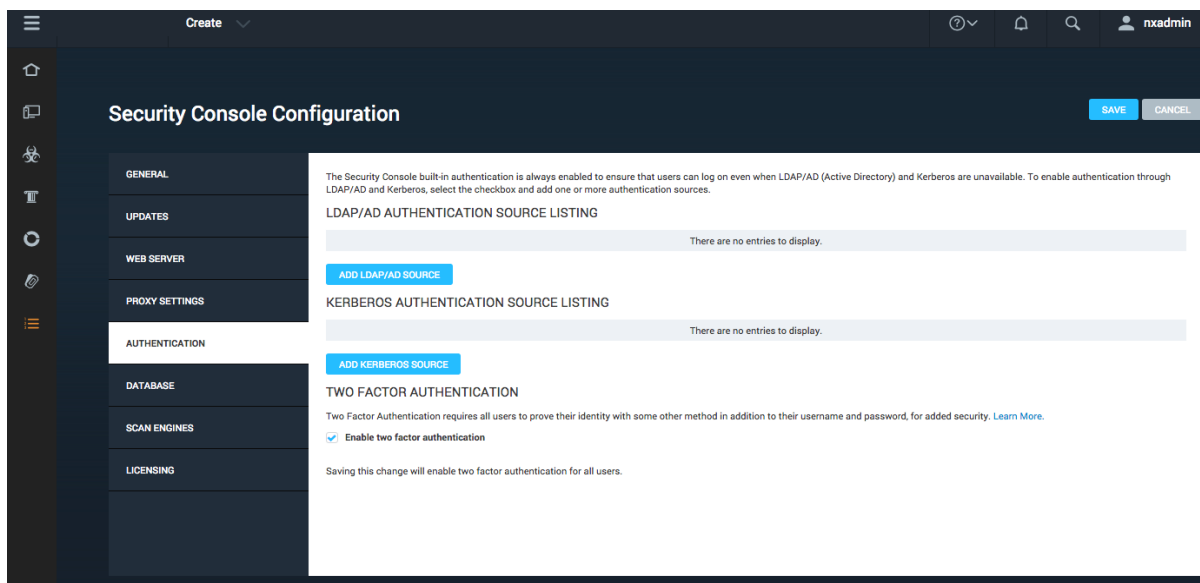
Enabling Two Factor Authentication

For organizations that want additional security upon login, the product supports Two Factor Authentication. Two Factor Authentication requires the use of a time-based one-time password application such as Google Authenticator.

Two Factor Authentication can only be enabled by a Global Administrator on the *Security Console*.

To enable Two Factor Authentication:

1. As a Global Administrator, go to the **Administration** tab.
2. Click the **Administer** link in the *Global and Console Settings* section.
3. Select **Enable two factor authentication**.



The next step is to generate a token for each user. The users can generate their own tokens, or you can generate tokens for them that they then change. In either case, you should communicate with them about the upcoming changes.

Method 1: Tokens created by users

Once Two Factor Authentication is enabled, when a user logs on, they will see a field where they can enter an access code. For the first time, they should log in without specifying an access code.

Once the user logs in, they can generate a token in the *User Preferences* page.

User Configuration

GENERAL
SITE ACCESS
ASSET GROUP ACCESS

User name

nxadmin

Full name

nxadmin

E-mail address

Old password

New password

Confirm password

Two Factor Authentication Token

GENERATE NEW TOKEN

Display user interface in

English (United States)

Run reports in

English (United States)

Color scheme

Dark

Account enabled

☒

The user should then open their time-based one-time password application such as Google Authenticator. They should enter the token as the key in the password application. The password application will then generate a new code that should be used as the user's access code when logging in.

A Global Administrator can check whether users have completed the Two Factor Authentication on the *Manage Users* page. The *Manage Users* page can be reached by going to the *Administration* tab and clicking the **Manage** link in the *Users* section. A new field, **Two Factor Authentication Enabled**, will appear in the table and let the administrator know which users have enabled this feature.

<input type="checkbox"/>	Authenticator	User Name	Full Name	Email	Administrator	Last Logon	Password Expires	Two Factor Authentication Enabled	Disabled	Sites	Groups	Unlock	Edit	Delete
<input type="checkbox"/>	Nexpose user	nxadmin	nxadmin		Yes	1/5/2016 12:39 PM	N/A	No	No	0	0			
<input type="checkbox"/>	Nexpose user	User1	User1		No		N/A	Yes	No	0	0			

NEW USER
DISABLE USERS
ENABLE USERS

If the user doesn't create a token, they will still be able to log in without an access code. In this case, you may need to take steps to enforce enablement.

Method 2: Generating tokens for users

You can enforce that all users log in with a token by disabling the accounts of any users who have not completed the process, or by creating tokens for them and emailing them their tokens.

To disable users:

1. Go to the *Manage users* page by going to the **Administration** tab and clicking the **Manage** link in the *Users* section.
2. Select the checkbox next to each user for whom the Two Factor Authentication Enabled column shows No.
3. Select **Disable users**.

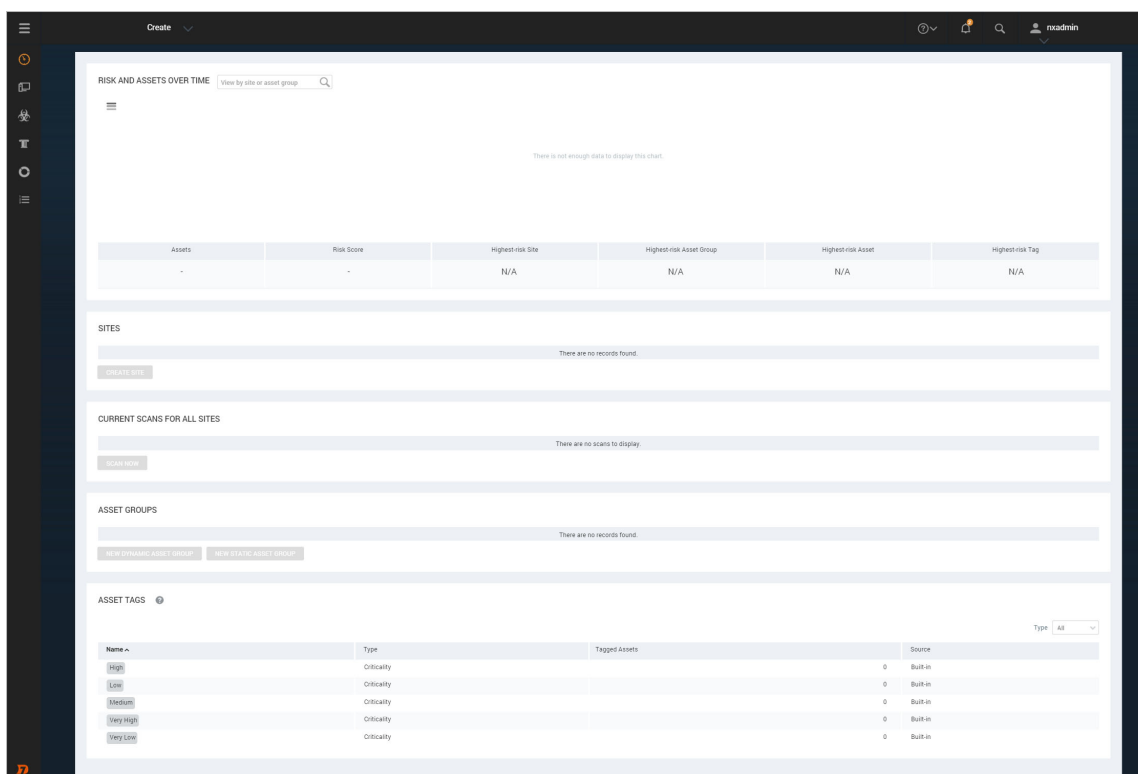
To generate a token for a user:

1. Go to the *Manage users* page by going to the **Administration** tab and clicking the **Manage** link in the *Users* section.
2. Select **Edit** for that user.
3. Generate a token for that user.
4. Provide the user with the token.
5. Once the user logs in with their access code, they can change their token if they would like in the *User preferences* page.

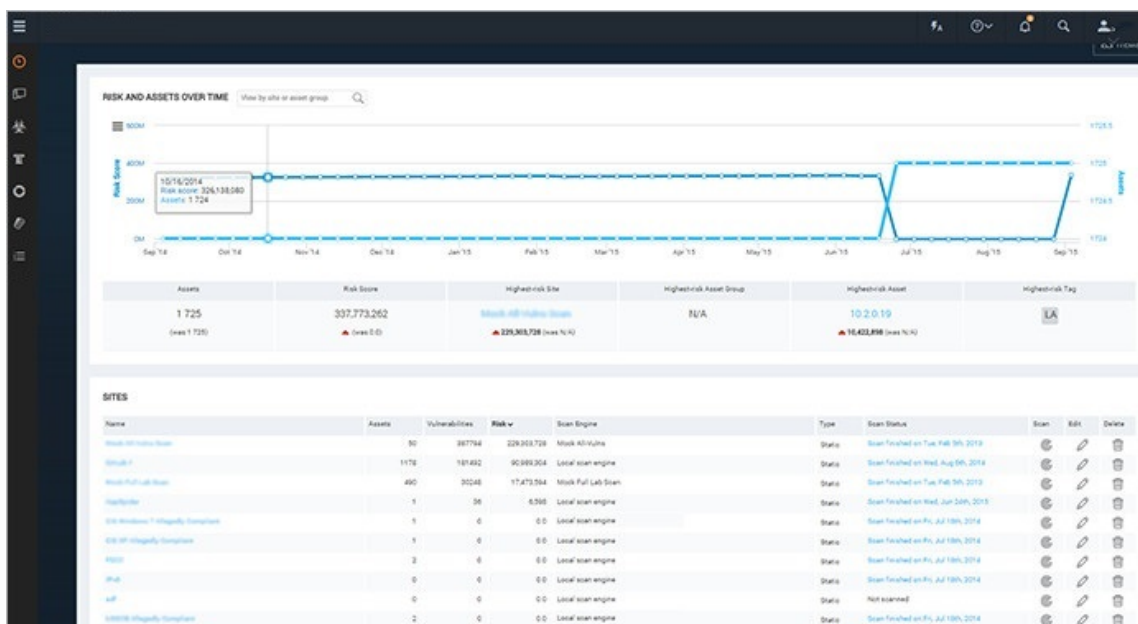
Navigating the Security Console Web interface

The Security Console includes a Web-based user interface for configuring and operating the application. Familiarizing yourself with the interface will help you to find and use its features quickly.

When you log on to the *Home* page for the first time, you see place holders for information, but no information in them. After installation, the only information in the database is the account of the default Global Administrator and the product license.



The Home page as it appears in a new installation



The Home page as it appears with scan data

The *Home* page shows sites, asset groups, tickets, and statistics about your network that are based on scan data. If you are a Global Administrator, you can view and edit site and asset group information, and run scans for your entire network on this page.

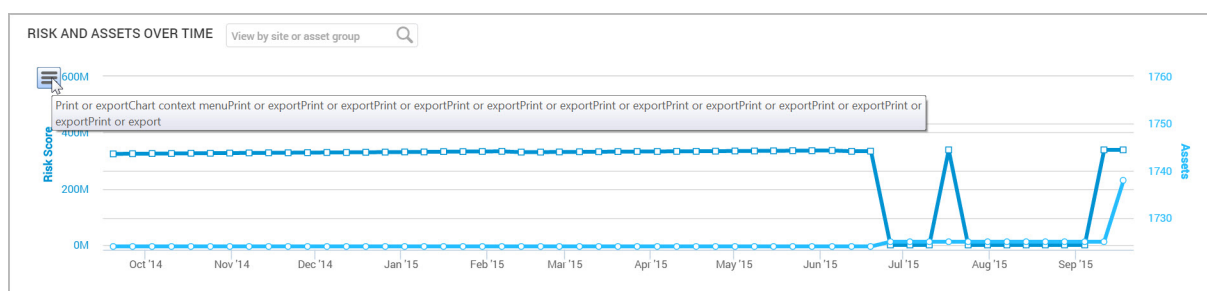
The *Home* page also displays a chart that shows trends of risk score and number of assets over time. The growth in assets over time is an increase in your surface area (total number of assets). As you add assets to your environment your level of risk can increase because the more assets you have, the more potential there is for vulnerabilities.

Each point of data on the chart represents a week. The darker blue line and measurements on the left show how much your risk score has increased or decreased over time. The lighter blue line displays the number of assets.

Note: This interactive chart shows a default of a year's worth of data when available; if you have been using the application for a shorter historical period, the chart will adjust to show only the months applicable.

The following are some additional ways to interact with charts:

- In the search filter at the top left of the chart, you can enter a name of a site or asset group to narrow the results that appear in the chart pane to only show data for that specific site or group.
- Click and drag to select a smaller, specific timeframe and view specific details. Select the **Reset/Zoom** button to reset the view to the previous settings.
- Hover your mouse over a point of data to show the date, the risk score, and the number of assets for the data point.
- Select the sidebar menu icon on the top left of the chart window to export and print a chart image.



Print or export the chart from the sidebar menu

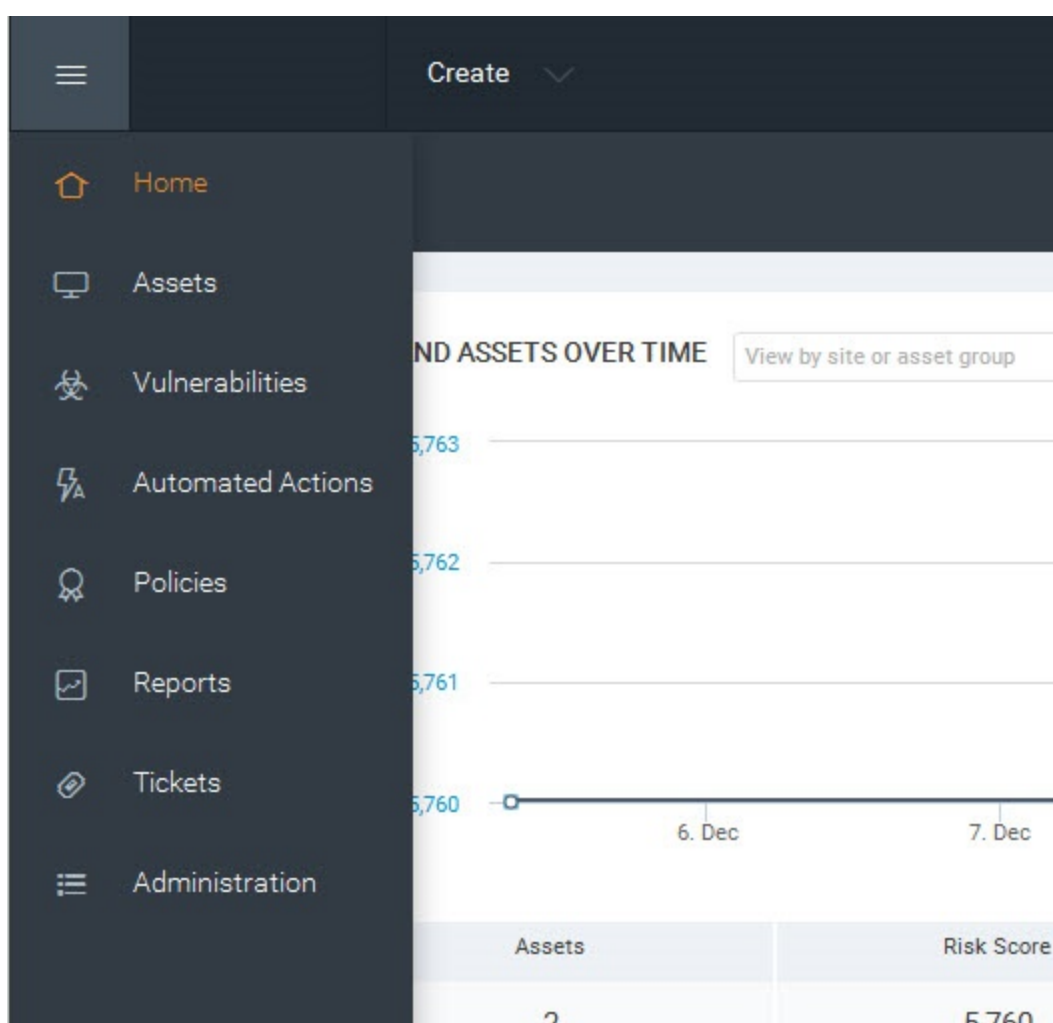
On the *Site Listing* pane, you can click controls to view and edit site information, run scans, and start to create a new site, depending on your role and permissions.

Information for any currently running scan appears in the pane labeled *Current Scan Listings for All Sites*.

On the *Ticket Listing* pane, you can click controls to view information about tickets and assets for which those tickets are assigned.

On the *Asset Group Listing* pane, you can click controls to view and edit information about asset groups, and start to create a new asset group.

A menu appears on the left side of the *Home* page, as well as every page of the Security Console. Mouse over the icons to see their labels, and use these icons to navigate to the main pages for each area.



Icon menu

The *Home* page links to the initial page you land on in the Security Console.

The *Assets* page links to pages for viewing assets organized by different groupings, such as the sites they belong to or the operating systems running on them.

The *Vulnerabilities* page lists all discovered vulnerabilities.

The *Policies* page lists policy compliance results for all assets that have been tested for compliance.

The *Reports* page lists all generated reports and provides controls for editing and creating report templates.

The *Tickets* page lists remediation tickets and their status.

The *Administration* page is the starting point for all management activities, such as creating and editing user accounts, asset groups, and scan and report templates. Only Global Administrators see this icon.

Selecting your language

Some features of the application are supported in multiple languages. You have the option to set your user preferences to view Help in the language of your choosing. You can also run Reports in multiple languages, giving you the ability to share your security data across multi-lingual teams.







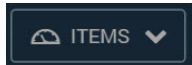










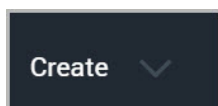
To select your language, click your user name in the upper-right corner and select **User Preferences**. This will take you to the *User Configuration* panel. Here you can select your language for Help and Reports from the corresponding drop down lists.

When selecting a language for Help, be sure to clear your cache and refresh your browser after setting the language to view Help in your selection.

Setting your report language from the *User Configuration* panel will determine the default language of any new reports generated through the *Create Report Configuration* panel. Report configurations that you have created prior to changing the language in the user preferences will remain in their original language. When creating a new report, you can also change the selected language by going to the **Advanced Settings** section of the *Create a report* page. See the topic *Creating a basic report* in the user's guide.

Using icons and other controls

Throughout the Web interface, you can use various controls for navigation and administration.

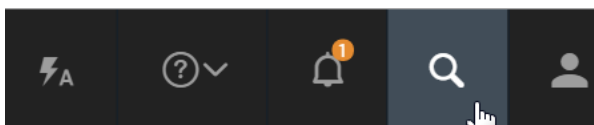
Control	Description	Control	Description
	Minimize any pane so that only its title bar appears.		Add items to your dashboard.
	Expand a minimized pane.		Copy a built-in report template to create a customized version.
	Close a pane.		Edit properties for a site, report, or a user account.
	Click to display a list of closed panes and open any of the listed panes.		View a preview of a report template.
	Export data to a comma-separated value (CSV) file.		Delete a site, report, or user account.
	Start a manual scan.		Exclude a vulnerability from a report.
	Pause a scan.		View Help. View the Support page to search FAQ pages and contact Technical Support. View the <i>News</i> page which lists all updates.
	Resume a scan.	Product logo	Click the product logo in the upper-left area to return to the <i>Home</i> page.
	Stop a scan.	User: <user name> link	This link is the logged-on user name. Click it to open the User Configuration panel where you can edit account information such as the password and view site and asset group access. Only Global Administrators can change roles and permissions.
	Initiate a filtered search for assets to create a dynamic asset group.	Log Out link	Log out of the Security Console interface. The <i>Logon</i> box appears. For security reasons, the Security Console automatically logs out a user who has been inactive for 10 minutes.
	Expand a drop-down list of options to create sites, asset groups, tags, or reports.		

Using the search feature

With the powerful full-text search feature, you can search the database using a variety of criteria, such as the following:

- full or partial IP addresses
- asset names
- site names
- asset group names
- vulnerability titles
- vulnerability CVE IDs
- internal vulnerability IDs user-added tags
- criticality tags
- Common Configuration Enumerator (CCE) IDs
- operating system names

Access the **Search** box on any a page of the Security Console interface by clicking the magnifying glass icon near the top right of the page.



Clicking the Search icon

Enter your search criteria into the **Search** box and then click the magnifying glass icon again. For example, if you want to search for discovered instances of the vulnerabilities that affect assets running ActiveX, enter *ActiveX* or *activex* in the **Search** text box. The search is not case-sensitive.



Starting a search

The application displays search results on the *Search* page, which includes panes for different groupings of results. With the current example,

ActiveX, results appear in the *Vulnerability Results* table. At the bottom of each category pane, you can view the total number of results and change settings for how results are displayed.

SEARCH CRITERIA

Search for

activex*

SEARCH AGAIN

Add an asterisk (*) to find all results that include a search string. For example: To find all IP addresses in the 10.2 range, enter 10.2.* To match your string exactly, do not add an asterisk.

☒ Include all words in each result.

VULNERABILITY RESULTS

Exposures:
☠ Susceptible to malware attacks
🔓 Metasploit-exploitable
📄 Exploit published

Title		CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
MS99-037: ImportExportFavorites Vulnerability		10	906	Fri Sep 10 1999	Mon Jul 30 2012	Critical	0	Exclude
MS00-085: ActiveX Parameter Validation Vulnerability		10	903	Thu Nov 02 2000	Mon Jul 30 2012	Critical	178	Exclude
MS01-038: Outlook View Control Exposes Unsafe Functionality		10	901	Thu Jul 12 2001	Mon Jul 30 2012	Critical	0	Exclude
MS99-018: Malformed Favorites Icon Vulnerability		7.6	885	Thu May 27 1999	Mon Jan 14 2013	Critical	0	Exclude
MS04-038: Cumulative Security Update for Internet Explorer (834707)		10	885	Tue Oct 12 2004	Fri Feb 13 2015	Critical	266	Exclude
MS00-042: Active Setup Download Vulnerability		7.6	877	Thu Jun 29 2000	Mon Jan 14 2013	Critical	132	Exclude
MS06-013: Cumulative Security Update for Internet Explorer (912812)		10	873	Tue Apr 11 2006	Fri Feb 13 2015	Critical	156	Exclude
Apple QuickTime ActiveX Buffer Overflow 2		7.6	870	Thu May 03 2001	Wed Dec 04 2013	Critical	22	Exclude
MS07-016: Cumulative Security Update for Internet Explorer (928090)		10	865	Tue Feb 13 2007	Fri Feb 13 2015	Critical	266	Exclude
MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution (826232)		9.3	855	Wed Oct 15 2003	Tue Mar 18 2014	Critical	112	Exclude

Showing 1 to 10 of 142
[Export to CSV](#)

Rows per page:
10
1
of 15

CCE RESULTS

ID	Description	Platform
CCE-10095-8	The "Download signed ActiveX controls" machine setting should be configured correctly for the Locked-Down Internet Zone.	ie8
CCE-16953-2	The "Initialize and script ActiveX controls not marked as safe" machine setting should be configured correctly for the Locked-Down Intranet Zone.	ie8
CCE-10380-4	The "Access data sources across domains" machine setting should be configured correctly for the Internet Zone.	ie8
CCE-10405-9	The "Restrict ActiveX Install: Internet Explorer Processes" machine setting should be configured correctly.	ie8

Search results

In the *Search Criteria* pane, you can refine and repeat the search. You can change the search phrase and choose whether to allow partial word matches and to specify that all words in the phrase appear in each result. After refining the criteria, click the **Search Again** button.

Using asterisks and avoiding stop words

When you run initial searches with partial strings in the *Search* box that appears in the upper-right corner of most pages in the Web interface, results include all terms that even partially match those strings. It is not necessary to use an asterisk (*) on the initial search. For example, you can enter *Win* to return results that include the word *Windows*, such as any *Windows* operating system. Or if you want to find all IP addresses in the 10.20 range, you can enter 10.20 in the Search text box.



If you want to modify the search after viewing the results, an asterisk is appended to the string in the *Search Criteria* pane that appears with the results. If you leave the asterisk in, the modified search will still return partial matches. You can remove the asterisk if you want the next set of results to match the string exactly.

SEARCH CRITERIA

Search for

10.2*

SEARCH AGAIN

Add an asterisk (*) to find all results that include a search string. For example: To find all IP addresses in the 10.2 range, enter 10.2.* To match your string exactly, do not add an asterisk.

☒ Include all words in each result.

SITE RESULTS

There are no records found.

ASSET GROUP RESULTS

There are no records found.

ASSET RESULTS

Address	Name	Site	Operating System			Vulnerabilities	Risk	Last Scan	Delete
10.2.0.11	machine11	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	
10.2.0.12	machine12	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	
10.2.0.15	machine15	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	
10.2.0.16	machine16	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	
10.2.0.18	machine18	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	
10.2.0.19	machine19	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	
10.2.0.2	machine2	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	
10.2.0.21	machine21	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	
10.2.0.26	machine26	Mock All-Vulns Scan	Microsoft 2003 Server SP2	257	254 7	17627	10,440,112	Feb 5th, 2013	

Searching with a partial string

If you precede a string with an asterisk, the search ignores the asterisk and returns results that match the string itself.

Certain words and individual characters, collectively known as *stop words* return no results, even if you enter them with asterisks. For better performance, search mechanisms do not recognize stop words. Some stop words are single letters, such as *a*, *i*, *s*, and *t*. If you want to include one of these letters in a search string, add one or more letters to the string. Following is a list of stop words:

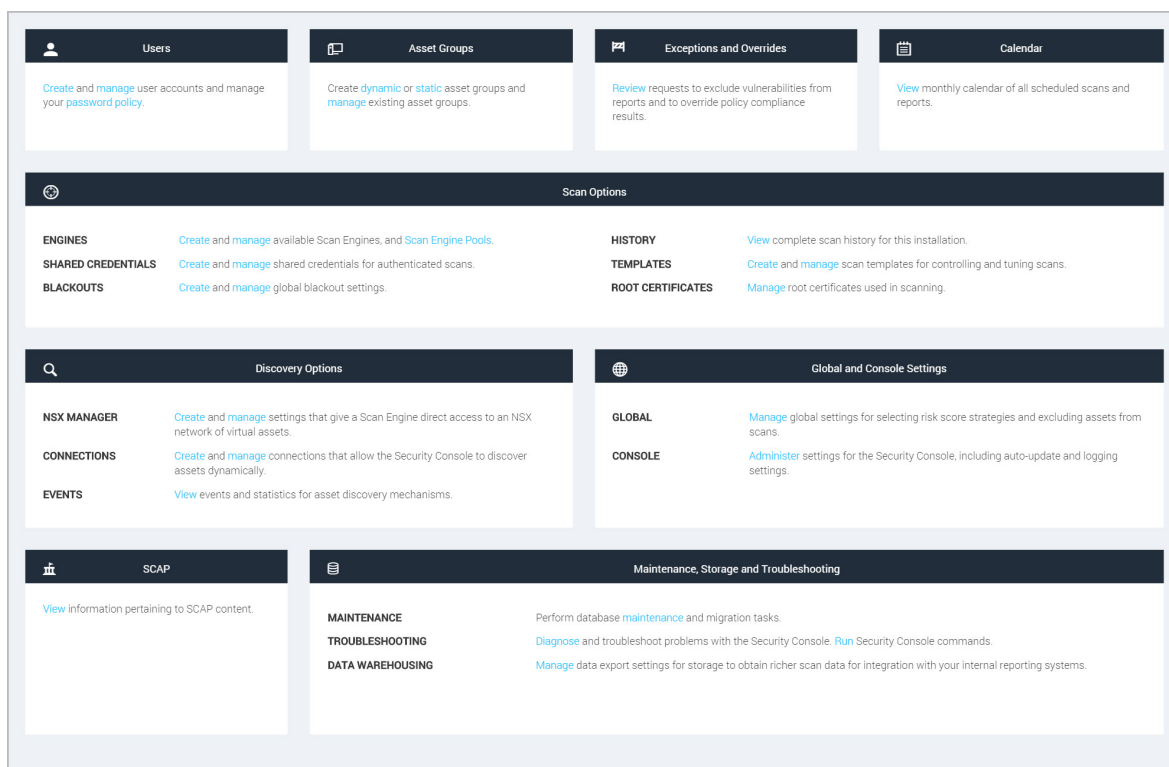
a	about	above	after	again	against	all	am	an	and
any	are	as	at	be	because	been	being	below	before
between	both	but	by	can	did	do	doing	don	does
down	during	each	few	for	from	further	had	has	have
having	he	her	here	hers	herself	him	himself	his	how
i	if	in	into	it	is	its	itself	just	me
more	most	my	myself	no	nor	not	now	of	off
on	once	only	or	other	our	ours	ourselves	out	over
own	s	same	she	should	so	some	such	t	than
that	the	their	theirs	them	themselves	then	there	these	they
this	those	through	to	too	under	until	up	very	was
we	were	what	when	where	which	while	who	whom	why
will	with	you	your	yours	yourself	yourselves			

Accessing operations faster with the Administration page

You can access a number of key Security Console operations quickly from the *Administration* page. To go there, click the **Administration** icon. The page displays a panel of tiles that contain links to pages where you can perform any of the following operations to which you have access:

- managing user accounts
- managing asset groups
- reviewing requests for vulnerability exceptions and policy result overrides
- creating and managing Scan Engines
- managing shared scan credentials, which can be applied in multiple sites
- viewing the scan history for your installation
- managing scan templates
- managing different models, or strategies, for calculating risk scores
- managing various activities and settings controlled by the Security Console, such as license, updates, and communication with Scan Engines
- managing settings and events related to discovery of virtual assets, which allows you to create dynamic sites
- viewing information related to Security Content Automation Protocol (SCAP) content
- maintaining and migrating the database
- troubleshooting the application
- using the command console to type commands
- managing data export settings for integration with third-party reporting systems

Tiles that contain operations that you do not have access to because of your role or license display a label that indicates this restriction.



Administration page

After viewing the options, select an operation by clicking the link for that operation.

Using configuration panels

The Security Console provides panels for configuration and administration tasks:

- creating and editing sites
- creating and editing user accounts
- creating and editing asset groups
- creating and editing scan templates
- creating and editing reports and report templates
- configuring Security Console settings
- troubleshooting and maintenance

Note: Parameters labeled in red denote required parameters on all panel pages.

Extending Web interface sessions

Note: You can change the length of the Web interface session. See *Changing Security Console Web server default settings* in the administrator's guide.

By default, an idle Web interface session times out after 10 minutes. When an idle session expires, the Security Console displays a logon window. To continue the session, simply log on again. You will not lose any unsaved work, such as configuration changes. However, if you choose to log out, you will lose unsaved work.

If a communication issue between your browser and the Security Console Web server prevents the session from refreshing, you will see an error message. If you have unsaved work, do not leave the page, refresh the page, or close the browser. Contact your Global Administrator.

Troubleshooting your activation

Your product key is your access to all the features you need to start using the application. Before you can begin using the application you must activate your license using the product key you received. Your license must be active so that you can perform operations like running scans and creating reports. If you received an error message when you tried to activate your license you can try the troubleshooting techniques identified below before contacting Technical Support.

Product keys are good for one use; if you are performing the installation for a second time or if you receive errors during product activation and these techniques have not worked for you, contact Technical Support.

Try the following techniques to troubleshoot your activation:

Did I enter the product key correctly?

- Verify that you entered the product key correctly.

Is there an issue with my browser?

- Confirm the browser you are using is supported. See *Using the Web interface* on page 24 for a list of supported browsers.
- Clear the browser cache.

Are my proxy settings correct?

- If you are using a proxy server, verify that your proxy settings are correct because inaccurate settings can cause your license activation to fail.
 - Go to the *Administration* page and click **Manage settings for the Security Console** to open the Security Console Configuration panel. Select Update Proxy to display the Proxy Settings section ensure that the address, port, domain, User ID, and password are entered correctly.
- If you are not using a proxy, ensure the **Name or address field** is specified as *updates.rapid7.com*. Changing this setting to another server address may cause your activation to fail. Contact Technical Support if you require a different server address and you receive errors during activation.

Are there issues with my network or operating system?

- By running diagnostics, you can find operating system and network issues that could be preventing license activation.
 - Go to the *Administration* page and click **Diagnose and troubleshoot problems with the Security Console**.
 - Select the OS Diagnostics and Network Diagnostics checkboxes.
 - Click **Perform diagnostics** to see the current status of your installation. The results column will provide valuable information such as, if DNS name resolution is successful, if firewalls are enabled, and if the Gateway ping returns a 'DEAD' response.
- Confirm that all traffic is allowed out over port 80 to updates.rapid7.com.
 - If you are using Linux, open a terminal and enter `telnet updates.rapid7.com 80`. You will see `Connected` if traffic is allowed.
 - If you are using Windows, open a browser and enter `http://updates.rapid7.com`. You should see a blank page.
 - White-list the IP address of the application server on your firewall so that it can send traffic outbound to `http://updates.rapid7.com`.
 - Make the same rule changes on your proxy server.
 - If you see an error message after adding the IP address to a white-list you will need to determine what is blocking the application.

Are there issues with firewalls in my network?

- Confirm that host-based firewall and antivirus detection are disabled on the system you are installing the application on. See *Using anti-virus software on the server* in the *administrator's guide* for more information.
- Ensure the IP address of the application server is white-listed through firewalls and content filters. This will allow you to reach the update server and pull down any necessary .jar files for activation and updates.

Have I tried everything?

- Restart the application, in some cases a browser anomaly can cause an error message that your activation failed. Restarting may be successful in those rare cases.

Scanning, viewing results, and reporting

Use this section to get started quickly by taking a three-step approach to vulnerability management:

1. **Discover on page 44:** To know what your security priorities are, you need to discover what devices are running in your environment and how these assets are vulnerable to attack. You discover this information by running scans.
2. **Assess on page 46:** After you discover all the assets and vulnerabilities in your environment, it is important to parse this information to determine what the major security threats are, such as high-risk assets, vulnerabilities, potential malware exposures, or policy violations.
3. **Act on page 51:** After you discover what is running in your environment and assess your security threats, you can initiate actions to remediate these threats.

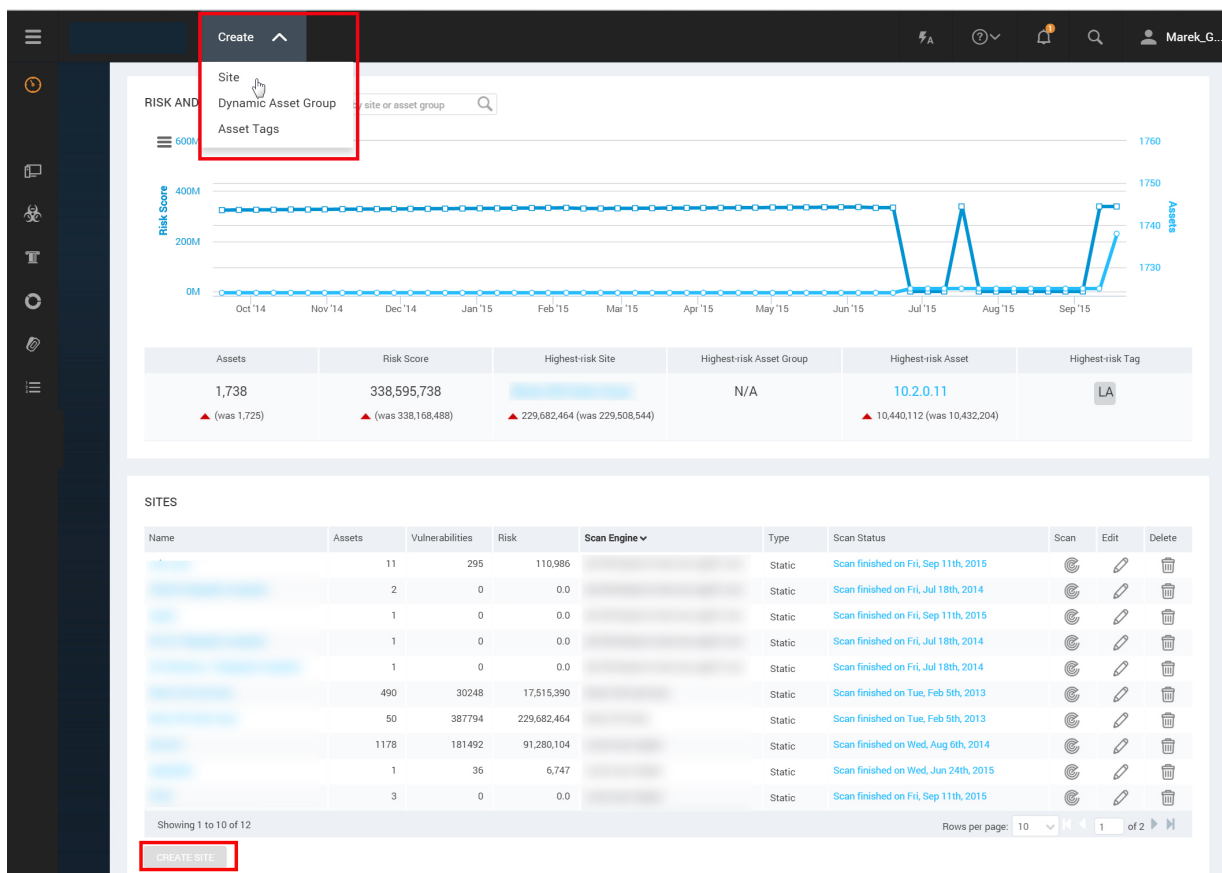
Discover

Find vulnerabilities in your environment.

Create a site

A site is a collection of assets to scan. You must have a site created before you run a scan.

1. On the *Home* page, click the **Create** tab at the top and then select *Site* from the drop-down list.
OR
Click the **Create Site** button at the bottom of the *Sites* table.



New static site button


2. On the **Info & Security** tab of the *Site Configuration* panel, enter a unique name for the site.
3. Click the **Assets** tab.
4. In the Include text box, enter host names, single IP addresses, or a range.
5. Click **Save**. The new site appears on in the *Site Listing* table of the *Home* page.

A site configuration also includes a scan template, which defines the settings for the scan. The default Full Audit without Web Spider template is good for first-time scans because it covers a large number of vulnerability checks. Click the **Templates** tab in the *Site Configuration* panel to see a list of scan templates.

Run a scan

Run a scan to discover assets and vulnerabilities.

1. Click **Scan** for the site you created.


SITES							
Name	Assets	Vulnerabilities	Risk	Scan Engine ▼	Type	Scan Status	Scan Edit Delete
vuln scan	11	295	110,986	ub1204-6aeu0-v0.dev.lax.rapid7.com	Static	Scan finished on Fri, Sep 11th, 2015	  

Site listing panel

2. In the *Start New Scan* window, click **Start now**.

Start New Scan dialog

3. The Security Console displays the page for your scan, so you can watch its progress as it discovers assets and vulnerabilities.

Full audit without Web Spider View all scans							
vuln scan View all sites							
SCAN PROGRESS							
Scan Type	Started	Assets	Vulnerabilities	Elapsed	Assets Scanned	Scan Engine	Download Log
Manual	9/18/2015 4:39 PM	11	64	4 minutes	<div> <div></div> <div>45.5%</div> </div> Active: 6, Pending: 0, Complete: 5	engine1	
<div>STOP SCAN PAUSE SCAN</div>							

Scan progress

4. You can confirm that the scan has completed by looking at the *Site Listing* table on the *Home* page.

SITES							
Name	Assets	Vulnerabilities	Risk	Scan Engine ▼	Type	Scan Status	Scan Edit Delete
vuln scan	11	297	111,010	ub1204-6aeu0-v0.dev.lax.rapid7.com	Static	Scan finished on Fri, Sep 18th, 2015	  

Scan status

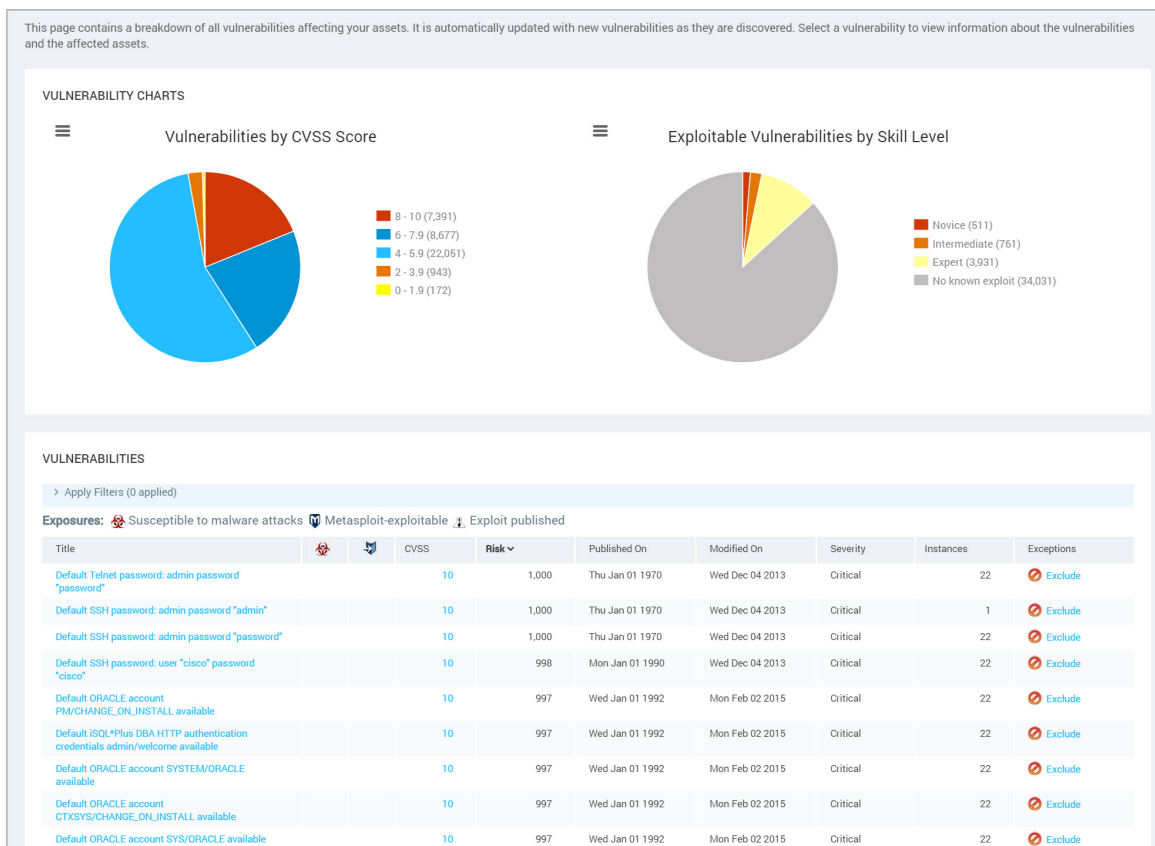
Assess

View and sort scan results to find out your security posture and remediation priorities.

You can drill down through scan data two different ways:

Option A

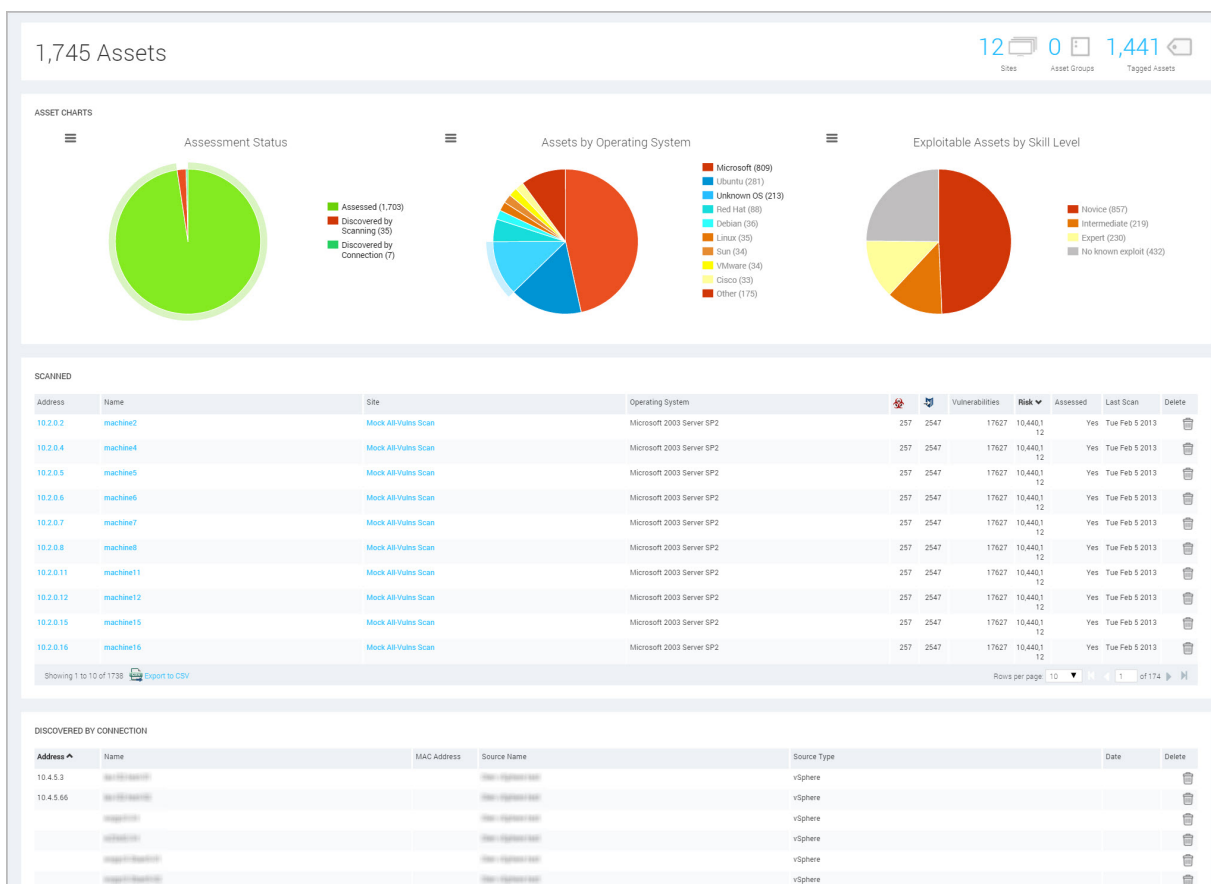
Click the **Vulnerabilities** icon to view and compare discovered vulnerabilities and then find out which assets are affected by each vulnerability. This approach is useful if you are concerned about specific vulnerabilities.



Vulnerabilities page

Option B

Click the **Assets** icon to see specific assets and then find out which vulnerabilities affect them. This approach is useful if you are concerned about certain sensitive assets. This guide shows the asset-based approach.



Assets panel

Using an asset-based approach

To see specific assets and find out which vulnerabilities affect them:

1. After a scan completes, click the **Assets** icon and drill down to the subset of assets that you want to see.

OPERATING SYSTEMS				
Operating System	Product	Vendor	Architecture	Instances
Unknown OS				213
Ubuntu Linux 12.04	Linux	Ubuntu	x86_64	148
Microsoft Windows 7 Enterprise Edition SP1	Windows 7 Enterprise Edition	Microsoft	x86_64	115
Microsoft Windows Server 2008 R2, Enterprise Edition SP1	Windows Server 2008 R2, Enterprise Edition	Microsoft	x86_64	60
Microsoft Windows Server 2012 Standard Edition	Windows Server 2012 Standard Edition	Microsoft	x86_64	49
Microsoft Windows 7 Enterprise Edition SP1	Windows 7 Enterprise Edition	Microsoft	x86	44
Ubuntu Linux 10.04	Linux	Ubuntu	x86_64	41
Microsoft Windows 7 Enterprise Edition	Windows 7 Enterprise Edition	Microsoft	x86_64	38
Microsoft Windows	Windows	Microsoft		36
Microsoft Windows 7 Professional Edition SP1	Windows 7 Professional Edition	Microsoft	x86_64	34

Showing 1 to 10 of 324 Rows per page: 10 1 of 33

Assets panel-Operating System Listing

2. Compare assets by different security metrics: Click column headings to sort assets by malware or exploit exposures, total vulnerabilities or risk scores.
3. Click an asset's IP address or host name to view details about it.

View all operating systems
The following assets are running Microsoft Windows Server 2008 R2, Enterprise Edition SP1

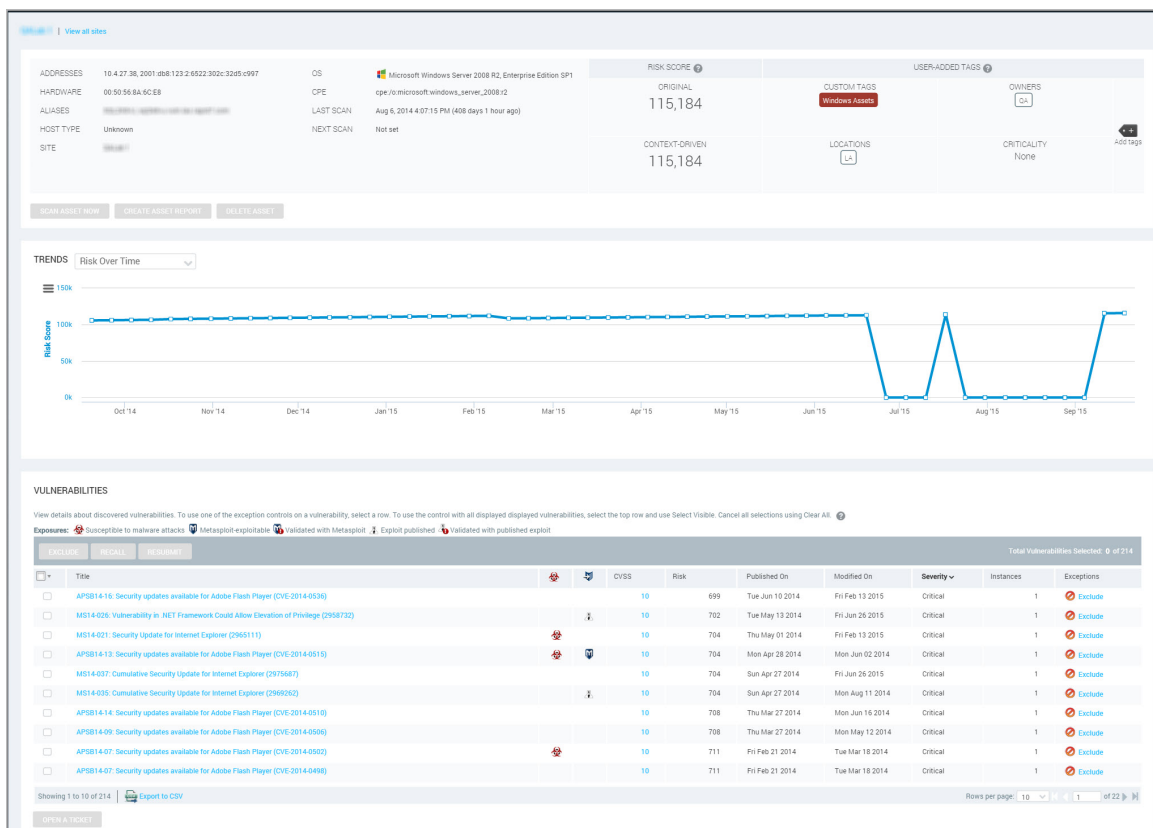
ASSETS

Address	Name	Site	Operating System	Malware	Exploit	Vulnerabilities	Risk	Last Scan
10.4.27.38	10.4.27.38	10.4.27.38	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	20	92	214	115,184	Aug 6th, 2014
10.4.25.31	10.4.25.31	10.4.25.31	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	20	92	203	107,550	Aug 6th, 2014
10.4.25.31	10.4.25.31	10.4.25.31	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	6	23	93	47,823	Aug 6th, 2014
10.4.24.89	10.4.24.89	10.4.24.89	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	1	15	58	32,386	Aug 6th, 2014
10.4.24.91	10.4.24.91	10.4.24.91	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	1	16	54	30,445	Aug 6th, 2014
10.4.27.247	10.4.27.247	10.4.27.247	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	0	1	26	14,003	Aug 6th, 2014
10.4.25.169	10.4.25.169	10.4.25.169	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	0	0	9	4,886	Aug 6th, 2014
10.4.24.114	10.4.24.114	10.4.24.114	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	0	0	9	4,549	Aug 6th, 2014
10.4.24.121	10.4.24.121	10.4.24.121	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	0	0	9	4,549	Aug 6th, 2014
10.4.24.120	10.4.24.120	10.4.24.120	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	0	0	8	4,193	Aug 6th, 2014

Showing 1 to 10 of 60 | Export to CSV | Rows per page: 10 | 1 of 6 |

Assets panel-Asset Listing table

4. View details about the asset, including all discovered vulnerabilities.
 - To sort vulnerabilities by name, click the **Title** heading in the *Vulnerability Listing* table.
 - To compare and prioritize vulnerabilities, click other column headings and sort them by different security metrics.



Asset properties page

- Click the name of a listed vulnerability to view details about it.

Vulnerability Listing						
Exposures: Susceptible to malware attacks Metasploit-exploitable Exploit published						
Title			CVSS	Risk	Instances	Published On
APSB11-18: Security update available for Adobe Flash Player (CVE-2011-2110)			10	919	1	Tue Jun 14 2011
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)			10	838	1	Thu Oct 23 2008

Vulnerabilities Listing panel

- The Security Console displays a page with details about the vulnerability, including its security metrics, affected assets, and remediation solutions.

VULNERABILITY INFORMATION

Title	Severity	Vulnerability ID	CVE	Published	Modified
APSB14-16: Security updates available for Adobe Flash Player (CVE-2014-0536)	Critical (10)	adobe-flash-apsb14-16-cve-2014-0536	10 (AV/N/AC/L/Au/N/C/C/C/A/C)	Jun 10, 2014	Feb 13, 2015

DESCRIPTION

Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

AFFECTS

Asset	Name	Site	Port	Status	Proof	Last Scan	Exceptions
10.4.27.38	10.4.27.38	10.4.27.38	-	Vulnerable Version	Vulnerable OS: Microsoft Windows Server 2008 R2, Enterprise Edition SP1 Vulnerable software installed: Adobe Flash 11.7.700.225	Aug 6th, 2014	Exclude

Showing 1 to 1 of 1

Export to CSV

Rows per page: 10 1 of 1

EXPLOITS

There are no exploits to display.

MALWARE KITS

There are no malware kits to display.

REFERENCES

Source	ID
BID	67961
CVE	CVE-2014-0536
URL	http://helpx.adobe.com/security/products/flash-player/apsb14-16.html

SOLUTION

Adobe Flash >= 11 and < 11.2.202.378 on Linux
Upgrade to Adobe Flash Player version 11.2.202.378 for Linux

Adobe Flash Player 11.2.202.378 can be downloaded from the [Flash Player Download Center](#), or from the [archived Flash Players page](#).

Adobe Flash >= 13 and < 13.0.0.223 on Apple Mac OS X
Upgrade to Adobe Flash Player version 13.0.0.223 for Mac OS X

Adobe Flash Player 13.0.0.223 can be downloaded from the [Flash Player Download Center](#), or from the [archived Flash Players page](#).

Adobe Flash >= 13 and < 13.0.0.223 on Microsoft Windows
Upgrade to Adobe Flash Player version 13.0.0.223 for Windows

Adobe Flash Player 13.0.0.223 can be downloaded from the [Flash Player Download Center](#), or from the [archived Flash Players page](#).

Adobe Flash >= 14 and < 14.0.0.125 on Apple Mac OS X
Upgrade to Adobe Flash Player version 14.0.0.125 for Mac OS X

Vulnerabilities overview

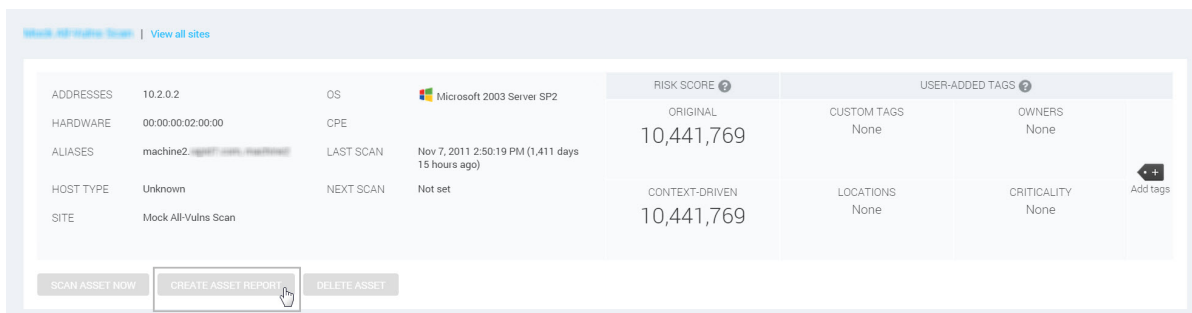
- Click the **Back** arrow on your browser to return to the asset details page.

Act

Create a report so that your organization can view its security posture and start to prioritize and remediate vulnerabilities.

Option A

If you want to share urgent information about a sensitive asset, click the **Create asset report** button on the page for that asset.



Create asset report

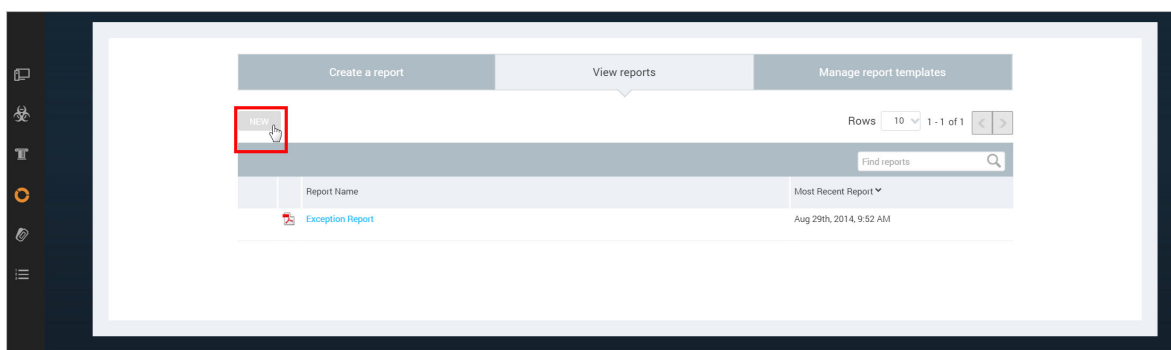
Option B

If you want to report on multiple assets, click the **Reports** icon. This guide shows the multiple-asset approach for creating an audit report in PDF format.

Using a multiple-asset based approach

For creating audit report in PDF format:

1. Click the **Reports** icon. The *Reports* page lists any reports that have been created.
OR
Click the **Create** tab at the top and then select *Site* from the drop-down list.
2. Click **New**.



Report panel—View Reports tab

3. Select the *Audit Report* template. Each template controls what specific information is included in the report.
4. Select the PDF format on the *Create a report* panel.

Create a report

View reports

Manage report templates

Name
Report time zone (GMT -0700) Pacific Time (US & Canada); Tijuana

Template

Document

Export

All

Search templates

1 Executive Summary

2 Trend Analysis

3 Executive Summary

Audit Report

Audit Report Copy

Baseline Comparison

Executive Overview

Displaying 4 of 22

See all

File format

PDF

Scope

Select Scan

Select Sites, Assets, Asset Groups or Tags

Filter report scope based on vulnerabilities

Frequency

Do not run a recurring report

Selecting the PDF report format

- Click **Select Sites, Assets, or Asset Groups** to view the *Select Report Scope* page.
- Select **Assets** from the drop-down list.

Select Report Scope

Report on the selected

Assets

Add filters to refine your search for scanned assets. For example, to find all assets running on a specific operating system, use the Operating system name filter. If you use multiple filters, choose whether you want the search to return assets that match all filter criteria or any criteria. Matching all criteria will produce a smaller, more specific set of results.

OS

contains

win

+

-

Match

all

 of the specified filters.

SEARCH

RESET

SELECT ALL DISPLAYED

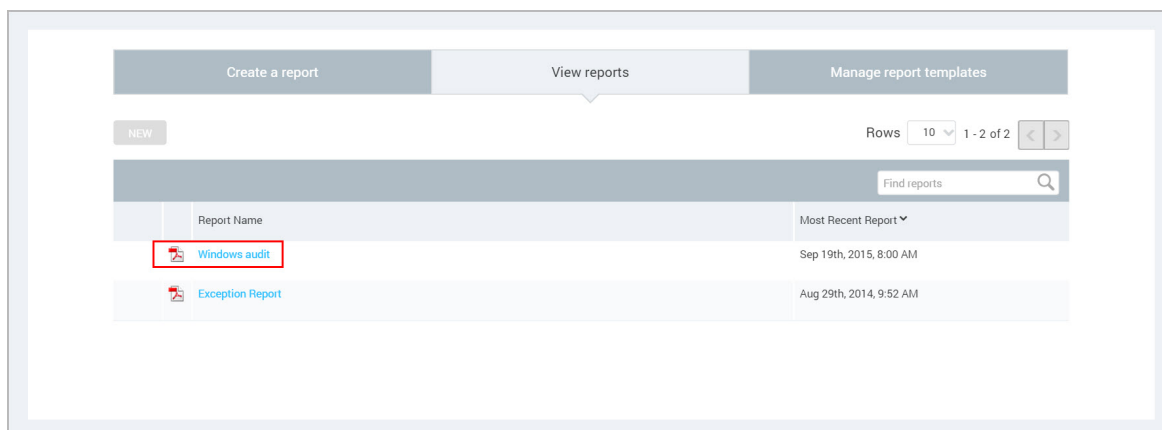
CLEAR ALL DISPLAYED

Total Selected 0

	Address	Name	Site	OS			Vulnerabilities	Risk Score	Last Scan
<input type="checkbox"/>	10.4.16.90	msedge-10.4.16.90-90		Microsoft Windows Server 2008 R2, Enterprise Edition SP1	0	3	5	2,169	Sep 11th, 2015
<input type="checkbox"/>	10.4.22.248	msedge-10.4.22.248-248		Microsoft Windows XP Professional SP3	0	0	0	0.0	Sep 11th, 2015
<input type="checkbox"/>	10.4.23.246	msedge-10.4.23.246-246		Microsoft Windows XP Professional SP3	0	0	0	0.0	Sep 11th, 2015
<input type="checkbox"/>	10.4.24.126	msedge-10.4.24.126-126		Microsoft Windows Server 2003, Enterprise Edition SP2	1	9	896	469,110	Aug 6th, 2014

Select Report Scope panel

7. Enter or select search criteria, and click **Search**. A list of assets is displayed.
8. Click check boxes for assets that you want to include in the reports, and click **Done**.
9. Click **Run the report** to generate the report. The Security Console displays the status of the report generation. When the report is complete, the creation date and time appear in the *View reports* page.
10. Click the report name to view the report.



Selecting a report

The report shows remediation steps for each vulnerability on each asset.

3.3.1. ICMP timestamp response (generic-icmp-timestamp)

Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
10.4.16.90	Able to determine remote system time.

References:

Source	Reference
CVE	CVE-1999-0524
OSVDB	95
XF	306

Source	Reference
XF	322

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

```
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

```
deny icmp any any 13
```

```
deny icmp any any 14
```

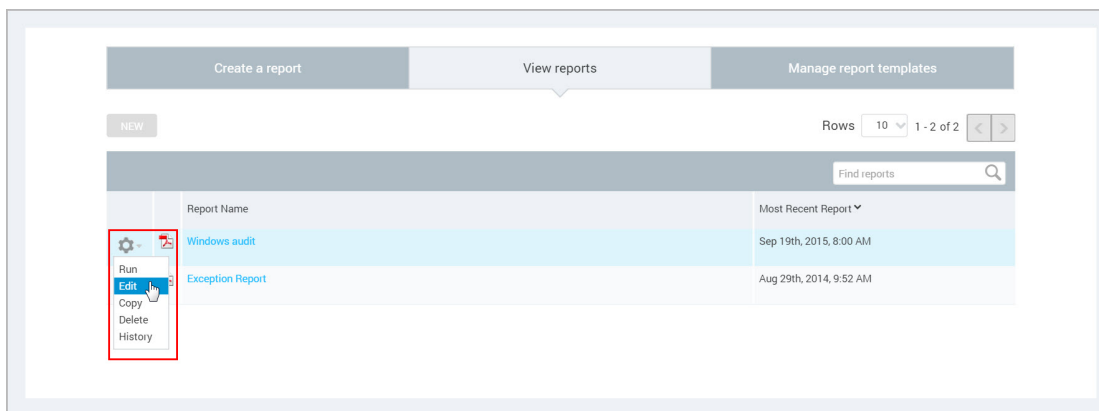
Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

```
permit icmp any any unreachable
```

Audit report-remediation steps

- Click the *View Reports* tab to access the report again, if you want to **Edit** it or **Generate** a new instance.

Tip: You can schedule reports to run automatically. This is useful if you create multiple sites and run scans on a regular basis. You can schedule reports to run after these scans are complete. To see scheduling options, select the **Run a reoccurring report** on a schedule option on the *Frequency* dropdown menu in the *Report Configuration* panel.



View reports tab-tools drop-down menu

Glossary

API (application programming interface)

An API is a function that a developer can integrate with another software application by using program calls. The term *API* also refers to one of two sets of XML APIs, each with its own included operations: API v1.1 and Extended API v1.2. To learn about each API, see the API documentation, which you can download from the *Support* page in Help.

Appliance

An Appliance is a set of InsightVM components shipped as a dedicated hardware/software unit. Appliance configurations include a Security Console/Scan Engine combination and an Scan Engine-only version.

Asset

An asset is a single device on a network that the application discovers during a scan. In the Web interface and API, an asset may also be referred to as a *device*. See *Managed asset* on page 63 and *Unmanaged asset* on page 70. An asset's data has been integrated into the scan database, so it can be listed in sites and asset groups. In this regard, it differs from a *node*. See *Node* on page 64.

Asset group

An asset group is a logical collection of managed assets to which specific members have access for creating or viewing reports or tracking remediation tickets. An asset group may contain assets that belong to multiple sites or other asset groups. An asset group is either static or dynamic. An asset group is not a site. See *Site* on page 69, *Dynamic asset group* on page 61, and *Static asset group* on page 69.

Asset Owner

Asset Owner is one of the preset roles. A user with this role can view data about discovered assets, run manual scans, and create and run reports in accessible sites and asset groups.

Asset Report Format (ARF)

The Asset Report Format is an XML-based report template that provides asset information based on connection type, host name, and IP address. This template is required for submitting reports of policy scan results to the U.S. government for SCAP certification.

Asset search filter

An asset search filter is a set of criteria with which a user can refine a search for assets to include in a dynamic asset group. An asset search filter is different from a *Dynamic Discovery filter* on page 61.

Authentication

Authentication is the process of a security application verifying the logon credentials of a client or user that is attempting to gain access. By default the application authenticates users with an internal process, but you can configure it to authenticate users with an external LDAP or Kerberos source.

Average risk

Average risk is a setting in risk trend report configuration. It is based on a calculation of your risk scores on assets over a report date range. For example, average risk gives you an overview of how vulnerable your assets might be to exploits whether it's high or low or unchanged. Some assets have higher risk scores than others. Calculating the average score provides a high-level view of how vulnerable your assets might be to exploits.

Benchmark

In the context of scanning for FDCC policy compliance, a benchmark is a combination of policies that share the same source data. Each policy in the Policy Manager contains some or all of the rules that are contained within its respective benchmark. See *Federal Desktop Core Configuration (FDCC)* on page 62 and *United States Government Configuration Baseline (USGCB)* on page 70.

Breadth

Breadth refers to the total number of assets within the scope of a scan.

Category

In the context of scanning for FDCC policy compliance, a category is a grouping of policies in the Policy Manager configuration for a scan template. A policy's category is based on its source, purpose, and other criteria. See *Policy Manager* on page 65, *Federal Desktop Core Configuration (FDCC)* on page 62, and *United States Government Configuration Baseline (USGCB)* on page 70.

Check type

A check type is a specific kind of check to be run during a scan. Examples: The Unsafe check type includes aggressive vulnerability testing methods that could result in Denial of Service on target

assets; the Policy check type is used for verifying compliance with policies. The check type setting is used in scan template configurations to refine the scope of a scan.

Center for Internet Security (CIS)

Center for Internet Security (CIS) is a not-for-profit organization that improves global security posture by providing a valued and trusted environment for bridging the public and private sectors. CIS serves a leadership role in the shaping of key security policies and decisions at the national and international levels. The Policy Manager provides checks for compliance with CIS benchmarks including technical control rules and values for hardening network devices, operating systems, and middleware and software applications. Performing these checks requires a license that enables the Policy Manager feature and CIS scanning. See *Policy Manager* on page 65.

Command console

The command console is a page in the Security Console Web interface for entering commands to run certain operations. When you use this tool, you can see real-time diagnostics and a behind-the-scenes view of Security Console activity. To access the command console page, click the **Run Security Console commands** link next to the *Troubleshooting* item on the *Administration* page.

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) is a standard for assigning unique identifiers known as CCEs to configuration controls to allow consistent identification of these controls in different environments. CCE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is a method for identifying operating systems and software applications. Its naming scheme is based on the generic syntax for Uniform Resource Identifiers (URI). CPE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) standard prescribes how the application should identify vulnerabilities, making it easier for security products to exchange vulnerability data. CVE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) is an open framework for calculating vulnerability risk scores. CVSS is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Compliance

Compliance is the condition of meeting standards specified by a government or respected industry entity. The application tests assets for compliance with a number of different security standards, such as those mandated by the Payment Card Industry (PCI) and those defined by the National Institute of Standards and Technology (NIST) for Federal Desktop Core Configuration (FDCC).

Continuous scan

A continuous scan starts over from the beginning if it completes its coverage of site assets within its scheduled window. This is a site configuration setting.

Coverage

Coverage indicates the scope of vulnerability checks. A coverage improvement listed on the News page for a release indicates that vulnerability checks have been added or existing checks have been improved for accuracy or other criteria.

Criticality

Criticality is a value that you can apply to an asset with a RealContext tag to indicate its importance to your business. Criticality levels range from *Very Low* to *Very High*. You can use applied criticality levels to alter asset risk scores. See *Criticality-adjusted risk*.

Criticality-adjusted risk

or

Context-driven risk

Criticality-adjusted risk is a process for assigning numbers to criticality levels and using those numbers to multiply risk scores.

Custom tag

With a custom tag you can identify assets by according to any criteria that might be meaningful to your business.

Depth

Depth indicates how thorough or comprehensive a scan will be. Depth refers to level to which the application will probe an individual asset for system information and vulnerabilities.

Discovery (scan phase)

Discovery is the first phase of a scan, in which the application finds potential scan targets on a network. Discovery as a scan phase is different from *Dynamic Discovery* on page 61.

Document report template

Document templates are designed for human-readable reports that contain asset and vulnerability information. Some of the formats available for this template type—Text, PDF, RTF, and HTML—are convenient for sharing information to be read by stakeholders in your organization, such as executives or security team members tasked with performing remediation.

Dynamic asset group

A dynamic asset group contains scanned assets that meet a specific set of search criteria. You define these criteria with asset search filters, such as IP address range or operating systems. The list of assets in a dynamic group is subject to change with every scan or when vulnerability exceptions are created. In this regard, a dynamic asset group differs from a static asset group. See *Asset group* on page 57 and *Static asset group* on page 69.

Dynamic Discovery

Dynamic Discovery is a process by which the application automatically discovers assets through a connection with a server that manages these assets. You can refine or limit asset discovery with criteria filters. Dynamic discovery is different from *Discovery (scan phase)* on page 61.

Dynamic Discovery filter

A Dynamic Discovery filter is a set of criteria refining or limiting Dynamic Discovery results. This type of filter is different from an *Asset search filter* on page 58.

Dynamic Scan Pool

The Dynamic Scan Pool feature allows you to use Scan Engine pools to enhance the consistency of your scan coverage. A Scan Engine pool is a group of shared Scan Engines that can be bound to a site so that the load is distributed evenly across the shared Scan Engines. You can configure scan pools using the Extended API v1.2.

Dynamic site

A dynamic site is a collection of assets that are targeted for scanning and that have been discovered through vAsset discovery. Asset membership in a dynamic site is subject to change if the discovery connection changes or if filter criteria for asset discovery change. See *Static site* on page 70, *Site* on page 69, and *Dynamic Discovery* on page 61.

Exploit

An exploit is an attempt to penetrate a network or gain access to a computer through a security flaw, or vulnerability. Malicious exploits can result in system disruptions or theft of data. Penetration testers use benign exploits only to verify that vulnerabilities exist. The Metasploit product is a tool for performing benign exploits. See *Metasploit* on page 64 and *Published exploit* on page 66.

Export report template

Export templates are designed for integrating scan information into external systems. The formats available for this type include various XML formats, Database Export, and CSV.

Exposure

An exposure is a vulnerability, especially one that makes an asset susceptible to attack via malware or a known exploit.

Extensible Configuration Checklist Description Format (XCCDF)

As defined by the National Institute of Standards and Technology (NIST), Extensible Configuration Checklist Description Format (XCCDF) “is a specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring.” Policy Manager checks for FDCC policy compliance are written in this format.

False positive

A false positive is an instance in which the application flags a vulnerability that doesn't exist. A false negative is an instance in which the application fails to flag a vulnerability that does exist.

Federal Desktop Core Configuration (FDCC)

The Federal Desktop Core Configuration (FDCC) is a grouping of configuration security settings recommended by the National Institute of Standards and Technology (NIST) for computers that are connected directly to the network of a United States government agency. The Policy

Manager provides checks for compliance with these policies in scan templates. Performing these checks requires a license that enables the Policy Manager feature and FDCC scanning.

Fingerprinting

Fingerprinting is a method of identifying the operating system of a scan target or detecting a specific version of an application.

Global Administrator

Global Administrator is one of the preset roles. A user with this role can perform all operations that are available in the application and they have access to all sites and asset groups.

Host

A host is a physical or virtual server that provides computing resources to a guest virtual machine. In a high-availability virtual environment, a host may also be referred to as a node. The term *node* has a different context in the application. See *Node* on page 64.

Latency

Latency is the delay interval between the time when a computer sends data over a network and another computer receives it. Low latency means short delays.

Locations tag

With a *Locations* tag you can identify assets by their physical or geographic locations.

Malware

Malware is software designed to disrupt or deny a target systems's operation, steal or compromise data, gain unauthorized access to resources, or perform other similar types of abuse. The application can determine if a vulnerability renders an asset susceptible to malware attacks.

Malware kit

Also known as an exploit kit, a malware kit is a software bundle that makes it easy for malicious parties to write and deploy code for attacking target systems through vulnerabilities.

Managed asset

A managed asset is a network device that has been discovered during a scan and added to a site's target list, either automatically or manually. Only managed assets can be checked for vulnerabilities and tracked over time. Once an asset becomes a managed asset, it counts against the maximum number of assets that can be scanned, according to your license.

Manual scan

A manual scan is one that you start at any time, even if it is scheduled to run automatically at other times. Synonyms include *ad-hoc scan* and *unscheduled scan*.

Metasploit

Metasploit is a product that performs benign exploits to verify vulnerabilities. See *Exploit* on page 62.

MITRE

The MITRE Corporation is a body that defines standards for enumerating security-related concepts and languages for security development initiatives. Examples of MITRE-defined enumerations include Common Configuration Enumeration (CCE) and Common Vulnerability Enumeration (CVE). Examples of MITRE-defined languages include Open Vulnerability and Assessment Language (OVAL). A number of MITRE standards are implemented, especially in verification of FDCC compliance.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The agency mandates and manages a number of security initiatives, including Security Content Automation Protocol (SCAP). See *Security Content Automation Protocol (SCAP)* on page 68.

Node

A node is a device on a network that the application discovers during a scan. After the application integrates its data into the scan database, the device is regarded as an *asset* that can be listed in sites and asset groups. See *Asset* on page 57.

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) is a development standard for gathering and sharing security-related data, such as FDCC policy checks. In compliance with an FDCC requirement, each OVAL file that the application imports during configuration policy checks is available for download from the *SCAP* page in the Security Console Web interface.

Override

An override is a change made by a user to the result of a check for compliance with a configuration policy rule. For example, a user may override a Fail result with a Pass result.

Payment Card Industry (PCI)

The Payment Card Industry (PCI) is a council that manages and enforces the PCI Data Security Standard for all merchants who perform credit card transactions. The application includes a scan template and report templates that are used by Approved Scanning Vendors (ASVs) in official merchant audits for PCI compliance.

Permission

A permission is the ability to perform one or more specific operations. Some permissions only apply to sites or asset groups to which an assigned user has access. Others are not subject to this kind of access.

Policy

A policy is a set of primarily security-related configuration guidelines for a computer, operating system, software application, or database. Two general types of policies are identified in the application for scanning purposes: *Policy Manager* policies and *standard* policies. The application's Policy Manager (a license-enabled feature) scans assets to verify compliance with policies encompassed in the United States Government Configuration Baseline (USGCB), the Federal Desktop Core Configuration (FDCC), Center for Internet Security (CIS), and Defense Information Systems Agency (DISA) standards and benchmarks, as well as user-configured custom policies based on these policies. See *Policy Manager* on page 65, *Federal Desktop Core Configuration (FDCC)* on page 62, *United States Government Configuration Baseline (USGCB)* on page 70, and *Scan* on page 67. The application also scans assets to verify compliance with standard policies. See *Scan* on page 67 and *Standard policy* on page 69.

Policy Manager

Policy Manager is a license-enabled scanning feature that performs checks for compliance with Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB), and other configuration policies. Policy Manager results appear on the *Policies* page, which you can access by clicking the **Policies** icon in the Web interface. They also appear in the *Policy Listing* table for any asset that was scanned with Policy Manager checks. Policy Manager policies are different from standard policies, which can be scanned with a basic license. See *Policy* on page 65 and *Standard policy* on page 69.

Policy Result

In the context of FDCC policy scanning, a result is a state of compliance or non-compliance with a rule or policy. Possible results include *Pass*, *Fail*, or *Not Applicable*.

Policy Rule

A rule is one of a set of specific guidelines that make up an FDCC configuration policy. See *Federal Desktop Core Configuration (FDCC)* on page 62, *United States Government Configuration Baseline (USGCB)* on page 70, and *Policy* on page 65.

Potential vulnerability

A potential vulnerability is one of three positive vulnerability check result types. The application reports a potential vulnerability during a scan under two conditions: First, potential vulnerability checks are enabled in the template for the scan. Second, the application determines that a target is running a vulnerable software version but it is unable to verify that a patch or other type of remediation has been applied. For example, an asset is running version 1.1.1 of a database. The vendor publishes a security advisory indicating that version 1.1.1 is vulnerable. Although a patch is installed on the asset, the version remains 1.1.1. In this case, if the application is running checks for potential vulnerabilities, it can only flag the host asset as being potentially vulnerable. The code for a potential vulnerability in XML and CSV reports is *vp* (vulnerable, potential). For other positive result types, see *Vulnerability check* on page 72.

Published exploit

In the context of the application, a published exploit is one that has been developed in Metasploit or listed in the Exploit Database. See *Exploit* on page 62.

RealContext

RealContext is a feature that enables you to tag assets according to how they affect your business. You can use tags to specify the criticality, location, or ownership. You can also use custom tags to identify assets according any criteria that is meaningful to your organization.

Real Risk strategy

Real Risk is one of the built-in strategies for assessing and analyzing risk. It is also the recommended strategy because it applies unique exploit and malware exposure metrics for each vulnerability to Common Vulnerability Scoring System (CVSS) base metrics for likelihood (access vector, access complexity, and authentication requirements) and impact to affected assets (confidentiality, integrity, and availability). See *Risk strategy* on page 67.

Report template

Each report is based on a template, whether it is one of the templates that is included with the product or a customized template created for your organization. See *Document report template* on page 61 and *Export report template* on page 62.

Risk

In the context of vulnerability assessment, risk reflects the likelihood that a network or computer environment will be compromised, and it characterizes the anticipated consequences of the compromise, including theft or corruption of data and disruption to service. Implicitly, risk also reflects the potential damage to a compromised entity's financial well-being and reputation.

Risk score

A risk score is a rating that the application calculates for every asset and vulnerability. The score indicates the potential danger posed to network and business security in the event of a malicious exploit. You can configure the application to rate risk according to one of several built-in risk strategies, or you can create custom risk strategies.

Risk strategy

A risk strategy is a method for calculating vulnerability risk scores. Each strategy emphasizes certain risk factors and perspectives. Four built-in strategies are available: *Real Risk strategy* on page 66, *TemporalPlus risk strategy* on page 70, *Temporal risk strategy* on page 70, and *Weighted risk strategy* on page 72. You can also create custom risk strategies.

Risk trend

A risk trend graph illustrates a long-term view of your assets' probability and potential impact of compromise that may change over time. Risk trends can be based on average or total risk scores. The highest-risk graphs in your report demonstrate the biggest contributors to your risk on the site, group, or asset level. Tracking risk trends helps you assess threats to your organization's standings in these areas and determine if your vulnerability management efforts are satisfactorily maintaining risk at acceptable levels or reducing risk over time. See *Average risk* on page 58 and *Total risk* on page 70.

Role

A role is a set of permissions. Five preset roles are available. You also can create custom roles by manually selecting permissions. See *Asset Owner* on page 57, *Security Manager* on page 69, *Global Administrator* on page 63, *Site Owner* on page 69, and *User* on page 71.

Scan

A scan is a process by which the application discovers network assets and checks them for vulnerabilities. See *Exploit* on page 62 and *Vulnerability check* on page 72.

Scan credentials

Scan credentials are the user name and password that the application submits to target assets for authentication to gain access and perform deep checks. Many different authentication mechanisms are supported for a wide variety of platforms. See *Shared scan credentials* on page 69 and *Site-specific scan credentials* on page 69.

Scan Engine

The Scan Engine is one of two major application components. It performs asset discovery and vulnerability detection operations. Scan engines can be *distributed* within or outside a firewall for varied coverage. Each installation of the Security Console also includes a local engine, which can be used for scans within the console's network perimeter.

Scan template

A scan template is a set of parameters for defining how assets are scanned. Various preset scan templates are available for different scanning scenarios. You also can create custom scan templates. Parameters of scan templates include the following:

- methods for discovering assets and services
- types of vulnerability checks, including safe and unsafe
- Web application scanning properties
- verification of compliance with policies and standards for various platforms

Scheduled scan

A scheduled scan starts automatically at predetermined points in time. The scheduling of a scan is an optional setting in site configuration. It is also possible to start any scan manually at any time.

Security Console

The Security Console is one of two major application components. It controls Scan Engines and retrieves scan data from them. It also controls all operations and provides a Web-based user interface.

Security Content Automation Protocol (SCAP)

Security Content Automation Protocol (SCAP) is a collection of standards for expressing and manipulating security data. It is mandated by the U.S. government and maintained by the National Institute of Standards and Technology (NIST). The application complies with SCAP criteria for an Unauthenticated Scanner product.

Security Manager

Security Manager is one of the preset roles. A user with this role can configure and run scans, create reports, and view asset data in accessible sites and asset groups.

Shared scan credentials

One of two types of credentials that can be used for authenticating scans, shared scan credentials are created by Global Administrators or users with the Manage Site permission. Shared credentials can be applied to multiple assets in any number of sites. See *Site-specific scan credentials* on page 69.

Site

A site is a collection of assets that are targeted for a scan. Each site is associated with a list of target assets, a scan template, one or more Scan Engines, and other scan-related settings. See *Dynamic site* on page 62 and *Static site* on page 70. A site is not an asset group. See *Asset group* on page 57.

Site-specific scan credentials

One of two types of credentials that can be used for authenticating scans, a set of single-instance credentials is created for an individual site configuration and can only be used in that site. See *Scan credentials* on page 68 and *Shared scan credentials* on page 69.

Site Owner

Site Owner is one of the preset roles. A user with this role can configure and run scans, create reports, and view asset data in accessible sites.

Standard policy

A standard policy is one of several that the application can scan with a basic license, unlike with a Policy Manager policy. Standard policy scanning is available to verify certain configuration settings on Oracle, Lotus Domino, AS/400, Unix, and Windows systems. Standard policies are displayed in scan templates when you include policies in the scope of a scan. Standard policy scan results appear in the *Advanced Policy Listing* table for any asset that was scanned for compliance with these policies. See *Policy* on page 65.

Static asset group

A static asset group contains assets that meet a set of criteria that you define according to your organization's needs. Unlike with a dynamic asset group, the list of assets in a static group does not change unless you alter it manually. See *Dynamic asset group* on page 61.

Static site

A static site is a collection of assets that are targeted for scanning and that have been manually selected. Asset membership in a static site does not change unless a user changes the asset list in the site configuration. For more information, see *Dynamic site* on page 62 and *Site* on page 69.

Temporal risk strategy

One of the built-in risk strategies, Temporal indicates how time continuously increases likelihood of compromise. The calculation applies the age of each vulnerability, based on its date of public disclosure, as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and asset impact (confidentiality, integrity, and availability). Temporal risk scores will be lower than TemporalPlus scores because Temporal limits the risk contribution of partial impact vectors. See *Risk strategy* on page 67.

TemporalPlus risk strategy

One of the built-in risk strategies, TemporalPlus provides a more granular analysis of vulnerability impact, while indicating how time continuously increases likelihood of compromise. It applies a vulnerability's age as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and asset impact (confidentiality, integrity, and availability). TemporalPlus risk scores will be higher than Temporal scores because TemporalPlus expands the risk contribution of partial impact vectors. See *Risk strategy* on page 67.

Total risk

Total risk is a setting in risk trend report configuration. It is an aggregated score of vulnerabilities on assets over a specified period.

United States Government Configuration Baseline (USGCB)

The United States Government Configuration Baseline (USGCB) is an initiative to create security configuration baselines for information technology products deployed across U.S. government agencies. USGCB evolved from FDCC, which it replaces as the configuration security mandate in the U.S. government. The Policy Manager provides checks for Microsoft Windows 7, Windows 7 Firewall, and Internet Explorer for compliance with USGCB baselines. Performing these checks requires a license that enables the Policy Manager feature and USGCB scanning. See *Policy Manager* on page 65 and *Federal Desktop Core Configuration (FDCC)* on page 62.

Unmanaged asset

An unmanaged asset is a device that has been discovered during a scan but not correlated against a managed asset or added to a site's target list. The application is designed to provide

sufficient information about unmanaged assets so that you can decide whether to manage them. An unmanaged asset does not count against the maximum number of assets that can be scanned according to your license.

Unsafe check

An unsafe check is a test for a vulnerability that can cause a denial of service on a target system. Be aware that the check itself can cause a denial of service, as well. It is recommended that you only perform unsafe checks on test systems that are not in production.

Update

An update is a released set of changes to the application. By default, two types of updates are automatically downloaded and applied:

Content updates include new checks for vulnerabilities, patch verification, and security policy compliance. Content updates always occur automatically when they are available.

Product updates include performance improvements, bug fixes, and new product features. Unlike content updates, it is possible to disable automatic product updates and update the product manually.

User

User is one of the preset roles. An individual with this role can view asset data and run reports in accessible sites and asset groups.

Validated vulnerability

A validated vulnerability is a vulnerability that has had its existence proven by an integrated Metasploit exploit. See *Exploit* on page 62.

Vulnerable version

Vulnerable version is one of three positive vulnerability check result types. The application reports a vulnerable version during a scan if it determines that a target is running a vulnerable software version and it can verify that a patch or other type of remediation has not been applied. The code for a vulnerable version in XML and CSV reports is *vv* (vulnerable, version check). For other positive result types, see *Vulnerability check* on page 72.

Vulnerability

A vulnerability is a security flaw in a network or computer.

Vulnerability category

A vulnerability category is a set of vulnerability checks with shared criteria. For example, the Adobe category includes checks for vulnerabilities that affect Adobe applications. There are also categories for specific Adobe products, such as *Air*, *Flash*, and *Acrobat/Reader*. Vulnerability check categories are used to refine scope in scan templates. Vulnerability check results can also be filtered according category for refining the scope of reports. Categories that are named for manufacturers, such as *Microsoft*, can serve as supersets of categories that are named for their products. For example, if you filter by the *Microsoft* category, you inherently include all Microsoft product categories, such as *Microsoft Path* and *Microsoft Windows*. This applies to other “company” categories, such as *Adobe*, *Apple*, and *Mozilla*.

Vulnerability check

A vulnerability check is a series of operations that are performed to determine whether a security flaw exists on a target asset. Check results are either negative (no vulnerability found) or positive. A positive result is qualified one of three ways: See *Vulnerability found* on page 72, *Vulnerable version* on page 71, and *Potential vulnerability* on page 66. You can see positive check result types in XML or CSV export reports. Also, in a site configuration, you can set up alerts for when a scan reports different positive results types.

Vulnerability exception

A vulnerability exception is the removal of a vulnerability from a report and from any asset listing table. Excluded vulnerabilities also are not considered in the computation of risk scores.

Vulnerability found

Vulnerability found is one of three positive vulnerability check result types. The application reports a vulnerability found during a scan if it verified the flaw with asset-specific vulnerability tests, such as an exploit. The code for a vulnerability found in XML and CSV reports is *ve* (vulnerable, exploited). For other positive result types, see *Vulnerability check* on page 72.

Weighted risk strategy

One of the built-in risk strategies, Weighted is based primarily on asset data and vulnerability types, and it takes into account the level of importance, or weight, that you assign to a site when you configure it. See *Risk strategy* on page 67.