Skybox

Reference Guide

10.1.300

Revision: 11

Contact information

Contact Skybox using the form on our website or by emailing info@skyboxsecurity.com

Customers and partners can contact Skybox technical support via the Skybox Support portal

Contents

Preface

Intended Audience

The *Skybox Reference Guide* is the reference companion to the *Skybox Firewall Assurance User Guide*, the *Skybox Network Assurance User Guide*, the *Skybox Vulnerability Control User Guide*, the *Skybox Threat Manager User Guide*, and the *Skybox Change Manager User Guide*.

The intended audience is readers of the User Guides who want additional technical and in-depth information.

How this manual is organized

This manual:

- Contains reference information about Skybox, including the configuration of components and devices
- Provides descriptions of the properties of analyses, tasks, and model entities
- Defines access, dependency, and routing rules

The manual includes the following parts:

Related documentation

The following documentation is available for Skybox:

- *Skybox Installation and Administration Guide*
- *Skybox Developer Guide*
- *Skybox Release Notes*

The entire documentation set (in PDF format) is available here

Note: If you are not using the latest version of Skybox, you can find the documentation for your version at `http://downloads.skyboxsecurity.com/files/Installers/Skybox_View/<your major version/<your minor version>/Docs`. For example, `http://downloads.skyboxsecurity.com/files/Installers/Skybox_View/10.0/10.0.600/Docs`

You can access a comprehensive Help file from any location in Skybox Manager by using the **Help** menu or by pressing **F1**.

Technical support

You can contact Skybox using the form on our website or by emailing info@skyboxsecurity.com

Customers and partners can contact Skybox technical support via the Skybox Support portal

When you open a case, you need:

- Your contact information (telephone number and email address)
- Skybox version and build numbers
- Platform (Windows or Linux)
- Problem description
- Any documentation or relevant logs

  You can compress logs before attaching them by using the Pack Logs tool (see Packing log files for technical support, in the Skybox Installation and Administration Guide).

Part I: Tasks

This part describes Skybox tasks and their properties.

Chapter 1

Managing tasks

This chapter gives an overview of how to set up and use Skybox tasks.

In this chapter

REQUIREMENTS

Python

Many collection tasks use scripts that are written in Python; to import device data to a Skybox model, Python version 2.7 or higher must be installed on the machine that is running the task (as specified by the **Run in** field of the task).

- If the Skybox Collector or Skybox Server for these tasks is running on a Skybox Appliance, you can install Python using an **Install Python Tools for Skybox Appliance** task (see Python installation task (on page 12)).
- To install Python manually, see Installing Python manually (on page 13).

Note: Some collection tasks require the installation of additional Python packages. These requirements are documented in the individual tasks.

SSH

The connection type between a Skybox Collector and a device is provided in the documentation of each task.

If the connection is over SSH, the Skybox Collector can only use a Diffie-Hellman key of up to 2048 bits. Collection from a remote device that uses a larger key will fail.

Python installation task

The **Install Python Tools for Skybox Appliance** task installs the Python infrastructure that is required by many collection tasks. The requirement for Python is documented in the individual tasks.

Run this task once only for each Skybox Collector and Skybox Server running on a Skybox Appliance that is used for these tasks.

Task properties

The properties that control **Install Python Tools for Skybox Appliance** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to install Python.
Python version	The version of Python to install.
Advanced tab	
Location Hint	The location of the Skybox Server or Collector on which to install Python. **Note**: Use this property if different locations use the same set of IP addresses, so that devices running Skybox components at different locations can have the same IP address.

Installing Python manually

> Note: If you are using Skybox Appliance, you can install Python by running an **Install Python Tools for Skybox Appliance** task (see Python installation task (on page 12)).

To download and install Python on Skybox

1. (If C++ is not installed on the Skybox Server machine) Install C++ by running `yum groupinstall "Development Tools"`
2. Download and install Python from https://www.python.org/downloads/
3. If you did not install Python to the default location, specify the location of the Python executable in `<Skybox_Home>\<component>\conf\sb_common.properties` (`<component>` is `server` or `collector`, depending on the value of the **Run in** field):
   - (Windows) `ScriptTask.WIN.PYTHON_EXEC`
   - (Linux) `ScriptTask.LINUX.PYTHON_EXEC`

USER ROLES AND TASKS

Only **Admins** and **Users** have access to the Operational Console where Skybox tasks are managed.

Admins can create, manage, and run all tasks.

Users can view tasks that add information to the model, delete information from the model, or save the model. They can create, manage, and run:

- All analysis tasks
- All report tasks, including CSV export tasks and XML vulnerability occurrence export tasks
- Ticket creation tasks
- Copy model tasks (which copy model data from one model to another)

WORKING WITH TASKS

The Task dialog box is described in Task properties (on page 18).

For information about the properties specific to each Skybox task, see the section relating to the task.

Tip: If you mouse over a field, a tooltip listing the values selected for that field appears. This is especially useful for fields of the Properties pane that hold multiple values.

To open the operational console

1 On the toolbar, click Operational Console.

The Operation Console is set up the same way as Skybox Manager, with a tree on the left and a workspace on the right.

2 Navigate to **Tasks** > **All Tasks** to display a list of existing tasks.

To create a Skybox task

› On the Operational Console toolbar, click New Task.

To create a Skybox task based on an existing task

1 In the Operational Console tree, select **Tasks** > **All Tasks**.

The workspace lists all tasks defined for this model.

2 Right-click a task and select **Create Task Like**.

A Task Properties dialog box containing a copy of the selected task appears.

To edit a task

1 In the Operational Console tree, select **Tasks** > **All Tasks**.

The workspace lists all tasks defined for this model.

2 Double-click a task to open its Task Properties dialog box.

3 You can:

- Change the task name
- Add a timeout for the task
- Edit task properties
- Enable the task to run according to a predefined schedule (by selecting the **Enable Auto-launch** property)

  Auto-launch is enabled for all new tasks. Predefined tasks can all be run manually but, as a precautionary measure, auto-launch is disabled.

To run a task manually

› Select the task in the Table pane and click Launch.

Task sequences

In a task sequence, each task in the sequence runs as soon as the previous task ends. This is useful when you often want to run a set of tasks in a specific order.

You can use separate task sequences for different purposes, different parts of the system, and different frequencies.

A task sequence can include task groups (on page 17). The tasks in a task group are run in parallel.

Creating task sequences

A task sequence is an ordered series of tasks. If the outcome of the previous task (the *triggering task*) is not what you specified, the next task and all subsequent tasks are not launched.

Note: Before you create a task sequence, define the tasks that are to run in the sequence.

To create a task sequence

1 On the Operational Console toolbar, click New Task Sequence.

2 Type a **Name** for the sequence; leave **Basic** selected as the type of the task sequence.

3 Click **Next**.

4 In the Tasks pane, click **Add**.

5 Select a task to add to the sequence and click **OK**.

The task is added as the 1st task in the task sequence.

6 Add additional tasks to the task sequence:

a. Click **Add**.

b. Select a task to add to the sequence.

A dependency is created so that this task runs after the previous task finishes with any of the specified exit codes.

Note: A task can only be used once per task sequence. However, you can use several different tasks of the same type.

c. To change the triggering task, select a different task in the **Depends on Task** field.

d. To change the exit codes (on page 16) of the triggering task, click the **Browse** button next to the **Depends on Exit Codes** field.

If the triggering task ends with a different exit code, the dependent task is not triggered.

7 Click **Next**.

The Firewall Filters page enables you to change the firewall filter values of the firewall collection or analysis tasks in your task sequence. If there are no tasks of these types, all the parameters are disabled. If there are any tasks, you can keep the original firewall filters for the tasks or change the set of firewalls on which the tasks are to run (to recently changed firewalls or new firewalls).

8 If your task sequence includes any firewall collection or analysis tasks, you can modify the values.

9 Click **Next**.

10 Schedule the task sequence (see page 17) to run as often as necessary.

11 Click **Finish**.

Creating similar task sequences

After a task sequence for a set of tasks is created, you can use it as a template for similar task sequences: Right-click the task sequence and select **Create Task Sequence Like**.

Task exit codes

The following table lists the task exit codes for all Skybox tasks.

Exit code	Description
Success	The task completed successfully.
Success (No Update)	The task completed but no data was updated. (Used only for **Dictionary Update** tasks when no update was available.)
Warning	The task was partially successful. For example, a task to collect 5 firewalls was only able to collect 3 of them. You can get more information from the warning messages.
Error	The task failed. You can get more information from the error messages.
Fatal	The task failed with a fatal error. For example, the configuration files being collected are corrupt.
Time Out	The task did not finish because no data or response was received by the time the task reached its timeout.
Terminated	The user aborted or terminated the task.

Viewing and editing task sequences

To view task sequences

1 In the Operational Console tree, select **Tasks** > **Task Sequences**.

2 Select a task sequence.

Tasks in the sequence are listed in the Table pane and general information or messages from the most recent run of the selected task in the Details pane.

Editing task sequences

You can add tasks to and remove tasks from a sequence and change the order of the tasks in the sequence and the exit conditions for the triggering task.

To edit a task sequence

› Right-click the task sequence in the tree and select **Properties**.

Scheduling task sequences

You can schedule a task sequence (or a task) so that it runs at specific times. Although sequences are usually scheduled to run on the Live model, you can schedule them to run on any model.

Note: We recommend that you group tasks into sequences rather than run or schedule individual tasks.

To schedule a task sequence (or task)

1 Locate the task sequence in the Operational Console tree.

2 Double-click the task sequence.

3 In the <Task name> Properties dialog box, click the **Schedule** tab.

4 For each schedule:

   a. Click **Add** to open the New Task Schedule dialog box.

   b. Select a time slice and fill in the corresponding fields.

   c. If the task sequence is to run a limited number of times, select **End after** and type the number of times that it is to run.

   d. If necessary, in the **Model** field, change the model on which the task sequence runs.

   e. Click **OK**.

   The new schedule is added to the list of schedules for this task sequence.

5 Click **OK**.

Note: If auto-launch is not enabled for a task, it does not run on its specified schedules. However, it does run as part of a task sequence.

To view scheduled tasks and sequences

› In the Operational Console tree, select **Tasks** > **Schedules**.

Defined schedules are listed in the Table pane and the scheduled entities are listed in separate tabs (**Tasks** and **Sequences**) in the Details pane.

Task groups

You can group a set of tasks together so that you can run them as part of a task sequence (see page 14).

When you create a task group, Skybox creates a separate folder for the group.

Note: You can only run a whole task group as part of a task sequence. Otherwise, launch or schedule each task separately. When run as part of a task sequence, the tasks in a task group run in parallel.

To create a task group

1 On the Operational Console tree, right-click **Task Groups**.

2 In the New Task Group dialog box:

   a. Type a name for the group.

   b. In the **User Comments** field, type a description of the group.

c. To select tasks to include in this group, click the **Browse** button next to the **Tasks** field.

d. Click **OK**.

   A folder for this group is added under the **Task Groups** node.

Monitoring task results

Task messages

After running a task, you can check the task results to make sure that the outcome is what you expected. For example, after updating firewall configurations (using tasks), check the task results to confirm that all data was imported into Skybox. Check for failed tasks; if a task failed, find out why it failed, make the necessary changes, and rerun the updated task for the failed firewall.

You can view a list of tasks that failed in the Operational Console window, at **Tasks** > **Failed Tasks**. For each task, you can see the messages from the task's most recent run.

Task alerts

You can set up Skybox to send email alerts to specific users for failed tasks. You can configure global settings and you can configure settings in the task properties of a task. By default, tasks alerts are sent for each task that runs. However, if you do not want task alerts sent for a task, you can disable them in the task properties.

To configure global task alerts

1 Navigate to **Tools** > **Options** > **Server Options** > **Task Settings** > **Task Alert Settings**.

2 In the **Email to** field:

- Type the email addresses to which alerts are to be sent.

  Multiple addresses must be comma-separated, with no space between the comma and the following address.

- Click the **Browse** button; select Skybox users who are to receive alerts and add the external email addresses of other desired recipients.

All alerts are sent to each specified recipient.

3 Modify:

- **Email on:** The exit codes on which to send task alerts.
- **Messages Count**: The maximum number of messages from the failed task to include in the task alert.

4 Click **OK**.

TASK PROPERTIES

The Task Properties dialog box contains the following tabs:

- **General**: This tab, described in General task properties (on page 19), contains the fields that define the selected task.

- **Alerts**: Use this tab, described in Task alert properties (on page 19), to define when and where alerts are sent for the task.
- **Comments**: This tab, which is the same for all tasks, contains your description of the task. We strongly recommend that you add a description (this does not affect the task).

  When the **Task** table is displayed in the Operational Console, view comments by showing the **User Comments** column.

- **Schedule**: This tab is the same for all tasks. You schedule the launching of the task in this tab. See Scheduling task sequences (on page 17).

General task properties

The **General** tab of the Task Properties dialog box consists of 2 panes:

- General: This pane, described in the following table, is the same for all tasks.
- Properties: This pane contains properties specific to each task. These properties are described in the task-specific sections.

Property	Description
Name	A name that you assign to the task.
Task Type	The task type. Task types are grouped into folders and can be filtered by typing a partial string. You can modify this property for new tasks only.
Collector	The Skybox Collector to be used by the task.
Timeout	Specifies whether the task has a timeout limit.
Hours	This field is enabled only if you select **Timeout**. The hours portion of the task timeout limit.
Minutes	This field is enabled only if you select **Timeout**. The minutes portion of the task timeout limit.
Show Properties Dialog Before Launch	This field is displayed only when working with Skybox Vulnerability Control. Specifies whether to open the task Properties dialog box before the task is launched.
Enable Auto-launch	Specifies whether to launch the task according to the schedules that are specified in the **Schedule** tab.

Task alert properties

Use the **Alerts** tab of the Task Properties dialog box to define who receives alerts for a task, and under what exit conditions. You can either use the global settings (from **Tools** > **Options** > **Server Options** > **Task Settings** > **Task Alert Settings**) or define specific settings.

Property	Description
Enable Task Alerts	Specifies whether to send task alerts for this task.

Property	Description
Include task messages in alert	This field is enabled only if you select **Enable Task Alerts**. Specifies whether to include the messages from the task in the alerts.
Email To	These fields are enabled only if you select **Enable Task Alerts**. Specifies the users to whom task alerts are sent: • **Use Global Settings**: Sends task alerts to the users specified in the global settings. • **Specific**: Sends task alerts to the specified users and email addresses.
Exit Codes	These fields are enabled only if you select **Enable Task Alerts**. Specifies on which exit codes task alerts are sent for this task: • **Use Global Settings**: Sends task alerts according to the exit codes specified in the global settings. • **Specific**: Sends task alerts according to the exit codes specified here for this task.

TASK MESSAGES

While a task is running there is a check mark in the **Running** column and the status bar of the Skybox Manager window displays a “Currently 1 task is running” message. After a task starts, the **Messages** tab of the Details pane shows all the messages generated by the task. Messages are always available for the most recent run of a task.

DEVICE ACCESS MANAGEMENT

For some tasks, you can instruct Skybox to take user name and password pairs from a repository instead of typing this data in fields in the Task Properties dialog box.

In many organizations, the same user name and password combination accesses multiple devices of 1 type. For example, there might be one user name and password to access Cisco routers in London and another combination to access the Cisco routers in New York. **Admins** can configure Skybox so that each user name and password combination is saved by Skybox and can be used by online collection tasks for devices of the specified type and scope.

This section contains information about setting up access for multiple devices.

Creating access tokens

In Skybox, each combination of user name and password for a set of devices is referred to as an *access token*. Only **Admins** can create (and manage) these access tokens, which are used by some online collection tasks.

For devices that require an admin user name and password combination, create 2 access tokens; a regular token (of type **<Device type>**) for the regular user name and password, and a separate token (of type **<Device type> Admin**) for the admin combination.

The online collection tasks that can use access tokens are listed in the following table.

Collection task	Token type
Routers – Cisco IOS	Cisco, Cisco Admin
Routers – Nortel Passport	Nortel Passport

To create an access token

1 Select **Tools** > **Administrative Tools** > **Device Access Management**.

2 In the Device Access Management dialog box, click **Add**.

3 In the New Access Token dialog box:

a. Type a **Device Name** for the access token.

b. In the **Field Type** field, select the device type.

Cisco IOS routers, which require an admin user name and password combination, require 2 access tokens; a token for a regular user whose **Type** is the device name type (**Cisco**) and another token for the admin user name and password combination whose **Type** has the string Admin appended to the name (**Cisco Admin**).

c. In the **Username** field, type the user name for this set of devices. For admin-type access tokens, type the admin user name.

d. In the **Password** and **Confirm Password** fields, type the password for this set of devices. For admin-type access tokens, type the admin password.

e. If necessary, click the **Browse** button next to the **Scope** field to limit the scope of the device set.

f. Click **OK** to save the new device access token.

How to use access tokens

After creating access tokens, you can use them in online collection tasks. Each access token type matches 1 type of collection. Admin-type access tokens are used when required.

Note: Access tokens are only used if you select **Use Access Tokens** in the Properties dialog box of the task.

If you select **Use Access Tokens**, Skybox checks the access tokens to find those that match the scope and type of the task.

- Access tokens that do not match either the scope or the type of the task are not used. For example, if there is 1 access token for Cisco routers in London and 1 for Cisco firewalls in London, a router collection task uses the router-type access token and a firewall collection task uses the firewall-type access token.
- If multiple access tokens match a task, the task uses the best match (the token with the most specific range).

For example, you create a collection task for a device with the IP address `192.170.1.127`; an access token with a range of `192.168.0.0-192.172.0.0` matches the task, but an access token with a range of `192.170.0.0-192.170.2.0` is a more specific match and is used by the task.

USING CYBERARK FOR DEVICE PASSWORD MANAGEMENT

CyberArk is a tool that enables passwords to be centrally stored, logged, and managed.

Many collection tasks can be authenticated with CyberArk, as documented in the individual tasks.

You must configure CyberArk (see page 22) so that Skybox tasks can retrieve device authentication credentials from CyberArk.

Configuring CyberArk for device credentials retrieval

CyberArk configuration workflow

1. Install the CyberArk client on machines running Skybox Collectors that connect to devices using authentication credentials stored in CyberArk.

   The CyberArk client creates a user named `Prov_<machine name>`.

2. Creating the CyberArk environment for Skybox requires a user with the following permissions:

   - Add/Update Users
   - Add Safes

     Only required if you are creating a separate safe for device authentication credentials required by Skybox collection tasks.

   - Audit Users

   We recommend that you create a separate user for this purpose.

3. Log in to CyberArk.

4. In the Privileged Identity Management window:

   a. Create a CyberArk application.

      Skybox uses the ID (name) of this application to connect to CyberArk.

   b. (Recommended) Create a separate safe in your CyberArk vault to contain all device authentication credentials required by Skybox collection tasks.

      Store CyberArk objects for Skybox collection tasks in this safe.

      When you create a Skybox collection task, type the name of the safe in the **Safe** field of the task.

   c. (*Not* recommended) Create a CyberArk folder.

      By default, objects are stored in the **Root** folder. We recommend that you do not change this.

   d. Create a CyberArk policy ID.

      The policy ID tells CyberArk how to connect to the devices.

   e. Create a CyberArk object (*account*).

If necessary, create separate objects for different devices or device types.

When you create a Skybox collection task, type the name of the object in the **Object** field of the task.

5 Configure Skybox to work with CyberArk.

The predefined directory for CyberArk is **Root** and the predefined application ID for connecting from Skybox is **SkyboxSecurity**. If you change these in CyberArk, change them in Skybox (**Tools** > **Options** > **Server Options** > **Task Settings** > **Global Task Settings** as well; see the Global Task Settings topic in the Skybox Installation and Administration Guide).

To create a CyberArk application

1 Select **Applications** from the drop-down list at the top of the Privileged Identity Management window.

2 Click **Add Application** on the toolbar.

3 Fill in the fields in the Add Application dialog box and click **Add**.

The predefined application ID (name) in product is **SkyboxSecurity**; we recommend that you use this.

4 (Recommended) Add CyberArk application security options:

- The IP address of the Skybox Server:

  a. Select the **Allowed Machines** tab.

  b. Click **Add**.

  c. In the Add allowed machine dialog box, type the IP **Address** of the Skybox Server.

  d. Click **Add**.

- The operating system user of the Skybox Server:

  a. Select the **Authentication** tab.

  b. Select **Add** > **OS user**.

  c. In the Add Operating System User Authentication dialog box, type the operating system user:

  (If you installed the Skybox Server as a service) **skyboxview**

  (If you did not install the Skybox Server as a service) The installation user (for example, **skybox\<user name>**)

- Path authentication:

  a. Select the **Authentication** tab.

  b. Select **Add** > **Path**.

  c. In the Add Path Authentication dialog box, select **Path is folder** and type the path to JBoss on the Skybox Server (`<Skybox_Home>\thirdparty\jboss`).

To create a CyberArk safe

1. Select **Safes** from the drop-down list at the top of the Privileged Identity Management window.
2. Click **Add Safe** on the toolbar.
3. Define the safe. You need the name of the safe when you define collection tasks in Skybox.
4. In the **Members** tab of the safe, click **Add Members**.
5. In the Add Safe Member dialog box, select a CyberArk client user (`Prov_<machine name>`) created when you installed the CyberArk client (if necessary, use the Search option in the dialog box), and click **Add**.
6. Repeat the previous 2 steps to add the application that you created in the preceding procedure and, if necessary, any additional CyberArk client users (if you are using multiple Skybox Collectors).

To create a CyberArk policy ID

1. Navigate to **System configuration** > **Policies** > **Devices** > **Network Devices**.
2. Right-click **Policies** and select **Add Policy**.
3. Type a descriptive **ID** (name) for the policy.

   You need this ID when you create CyberArk objects.
4. Expand the policy and select **Properties** > **Required**.
5. Add a mandatory property: Right-click and select **Add property**. Set **Name** and **Display Name** to **Username**.
6. Add a mandatory property: Right-click and select **Add property**. Set **Name** and **Display Name** to **Password**.

To create a CyberArk object

1. Select **Accounts** from the drop-down list at the top of the Privileged Identity Management window.
2. Click **Add Account** on the toolbar.
3. Define the account; use the safe and policy ID created in the preceding procedures. (CyberArk returns the user name and password that you define here.)
   - Set **Device type** to **Network device**.

   You need the name of the object (account) when you define collection tasks in Skybox.

Chapter 2

Quick reference for data collection

This chapter provides a quick reference for data collection from devices supported by Skybox. More detailed information for each device is provided in subsequent chapters.

You can collect device data by:

- Connecting directly to the device or management system and collecting device data.

  For this method, you must know device details. Skybox has collection tasks for many device types.

- Importing saved device files.

  For this method, you must save copies of the necessary files on your file system. Skybox includes offline file import tasks that import these data files.

In this chapter

QUICK REFERENCE: FIREWALL CONFIGURATION COLLECTION

You can collect device data by:

- Connecting directly to the device () or device management system () and collecting device data.

  For this method, you must know device details. Skybox has many tasks that connect to specific device types.

- Importing saved device files ().

  For this method, you must save copies of the necessary files on your file system. Skybox includes offline file import tasks that import these data files.

In the following table, the **Log files** column shows whether data collection from log files is supported for rule usage analysis (RUA) and change tracking (CT) (see Quick reference: Firewall traffic log and audit log collection (on page 30)). Unless otherwise stated, the data is collected from syslog events.

Device	Data source	Integration requirements	Log files
Alcatel-Lucent VPN Firewall Brick	📄	Skybox includes a parser that creates an iXML file from Alcatel-Lucent firewall configuration files. This iXML file can then be imported into Skybox. The parser is `<Skybox_Home>\intermediate\bin\parsers\firewalls\brick\BrickParser.pl` For help using the script, run the script without any arguments. For additional help, open a case at the Skybox Support portal.	
Arkoon	📄	Skybox includes a parser that creates an iXML file from Arkoon firewall configuration files. This iXML file can then be imported into Skybox. The parser is `<Skybox_Home>\intermediate\bin\parsers\firewalls\arkoon\arkoonParser.pl` For help using the script, run the script without any arguments. For additional help, open a case at the Skybox Support portal.	
Barracuda Networks (Phion) Barracuda NG Firewall	📄	Skybox includes a parser that creates an iXML file from Barracuda Networks Barracuda NG firewall configuration files. This iXML file can then be imported into Skybox. The parser is `<Skybox_Home>\intermediate\bin\parsers\firewalls\barracuda\barracudaNGParser.pl` For help using the script, run the script without any arguments. For additional help, open a case at the Skybox Support portal.	
Check Point FireWall-1 (on page 66) Check Point Provider-1 (on page 79) Check Point Security Management (on page 91)	🗄 🖧	(R77 and lower) The OPSEC API gets configurations remotely from a FireWall-1 Management Server or from a Provider-1 Domain Server (CMA). (R80 and higher) A REST API gets configurations remotely from Security Management. Use SSH to get installed hotfixes remotely from FireWall-1 firewalls.	RUA (syslog or OPSEC), CT (OPSEC)
	📄	The following files are required if the files come from a FireWall-1 Management Server: • `objects_5_0.c`: The network objects • `rulebases_5_0.fws`: The rulebase The following files are required if the files come from a Provider-1 Domain Server (CMA): • `objects.c` or `objects_5_0.c`: The Domain Server network objects • `rulebases.fws` or `rulebases_5_0.fws`: The Domain	

Device	Data source	Integration requirements	Log files
		Server rulebase • g_objects.c or g_objects_5_0.c: The global network objects The following files are optional for both FireWall-1 and Provider-1: • install_statuses.c: The statuses **Note**: If the Check Point configuration contains multiple policies, install_statuses.c is mandatory. • vsx_objects.c: The VSX device objects You also need the name of the active policy on each firewall module and the ifconfig and netstat -rnv output from each firewall module.	
Check Point FireWall-1 hotfix (on page 78)	⛁	• The IP address of the firewall • SSH access to the firewall	
Check Point Gaia (on page 89)	⛁	• The IP address of the Management Server • SSH access to the Management Server	
Cisco Firepower Management Center (on page 98)	⛁	• The name or IP address of the Management Center • A user name and password to access the Management Center	RUA
Cisco PIX/ASA/FWSM (on page 99)	⛁	• The IP address of the firewall • SSH or Telnet access to the firewall • An admin user with level 5 privileges	RUA, CT
	🗎	The following files are required: • run.txt: The PIX/ASA/FWSM configuration • (Optional) route.txt: Dump of the PIX/ASA/FWSM routing table	
Cisco Security Manager (on page 105)	🖧	• The IP address of the Cisco Security Manager (CSM) • A user name and password to access the CSM	RUA
	🗎	The following file is required: • *.xml: The CSM source file	
CiscoWorks (on page 270)	🗎	The following file is required: • <device IP address>.cfg: The firewall configuration	
Dell SonicWALL (on page 107)	⛁	• The name or IP address of the firewall • A user name and password to access the firewall	
DioNIS (on page 108)	⛁	• DioNIS agent software • The name or IP address of the firewall • A user name and password to access the firewall	
DPtech (on page 109)	⛁	• The IP address of the firewall • SSH access to the firewall • A user name and password to access the firewall	
Forcepoint (StoneGate) (on page 111)	⛁	• The IP address of the Forcepoint NGFW appliance • An API-key to access the appliance	RUA

Device	Data source	Integration requirements	Log files
Fortinet FortiGate (on page 112)		• The IP address of the firewall • SSH or Telnet access to the firewall • A user name and password to access the firewall	RUA, CT
		The following files are required: • `config.txt`: The FortiGate configuration • (Optional) `route.txt`: Dump of the FortiGate routing table	
Fortinet FortiManager (on page 116)		• The name or IP address of the FortiManager Security Management appliance • A super user name and password to access the FortiManager Security Management appliance	CT
Genband (on page 120)		• The IP address of the firewall • SSH or SCP access to the firewall • A user name and password to access the firewall	
Huawei Eudemon (on page 122)		• The IP address of the firewall • SSH access to the firewall • A user name and password to access the firewall	
Juniper Networks Junos (on page 123)		• The IP address of the firewall • SSH or Telnet access to the firewall • A user name and password to access the firewall	RUA, CT
		The following files are required: • `config.txt`: The Junos configuration • (Optional) `route.txt`: Dump of the Junos routing table	
Juniper Networks Junos Space (on page 127)		• A global domain Read-Only Administrator account. • The name or IP address of the Junos Space platform • A user name and password to access the Junos Space platform	
Juniper Networks NetScreen (on page 129)		• The IP address of the firewall • SSH or Telnet access to the firewall • A user name and password to access the firewall	RUA, CT
		The following files are required: • `config.txt`: The NetScreen configuration • (Optional) `route.txt`: Dump of the NetScreen routing table	
Juniper Networks NSM (on page 131)		• A global domain Read-Only Administrator account. • The name or IP address of the NSM • A user name and password to access the NSM	
Linux iptables (on page 133)		The following files are required: • `ifconfig.txt`: The iptables interfaces configuration report • `filter.txt`: The iptables filter table • `nat.txt`: The iptables NAT table • `mangle.txt`: The iptables mangle table • (Optional) `ipset.xml`: The iptables ipset table	
McAfee Enterprise (Sidewinder) (on page 134)		• The name or IP address of the firewall • A user name and password to access the firewall	RUA

Device	Data source	Integration requirements	Log files
Microsoft Azure (on page 136)	⛁	Azure credentials: - Directory ID, Application ID, and Key - (Optional) Subscription ID	
Palo Alto Networks (on page 138)	⛁	- The name or IP address of the firewall - A user name and password to access the firewall	RUA, CT
	🗎	The following files are required: - `config.xml`: The Palo Alto configuration and system information - (Optional) `route.txt`: Dump of the Palo Alto Networks routing table	
Palo Alto Networks Panorama (on page 144)	🖧	- The name or IP address of the Panorama - A user name and password to access the Panorama	CT
pfSense	🗎	Skybox includes a parser that creates an iXML file from pfSense firewall configuration files. This iXML file can then be imported into Skybox. The parser is `<Skybox_Home>\intermediate\bin\parsers\firewalls\pfsense\pfsenseParser.pl` For help using the parser, run the parser without any arguments. For additional help, open a case at the Skybox Support portal.	
Sidewinder G2 (McAfee Enterprise) (on page 146)	🗎	The following files are required: - The interfaces file - The ipfilter data file - The proxy services definitions file - The proxy rules data (ACL) file - (Optional) Burbs definition file - (Optional) Routing information file The Skybox Sidewinder G2 parser creates an iXML file from these files. This iXML file can then be imported into Skybox.	
Sophos Unified Threat Management (on page 148)	🖧	- The name or IP address of the Unified Threat Management (UTM) firewall - A user name and password to access the UTM	
Topsec	🗎	Skybox includes a parser that creates an iXML file from Topsec firewall configuration files. This iXML file can then be imported into Skybox. The parser is `<Skybox_Home>\intermediate\bin\parsers\firewalls\topSec\topSecParser.pl` For help using the parser, run the parser without any arguments. For additional help, open a case at the Skybox Support portal.	

Device	Data source	Integration requirements	Log files
VMware vShield Edge (on page 149)		• The name or IP address of the vShield Edge Manager • A user name and password to access the vShield Edge Manager	
WatchGuard Technologies		Skybox includes a script that retrieves WatchGuard Technologies firewall configuration files and a parser that creates an iXML file from these files. This iXML file can then be imported into Skybox. The script is `<Skybox_Home>\intermediate\bin\collectors\firewalls\watchguard\watchguardCollection.pl` The parser is `<Skybox_Home>\intermediate\bin\parsers\firewalls\watchguard\WatchguardParser.pl` For help using a script, run the script without any arguments. For additional help, open a case at the Skybox Support portal.	
Zscaler Cloud Security Platform		• The name of the Zscaler Cloud Security Platform • A user name and password to access the Zscaler Cloud Security Platform • A user API key for the Zscaler Cloud Security Platform	

QUICK REFERENCE: FIREWALL TRAFFIC LOG AND AUDIT LOG COLLECTION

You can collect firewall traffic and audit data by:

- Connecting directly to the management system ( ) that manages the firewalls and collecting log data.

  For this method, you must know management system details. Skybox has many tasks that connect to specific management systems.

- Importing saved firewall log files ( ).

  For this method, you must save copies of the necessary files on your file system. Skybox includes offline file import tasks that import these data files.

Data	Data source	Integration requirements
Check Point FireWall-1 activity log data (on page 163) (LEA collection)		• The IP address of the FireWall-1 Management Server • (If collecting from a log server) The IP address of the log server
Check Point FireWall-1 change events (on page 175) (audit log data)		• The IP address of the FireWall-1 Management Server • (If collecting from a log server) The IP address of the log server

Data	Data source	Integration requirements
Syslog change events (on page 170)	📄	- Configure the firewall or syslog server to forward the change events - The path to the directory containing the syslog files
Syslog traffic events (on page 154)	📄	- Configure the firewall or syslog server to forward the traffic events - The path to the directory containing the syslog files

QUICK REFERENCE: PROXIES, VPN DEVICES, AND IPS DEVICES

You can collect device data by:

- Connecting directly to the device (⛁) or device management system (🖧) and collecting device data.

  For this method, you must know device details. Skybox has many tasks that connect to specific device types.

- Importing saved device files (📄).

  For this method, you must save copies of the necessary files on your file system. Skybox includes offline file import tasks that import these data files.

Device	Data source	Integration requirements
Balabit Shell Control Box	📄	Skybox includes a parser that creates an iXML file from Balabit Shell Control Box (SCB) proxy configuration files. This iXML file can then be imported into Skybox. The parser is `<Skybox_Home>\intermediate\bin\parsers\proxy\balabitScb\balabitScbParser.pl` For help using the parser, run the parser without any arguments. For additional help, open a case at the Skybox Support portal.
Blue Coat (on page 63)	⛁	- The IP address of the proxy - A user name and password to access the proxy
	📄	The following files are required: - `*.txt` or `*.log`: The Blue Coat configuration - (Optional) `route.txt`: Dump of the Blue Coat routing table
IBM ISS Proventia G (on page 303)	⛁	- The IP address of the Proventia G appliance - A user name and password to access the SiteProtector database
Juniper SA Series SSL VPN (now Pulse Connect Secure) (on page 58)	📄	The following files are required: - `*.xml`: The Juniper SA appliance configuration data

Device	Data source	Integration requirements
McAfee IPS (on page 302)		- The IP address of the McAfee IPS device - A user name and password to access the device
Squid		Skybox includes a parser that creates an iXML file from Squid proxy configuration files. This iXML file can then be imported into Skybox. The parser is `<Skybox_Home>\intermediate\bin\parsers\proxy\squid\squidParser.pl` For help using the parser, run the parser without any arguments. For additional help, open a case at the Skybox Support portal
Trend Micro TippingPoint (on page 299)	+ 	- The name or IP address of the SMS appliance - A Super User name and password to access the SMS appliance - The IP address of the TippingPoint device - A user name and password to access the TippingPoint device

QUICK REFERENCE: LOAD BALANCERS

You can collect load balancer data by:

- Connecting directly to the load balancer () and collecting device data.

  For this method, you must know load balancer details. Skybox has many tasks that connect to specific device types.

- Importing saved load balancer files ().

  For this method, you must save copies of the necessary files on your file system. Skybox includes offline file import tasks that import these data files.

Device	Data source	Integration requirements
A10 Networks (on page 277)		- The IP address of the load balancer - A user name and password to access the load balancer
		The following files are required: - `*.txt` or `*.log`: The A10 configuration - (Optional) `route.txt`: Dump of the A10 routing table
Brocade ADX (on page 280)		- The IP address of the load balancer - A user name and password to access the load balancer
Cisco ACE (on page 281)		- The IP address of the load balancer - A user name and password to access the load balancer
		The following files are required: - `run.txt`: The ACE configuration - (Optional) `route.txt`: Dump of the ACE

Device	Data source	Integration requirements
		routing table
Cisco CSS (on page 283)	🛢	- The IP address of the load balancer - A user name and password to access the load balancer
	📄	The following files are required: - `run.txt`: The CSS configuration - (Optional) `route.txt`: Dump of the CSS routing table
Citrix NetScaler (on page 285)	🛢	- The IP address of the load balancer - A user name and password to access the load balancer
	📄	The following file is required: - `*.*`: The NetScaler configuration
F5 BIG-IP (on page 287)	🛢	- The IP address of the load balancer - A user name and password to access the load balancer
	📄	The following files are required: - `bigip.conf`: The BIG-IP configuration - (Optional) `netroute.txt`: Dump of the BIG-IP routing table
Pulse Secure vTM (on page 291)	🛢	- The IP address of the load balancer - A user name and password to access the load balancer
Radware Alteon (on page 292)	🛢	- The IP address of the load balancer - A user name and password to access the load balancer
Radware AppDirector (on page 294)	🛢	- The IP address of the load balancer - A user name and password to access the load balancer
	📄	The following files are required: - `*.*`: The AppDirector configuration - (Optional) `route.txt`: Dump of the AppDirector routing table
Radware WSD (on page 296)	🛢	- The IP address of the load balancer - The SNMP Community string to access the load balancers
	📄	The following file is required: - `*.txt`: A WSD SNMP dump file

QUICK REFERENCE: ROUTERS, SWITCHES, AND CONTROLLERS

With Skybox, you can collect device configuration data by:

- Connecting directly to the device (🛢) and collecting device data.

  For this method, you must know device details. Skybox has many tasks that connect to specific device types.

- Importing saved device files (📄).

  For this method, you must save copies of the necessary files on your file system. Skybox includes offline file import tasks that import these data files.

Note: For Cisco IOS routers, Skybox supports data collection from log files for rule usage analysis.

Device	Data source	Integration requirements
Alcatel-Lucent (on page 178)	⊛	• The IP address of the router • A user name and password to access the router
Arista Networks (on page 180)	⊛	• The IP address of the router • A user name and password to access the router
	📄	The following files are required: • `run.txt`: The Arista configuration • (Optional) Dump of the Arista routing table
Aruba Networks (on page 182)	⊛	• The IP address of the wireless controller • A user name and password to access the wireless controller
Avaya (on page 183)	⊛	• The IP address of the router • A user name and password to access the router
Avaya ERS (on page 185)	⊛	• The IP address of the switch • A user name and password to access the switch
	📄	The following files are required: • `run.txt`: The Avaya ERS configuration • (Optional) `route.txt`: Dump of the Avaya ERS routing table
Brocade VDX (on page 187)	⊛	• The IP address of the router • A user name and password to access the router
	📄	The following files are required: • `run.txt`: The VDX configuration • `route.txt`: Dump of the VDX routing table
Cisco IOS (on page 189)	⊛	• The IP address of the router • A user name and password to access the router
	📄	The following files are required: • `run.txt`: The IOS configuration • (Optional) `route.txt`: Dump of the IOS routing table
Cisco Nexus (on page 195)	⊛	• The IP address of the router • A user name and password to access the router
	📄	The following files are required: • `run.txt`: The Nexus configuration • (Optional) `route.txt`: Dump of the Nexus routing table

Device	Data source	Integration requirements
Cisco Wireless LAN Controller (on page 199)	⛁	- The IP address of the wireless controller - A user name and password to access the wireless controller
	📄	The following file is required: - `*.*`: The Cisco Wireless LAN Controller configuration
CiscoWorks (on page 270)	📄	The following file is required: - `<device IP address>.cfg`: The router configuration
Dionis NX (on page 201)	⛁	- The IP address of the router - A user name and password to access the router
Enterasys (on page 202)	⛁	- The IP address of the router - A user name and password to access the router
	📄	The following files are required: - `run.txt`: The Enterasys configuration - (Optional) `route.txt`: Dump of the Enterasys routing table
Extreme Networks (on page 204)	⛁	- The IP address of the router - A user name and password to access the router
	📄	Skybox includes a script that retrieves Extreme Networks router configuration files and a parser that creates an iXML file from these files. This iXML file can then be imported into Skybox. The script is `<Skybox_Home>\intermediate\bin\collectors\router\extremeNetworks\extremeNetworksCollection.pl` The parser is `<Skybox_Home>\intermediate\bin\parsers\router\extremeNetworks\extremeNetworksParser.pl` For help using a script, run the script without any arguments. For additional help, open a case at the Skybox Support portal.
H3C (on page 211)	⛁	- The IP address of the router - A user name and password to access the router
	📄	The following files are required: - `run.txt`: The H3C configuration - (Optional) `route.txt`: Dump of the H3C routing table
HP ProCurve (on page 206)	⛁	- The IP address of the router - A user name and password to access the router

Device	Data source	Integration requirements
	📄	The following files are required: • `*.*`: The ProCurve configuration • (Optional) `route.txt`: Dump of the ProCurve routing table
Huawei (on page 208)	⛁	• The IP address of the router • A user name and password to access the router
	📄	The following files are required: • `run.txt`: The Huawei configuration • (Optional) Dump of the Huawei routing table • (Optional) Dump of the routing table for each VPN instance
Juniper Networks MX (on page 206)	⛁	• The IP address of the router • SSH or Telnet access to the router • A user name and password to access the router
	📄	The following files are required: • `config.txt`: The Junos configuration • (Optional) `route.txt`: Dump of the Junos routing table
Nortel Passport 8600 (on page 212)	⛁	• The IP address of the router • SSH or Telnet access to the router • A user name and password to access the router
	📄	The following files are required: • `run.txt`: The Nortel configuration • (Optional) `route.txt`: Dump of the Nortel routing table
Vyatta (on page 214)	⛁	• The IP address of the router • A user name and password to access the router

QUICK REFERENCE: SCANNERS AND OPERATIONAL TECHNOLOGY

You can collect device data by:

- Connecting directly to the device (⛁) or device management system (🖧) and collecting device data.

  For this method, you must know device details. Skybox has many tasks that connect to specific device types.

- Importing saved device files (📄).

  For this method, you must save copies of the necessary files on your file system. Skybox includes offline file import tasks that import these data files.

Device	Data source	Integration requirements
BeyondTrust (eEye) Retina (on	⛁	The path to an RTD file

Device	Data source	Integration requirements
page 217)		
Claroty (on page 272)	⛁	- The name or IP address of the platform - A user name and password to access the platform
CyberX (on page 273)	⛁	- The IP address of the platform - A user token (password) to access the platform
McAfee Vulnerability Manager (Foundstone) (on page 218)	⛁	- The name or IP address of the database server that hosts the McAfee Vulnerability Manager database - A user name and password to access the McAfee Vulnerability Manager (Foundstone) database
HP Software & Solutions (OpenView) (on page 270)	🗎	The following file is required: - `*.txt`: HPOV topology dump
IBM Security AppScan (on page 220)	🗎	The following file is required: - `*.xml`: AppScan XML file
IBM Security SiteProtector System (on page 221)	🖧	- The IP address of the scanner - The name or IP address of the database server that hosts the SiteProtector database - A user name and password to access the SiteProtector database
Indegy (on page 274)	⛁	- The name or IP address of the platform - The Indegy certificate and key
Nmap	🗎	The following file is required: - `*.xml`: Nmap XML file (output of `nmap –v –sS –O –oX <output file> <scan range>`)
Outpost24	🗎	Skybox includes a parser that creates an iXML file from Outpost24 scanner files. This iXML file can then be imported into Skybox. The parser is `<Skybox_Home>\intermediate\bin\parsers\scanners\outpost24\outpost24Parser.pl` For help using the parser, run the parser without any arguments. For additional help, open a case at the Skybox Support portal.
Qualys QualysGuard (on page 222)	⛁	A user name and password to access the Qualys account
	🗎	The following files are required: - `scan.xml`: Qualys scan - (Optional) `map.xml`: Qualys map
Rapid7 Nexpose (on	⛁	- The IP address of the scanner - A user name and password to access the scanner

Device	Data source	Integration requirements
page 226)	📄	The following files are required: - A set of `*.xml`: Rapid7 Nexpose audit report files The files can be in ns-xml, raw-xml, or qualys-xml format.
SecurityMatters (on page 275)	⛁	- The IP address of the platform - A user name and password to access the platform
SNMP walk	📄	Use a basic file import (see page 47) or advanced file import (see page 49) task. The following file is required: - `*.*`: SNMP walk dump
Tenable Network Security Nessus (on page 228)	⛁	- The IP address of the scanner - A user name and password to access the scanner
	📄	The following file is required: - `*.nessus`: Nessus XML file
Tenable.io (on page 230)	🖧	- The name or IP address of Tenable.io - A user name and password to access the Tenable.io
Tenable.sc (on page 231)	🖧	- The name or IP address of Tenable.sc - A user name and password to access the Tenable.sc
Tripwire IP360 (nCircle) (on page 233)	⛁	- The name or IP address of the VnE Manager - A user name and password to access the VnE Manager
	📄	The following files are required for nCircle XML3: - `scan.xml`: nCircle export XML - `aspl.xml`: nCircle ASPL XML The following file is required for nCircle XML2: - `*.xml`: nCircle export XML
WhiteHat Sentinel (on page 235)	⛁	An API key to access the WhiteHat site

Chapter 3

File import tasks

This chapter describes how to set the properties of file import tasks.

In this chapter

IMPORT DIRECTORY TASKS

Import – Directory tasks import the configuration files or scan data files of multiple devices into the model. The files must be in a specified directory on the Skybox Server or on a Skybox Collector.

For a list of supported devices, scanners, and files and their file formats, see Supported devices and files for import directory tasks (on page 42).

Directory structure

Single configuration files for devices and scanner output files must be in any of the specified directories (a directory can contain any number of these files, for the same or different devices); if a device has multiple configuration files, the files must be in a 1st-level subdirectory of the specified directory (a single subdirectory per device).

Note: Even if you are importing a *single* device with multiple configuration files, the files must be in a 1st-level subdirectory (*not* in the specified directory).

You can specify any number of directories in an **Import – Directory** task.

A specified directory can contain:

- A device configuration file
- A file that combines device configuration and a dump of the routing table
- A file that combines the netstat and ifconfig data

- A scanner output file
- An iXML file

Each (1st-level) subdirectory can contain one of the following sets of files (a single file of each type):

- Device configuration and a dump of the routing table in separate files
- Check Point files:
  - (Mandatory) `objects.c`, `rulesbases.fws`
  - (Optional) `global objects`, `statuses file`

  Note: If the Check Point configuration contains multiple policies, `install_statuses.c` is mandatory (it specifies the policy that is installed on each device).
- netstat and ifconfig data in separate files

Note: In all cases the files can have any names: Skybox identifies the file type.

Task properties

The properties that control **Import – Directory** tasks are described in the following table.

Property	Description
Basic tab	
Run in	The location of the files to import.
Modified in	The age of the files to import. • **Custom**: Select **Specific** or **Relative** start and end times.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td><em>Set &lt;n&gt;</em></td><td>Specify up to 4 sets of devices (directories). (To import more sets, use the <strong>Additional Sets</strong> field.)
If you specify <strong>Location Hint</strong> in the <strong>Advanced</strong> tab, all devices must be at the same location.
<table>
<tr><td>Directory</td><td>The full path to the directory containing the files (or subdirectories) to import.
<strong>Note</strong>: Even if you are importing a single device with multiple configuration files, the files must be in a subdirectory.</td></tr>
<tr><td>Comment</td><td>A description of the content of <strong>Directory</strong>.</td></tr>
<tr><td>Import BGP Routes</td><td>(Cisco IOS, Cisco Nexus, Cisco ASA, Juniper Junos, and Fortinet FortiGate devices only. Ignored for all other devices.)
Specifies whether to import BGP routing rules:
<strong>System default</strong>: Uses the relevant values (in <code>&lt;Skybox_Home>\server\conf\sb_common.properties</code>) of:<ul><li><code>ios_ignore_BGP_routing_rules</code></li><li><code>nexus_ignore_BGP_routing_rules</code></li><li><code>fwsm_ignore_BGP_routing_rules</code></li><li><code>junos_ignore_BGP_routing_rules</code></li><li><code>fortigate_ignore_BGP_routing_rules</code></li></ul>These properties have default values of <code>true</code>.</td></tr>
</table></td></tr>
<tr><td>Additional Sets</td><td>Click the <strong>Browse</strong> button and type the directories containing the configuration data of additional sets of devices (1 per line).
Optionally, specify a location hint per directory.</td></tr>
<tr><td>Import BGP Routes</td><td>(Cisco IOS, Cisco Nexus, Cisco ASA, Juniper Junos, and Fortinet FortiGate devices only. Ignored for all other devices.)
Specifies whether to import BGP routing rules for the additional sets of devices:
<strong>System default</strong>: Uses the relevant values (in <code>&lt;Skybox_Home>\server\conf\sb_common.properties</code>) of:<ul><li><code>ios_ignore_BGP_routing_rules</code></li><li><code>nexus_ignore_BGP_routing_rules</code></li><li><code>fwsm_ignore_BGP_routing_rules</code></li><li><code>junos_ignore_BGP_routing_rules</code></li><li><code>fortigate_ignore_BGP_routing_rules</code></li></ul>These properties have default values of <code>true</code>.</td></tr>
<tr><td colspan="2"><strong>Advanced tab</strong></td></tr>
<tr><td>Location Hint</td><td>The location of the devices whose data is imported. (To import the data of multiple devices, the devices must be at the same location.)
<strong>Note</strong>: Use this property if different locations use the same set of IP addresses, so that devices at different locations can have the same IP address.</td></tr>
</table>

Property	Description
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Do Not Force Unique Tag Merging	If selected, and the imported device has a unique tag, the task tries to match the device to devices existing in the model based on network interfaces. If unsuccessful, the task adds the device to the model. If cleared, the task adds the device to the model if it has a unique tag.
Import from Autonomous Collector	Select this option only if you are importing data collected by a Skybox autonomous collection unit. (See Importing data from Skybox autonomous collection units (on page 43)).
Rematch all vulnerability occurrences	This field is displayed for Skybox Vulnerability Control and Skybox Threat Manager only. Specifies whether to rematch all vulnerability occurrences with services. Select this option only when combining 2 Skybox models.
Merge risk and attack information	This field is displayed for Skybox Vulnerability Control and Skybox Threat Manager only. Specifies whether to merge risk and attack information (used for attack simulation). Select this option only when combining 2 Skybox models.
Tripwire ASPL File	(For nCircle XML3 imports) The ASPL file to use for all Tripwire IP360 (nCircle) imports (so that the file is only parsed once by Skybox). If this field is empty, the ASPL file is parsed separately for each Tripwire import.
Qualys Filter by Kernel Activity	(For Qualys QualysGuard imports) Specifies whether to add vulnerability occurrence data to the model for some kernels only.
Kernel Activity	This field is enabled only if **Qualys Filter by Kernel Activity** is selected. The kernels for which to add vulnerability occurrence data to the model.
Qualys Attach services to interfaces	(For Qualys QualysGuard imports) Specifies whether to attach each service to an interface (instead of attaching it to all interfaces) after importing a scan.

Supported devices and files for import directory tasks

Import – Directory tasks import configuration and other data to the model for devices, scanners, and files:

- Devices and scanners with collection tasks

  Configuration data of most devices and scanners that have dedicated collection tasks can be imported using an **Import – Directory** task, as documented in the individual tasks.

- Devices and scanners with parsers

There are parsers for less common devices and scanners. (In some cases, there is also a collection script.) Parsers input configuration files of a device and output an iXML file.

Devices with parsers are included in the tables in the Quick reference for data collection chapter (see page 25).

- iXML files

  Files containing device configuration written in iXML.

  For information about iXML, see the Integration part of the Skybox Developer Guide.

- Network state files (see Importing interface and routing configuration (on page 60))

Appending routing information to device configuration

If you cannot extract routing rules in device native format, you can manually append the rules to the end of the device configuration file.

The appended text must have the following format:

```
ROUTE_START
<destination IP address>,<netmask>,<gateway>,<interface
name>,<metric>,<type>,[<VRF>],[<via VRF>]
...
ROUTE_END
```

Notes

- For via global rules, set `via` VRF to GLOBAL
- `interface` name is the name of the interface, not its IP address
- `type` is connected, `static`, or dynamic

Supported devices

- Cisco IOS
- FortiGate
- Cisco PIX/ASA/FWSM
- Juniper Junos

Importing data from Skybox autonomous collection units

If an organization's network is an air-gapped system, they cannot use Skybox Collectors in the network. Instead, they must use a Skybox autonomous collection unit. The collected data is then saved to a removable storage device.

To import data collected from a Skybox autonomous collection unit

1. Copy the data from the removable storage device to the Skybox Server.

   If the data was zipped, make sure to unzip it.

2. Use an **Import – Directory** task to import the data to a Skybox model.

   Important: When you create the **Import – Directory** task, you must select **Import from Autonomous Collector** in the **Advanced** tab.

For information about Skybox autonomous collection units, see the Autonomous collection units section in the Skybox Installation and Administration Guide.

DATA FORMATS FOR FILE IMPORT TASKS

Note: We recommend that you use Import – Directory tasks (see page 39) for all supported devices and file types (see page 42) (including network state files and iXML files).

The import data format types supported by Skybox are listed in the following table. The table also lists the relevant source file or directory required for the file import. The information in this table is used by **Import – Basic**, **Import – Advanced**, **Import – Collector**, and **Import – Collector Advanced** file import tasks.

Note: For **Import – Basic** tasks, specify the location of each file separately (not the directory).

Format name	Import data type	Source file or directory
A10	A10	Directory containing the following files: • `*.txt` or `*.log`: The A10 configuration • (Optional) `route.txt`: Dump of the A10 routing table
AppDirector	APPDIRECTOR	Directory containing the following files: • `*.*`: The AppDirector configuration • (Optional) `route.txt`: Dump of the AppDirector routing table
Blue Coat	BLUECOAT	Directory containing the following files: • `*.txt` or `*.log`: The Blue Coat configuration • (Optional) `route.txt`: Dump of the Blue Coat routing table
Brocade Configuration	FOUNDRY	Directory containing the following files: • `run.txt`: The Brocade configuration • (Optional) `route.txt`: Dump of the Brocade routing table; output of the `show ip route` command
Cisco Router Configuration (Used for Cisco IOS and Cisco Nexus routers)	IOS_CONF	Directory containing the following files: • `run.txt`: The Cisco router configuration • (Optional) `route.txt`: Dump of the Cisco router routing table **Note**: **Import – Advanced** and **Import – Collector** tasks can import the output of selected subcommands of the show `ip route vrf all` command. If `route.txt` is not found in the specified directory, the tasks process all files named `route_XXX.txt` For example, execute the command: `show ip route vrf connected` Save the output in `route_connected.txt`

Format name	Import data type	Source file or directory
Cisco Security Manager Configuration	CSM_CONFIG_FILE	Cisco Security Manager source file (`*.xml`)
FireWall-1 Configuration	FW1_CONF	Directory containing the following files: • `objects_5_0.c`: The network objects • `rulebases_5_0.fws`: The rulebase • (Optional) `install_statuses.c`: The statuses • (Optional) `vsx_objects.c`: The VSX device objects (from the vsx_slot_objects table) **Note**: For **Import – Basic** tasks, any file names with these extensions (`*.c` and `*.fws`) are permitted.
FortiGate Configuration file	FORTIGATE_CONFIG_FILE	Directory containing the following files: • `config.txt`: The FortiGate configuration • (Optional) `route.txt`: Dump of the FortiGate routing table
FWSM Configuration (Can be used for Cisco PIX/ASA/FWSM firewalls)	FWSM_CONF	Directory containing the following files: • `run.txt`: The PIX/ASA/FWSM configuration • (Optional) `route.txt`: Dump of the PIX/ASA/FWSM routing table
HFNetChk Vulnerability Scanner Report	HFNETCHK	Shavlik NetChk Protect Vulnerability Scanner Report file (`*.txt`)
HP ProCurve	HPPROCURVE	Directory containing the following files: • `*.*`: The ProCurve configuration • (Optional) `route.txt`: Dump of the ProCurve routing table
HPOV Topology Dump	HPOV_TOPODUMP	HP Software & Solutions (OpenView) topology dump file (`*.txt`)
Integration XML	INTERMEDIATE_XML	iXML file (`*.xml`)
iptables Configuration	IPTABLES	Directory containing the following files: • `ifconfig.txt`: The iptables interfaces configuration report • `filter.txt`: The iptables filter table • `nat.txt`: The iptables NAT table • `mangle.txt`: The iptables mangle table • (Optional) `ipset.xml`: The iptables ipset table
Junos Configuration	JUNOS_CONFIG_FILE	Directory containing the following files: • `config.txt`: The Junos configuration

Format name	Import data type	Source file or directory
file		- (Optional) route.txt: Dump of the Junos routing table
Nessus Scan	NESSUS_XML	Nessus XML file (usually *.xml or *.nessus)
NetScreen Configuration file	NETSCREEN_CONFIG_FILE	Directory containing the following files: - config.txt: The NetScreen configuration - (Optional) route.txt: Dump of the NetScreen routing table
NetScreen SNMP Dump file	NETSCREEN_SNMP_DUMP	NetScreen SNMP dump file (*.txt)
Network State	HOST_ROUTING_AND_INTERFACES	Directory containing the following files: - netstat.txt: The network status report - ifconfig.txt: The interfaces configuration report
NMap Scan	NMAP_XML	Nmap XML file (*.xml)
Nortel Bay 8600 Configuration	NORTEL_BAY	Directory containing the following files: - run.txt: The Nortel configuration - (Optional) route.txt: Dump of the Nortel routing table
Palo Alto Firewall Configuration	PALO_ALTO	Directory containing the following files: - config.xml: The Palo Alto configuration - (Optional) route.txt: Dump of the Palo Alto routing table
PIX Configuration (Can be used for Cisco PIX/ASA/FWSM firewalls)	PIX_CONF	Directory containing the following files: - run.txt: The PIX/ASA/FWSM configuration - (Optional) route.txt: Dump of the PIX/ASA/FWSM routing table
Provider-1 Configuration	PFW1_CONF	Directory containing the following files: - objects.c or objects_5_0.c: The Domain Server (CMA) network objects - rulebases.fws or rulebases_5_0.fws: The Domain Server (CMA) rulebase - g_objects.c or g_objects_5_0.c: The global network objects - (Optional) install_statuses.c: The statuses - (Optional) vsx_objects.c: The VSX device objects (from the vsx_slot_objects table) **Note**: For **Import – Basic** tasks, any file names with these extensions (*.c and *.fws) are permitted

Format name	Import data type	Source file or directory
Qualys Map and Scan	QUALYS	Directory containing the following files: • scan.xml or scan.txt: The Qualys scan • (Optional) map.xml or map.txt: The Qualys Map
Rapid7	RAPID_7	
Skybox Netmodel	SKYBOX_XML	Skybox XML file (*.xml)
Skybox Netmodel Encrypted	SKYBOX_XML_ENC	Encrypted Skybox XML file (*.xmlx)
SnmpWalk Configuration	SNMPWALK_DUMP	SNMP walk dump file (*.*)
Tripwire Scan	NCIRCLE	(nCircle XML2) Tripwire IP360 (nCircle) export XML file (*.xml) (nCircle XML3) Directory containing the following files: • Tripwire IP360 (nCircle) export XML (scan.xml) • Tripwire IP360 (nCircle) ASPL XML (aspl.xml)
WSD SNMP Dump	RADWSD_SNMP_DUMP	WSD SNMP dump file (*.txt)

BASIC FILE IMPORT TASKS

Import – Basic tasks import scan data files or configuration files of selected devices (up to 5) into the model. The files must be on the local machine.

To import data of multiple devices into Skybox using a single task, see Advanced file import tasks (on page 49). To import configuration files on a remote machine, see Collector file import tasks (on page 51) and Advanced Collector file import tasks (on page 52).

Task properties

The properties that control **Import – Basic** tasks are described in the following table.

Property	Description
Basic tab	
Import Data 1	A data set to import. Open the Import Data dialog box to specify the import properties. For an explanation of the dialog box properties, see Import data properties (on page 48).
Import Data 2 ... 5	(Optional) Additional data sets to import.

Property	Description
Advanced tab	
Location Hint	The location of the devices whose data is imported. (To import the data of multiple devices, the devices must be at the same location.) **Note**: Use this property if different locations use the same set of IP addresses, so that devices at different locations can have the same IP address.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Rematch all vulnerability occurrences	(Skybox Vulnerability Control and Skybox Threat Manager only) Specifies whether to rematch all vulnerability occurrences with services. Select this option only when combining 2 Skybox models.
Merge risk and attack information	(Skybox Vulnerability Control and Skybox Threat Manager only) Specifies whether to merge risk and attack information (used for attack simulation). Select this option only when combining 2 Skybox models.

Import data properties

The properties in the Import Data dialog box are described in the following table.

Property	Description
Format	The format type for the offline file import. Format types are listed in the 1st column of the table in Data formats for file import tasks (on page 44). Only this field is displayed when you open the dialog box. After you select a **Format**, additional fields are displayed that enable you to select the required file types. • For information about file types, refer to the 3rd column of the table in Data formats for file import tasks (on page 44).
<file type 1>	The 1st file type required for the selected **Format**.
<file type 2> ... <file type n>	Additional file types required for the selected **Format**.

Import Data dialog box for FireWall-1 or Provider-1 Configuration

If you select **FireWall-1 Configuration** or **Provider-1 Configuration** in the **Format** field of the Import Data dialog box, additional properties are displayed in the dialog box. These properties are described in the following table.

Property	Description
Modules List	A comma-separated (or semicolon-separated) list of the names of Enforcement Modules to import into Skybox.
Rulebase	The policy (rulebase) to import: • **Use active policy**: If a statuses file (usually `install_statuses.c`) is specified in **Statuses file**, the active policy as specified in the statuses file.

Property	Description
	Otherwise, the most recently edited policy as specified in the objects file. - **Use Specific Policy**: Type the name of a policy.
- Network Objects file - Rulebases file - Global Network Objects file (Provider-1 only) - Statuses file - VSX Objects File	The locations of the configuration files required for the offline file import. - For information about these files, see Importing Check Point FireWall-1 configuration data (on page 77) or Importing Check Point Provider-1 Domain Server configuration data (on page 88).

ADVANCED FILE IMPORT TASKS

Import – Advanced tasks import scan data files or configuration files of any number of devices into the model. The files must be on the local machine. These tasks require a *definition file* – a text file that specifies, for each device, the data type to be imported, the path of the data file to be imported, and, possibly, additional properties. For information about the definition file, see Definition file for advanced file import tasks (on page 50).

Task properties

The properties that control **Import – Advanced** tasks are described in the following table.

Property	Description
Basic tab	
Definition Filename	The full path to the definition file that the Skybox Server can access. - For information about the definition file, see Definition file for advanced file import tasks (on page 50).
XML Output Filename	If the file import succeeds, this file (in iXML format) is created on the Skybox Server and contains the imported data. If the file exists, it is overwritten. **Note**: If the definition file includes location hints, an output file is created for each location. (The location is added to the file name specified by this property.)
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Rematch all vulnerability occurrences	(Skybox Vulnerability Control and Skybox Threat Manager only) Specifies whether to rematch all vulnerability occurrences with services. Select this option only when combining 2 Skybox models.

Property	Description
Merge risk and attack information	(Skybox Vulnerability Control and Skybox Threat Manager only) Specifies whether to merge risk and attack information (used for attack simulation). Select this option only when combining 2 Skybox models.

Definition file for advanced file import tasks

Import – Advanced and **Import – Collector Advanced** tasks require a text file (the *definition file*) that specifies the data type to be imported, the path of the data file to be imported, and possibly some additional properties. Each line of the text file represents a data file to import.

Format of lines in a definition file

Each line in a definition text file has the format

```
<import format type> <source file | directory> [<rulebase> [<modules>]]
```

- `<import format type>` is the data type to be imported. For a list of import format types, refer to the 2nd column of the table in Data formats for file import tasks (on page 44).
- `<source file | directory>` is either of:
  - The full path of the data file to be imported
  - The full path of a directory containing multiple data files to be imported (if the import type requires multiple files)

  The path must not contain quotes or spaces.

  Important: If you run a Skybox Collector as a service on Windows, you cannot use a mapped network drive when specifying the full path.

  Workaround: Use the Universal Naming Convention (UNC) name: `\\<server name>\<share name>\<directory>[\<file name>]`.

- `<rulebase>` is required only if the value for `<import format type>` is `FW1_CONF` or `PFW1_CONF`.

  `<rulebase>` and `<modules>` are described in the following table.

Property	Description
<rulebase>	Either of: • The name of the policy (rulebase) to import. • USE_AUTOMATIC: If `install_statuses.c` is included in the specified directory, the active policy as specified in `install_statuses.c` is imported. Otherwise, the most recently edited policy as specified in `objects.c` is imported.
<modules>	A comma-separated (or semicolon-separated) list of the names of the Enforcement Modules to be imported. If no Enforcement Modules are specified, all modules are imported.

Examples of lines in a definition file

- For importing a Nessus XML:

```
NESSUS_XML c:\scans\network_scan.xml
```

- For importing a Cisco IOS router configuration:

```
IOS_CONF c:\ios\router1
```

  To import `run.txt` and, if it exists, `route.txt`, a directory is specified.

- For importing a FireWall-1 configuration:

```
FW1_CONF c:\fws\mainfw Standard
```

  The directory must contain 2 files, `objects_5_0.c` and `rulebases_5_0.fws`. Because no Enforcement Modules are specified, all modules are imported.

Including location hints in a definition file

If your organization has overlapping networks, you might need to add a *location hint* to some lines of the definition file. *Overlapping networks* are networks in your organization that have identical or overlapping IP addresses and subnets. These networks are usually in different parts of your organization, separated by network devices.

Each line that imports an overlapping network must have the format

```
<import format type> <source file | directory> [<location hint>]
```

Important: The square brackets (**[** and **]**) are part of the format of the line; they do *not* denote an optional element.

Examples of lines with location hint in a definition file

- `NMAP_XML c:\sample\result.xml [London\Bakers]`
- `PIX_CONF c:\sample\file.cfg [Paris]`

You can use “\” and “/” as delimiters in the location hint.

To preserve whitespace in location names, place the location inside double quotation marks. For example:

- `PIX_CONF c:\sample\file.cfg [North America/New York]`: The location is read as `NorthAmerica >> NewYork`
- `PIX_CONF c:\sample\file.cfg ["North America/New York"]`: The location is read as `North America >> New York`

COLLECTOR FILE IMPORT TASKS

Import – Collector tasks import scan data files or configuration files of a device into the model. The files must be on a machine that is accessible by the selected Skybox Collector.

To import data of multiple devices held on a remote machine into Skybox using 1 task, see Advanced Collector file import tasks (on page 52).

Task properties

The properties that control **Import – Collector** tasks are described in the following table.

Property	Description
Basic tab	
File Type	The format type for the file import. Possible format types are listed in the 1st column of the table in Data formats for file import tasks (on page 44).
Path	The full path of the source file to import or the directory containing the source files to import. The required value depends on the value of **File Type**; refer to the 3rd column of the table in Data formats for file import tasks (on page 44).
Property	The name of the policy (rulebase) to import. **Note**: This value is relevant only if **File Type** has the value **FireWall-1 Configuration** or **Provider-1 Configuration**.
Advanced tab	
Location Hint	The location of the device whose data is imported. **Note**: Use this property if different locations use the same set of IP addresses, so that devices at different locations can have the same IP address.

ADVANCED COLLECTOR FILE IMPORT TASKS

Import – Collector Advanced tasks import scan data files or configuration files of any number of devices into the model. The files must be on a machine that is accessible from the selected Skybox Collector. These tasks require a *definition file* – a text file that specifies, for each device, the data type to be imported, the path of the data file to be imported, and, possibly, additional properties. For information about the definition file, see Definition file for advanced file import tasks (on page 50).

Task properties

The properties that control **Import – Collector Advanced** tasks are described in the following table.

Property	Description
Definition Filename	The full path to the definition file that the Skybox Collector can access. • For information about the definition file, see Definition file for advanced file import tasks (on page 50).
XML Output Filename	If the file import succeeds, this file (in iXML format) is created on the Skybox Server and contains the imported data. If the file exists, it is overwritten.

GENERIC CSV FILE IMPORT TASKS

CMDB CSV file import tasks

Import – Generic CMDB CSV Parser tasks import Business Asset Group configuration data from user-generated CSV files to the current model.

If the CSV files contain any custom business attributes, Skybox creates the attributes automatically for each asset; you do not need to define them.

Task properties

The properties that control **Import – Generic CMDB CSV Parser** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Hosts Path (v2 only)	The path to the hosts file.
Hosts File (v1 only)	(Mandatory) The location of the CSV file containing the asset configuration data. An example of this file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_cmdb_hosts.csv`
Business Asset / Applications Groups File (v1 only)	The location of the CSV file containing the application configuration data. An example of this file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_cmdb_applications.csv`
Business Units File (v1 only)	The location of the CSV file containing the Business Unit configuration data. An example of this file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_cmdb_bu.csv`
Mapping File	(Mandatory) The location of the *mapping file*. The mapping file contains a map between the asset property names that Skybox uses and the column headers in **Input Host File**. An example of a mapping file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_cmdb_map.txt`

Property	**Description**
Config File	The location of the *configuration file*. The configuration file contains a map between metadata that Skybox uses and metadata in **Input Host File**. An example of a configuration file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_cmdb_config.txt` The following CMDB fields are supported: - IP - Hostname - type - OS - Comment - Owner - AssetValue - - Email - Tag - Business - Function - Site - InterfaceName - ValueScale
Patches File (v1 only)	The location of the CSV file containing the implemented patches data. An example of a patch file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_cmdb_patchlist.csv`
Packages File (v1 only)	The location of the CSV file containing the installed packages data. An example of a package file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_cmdb_packagelist.csv`
Advanced tab	
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.) The location of the debug log file. If this field is empty, the task does not save debug messages.
Delimiter (v1 only)	The CSV file delimiter. Use the same delimiter for all CSV files. The default value is *comma*. For tab-separated files, use the 2-character string `\t`.
Use Parent Name In Path (v1 only)	Specifies whether to include the parent name when creating applications. If selected, the parent name is prepended to the entity name.
CMDB Parser	The version of the parser to use. (Do not change the default unless told to do so by Skybox Professional Services.)
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the Business Asset Groups. **Note**: Use this property if different locations use the same set of IP addresses, so that assets at different locations can have the same IP address.

Host CSV file import tasks

Import – Generic Host CSV Parser tasks import asset configuration data from user-generated CSV files to the current model.

Task properties

The properties that control **Import – Generic Host CSV Parser** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Input File	The location of the CSV file containing the asset configuration data. An example of this file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\Example_input_csv.csv`
Mapping File	The location of the *mapping file*. The mapping file contains a map between the asset property names that Skybox uses and the column headers in **Input File**. An example of a mapping file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\Example_fields_mapping_file.txt`
Config File	(Optional) The location of the *configuration file*. The configuration file contains a map between metadata that Skybox uses and metadata in **Input File**. An example of a configuration file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\Example_config_file.txt`
Advanced tab	
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.) The location of the debug log file. If this field is empty, the task does not save debug messages.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the assets. **Note**: Use this property if different locations use the same set of IP addresses, so that assets at different locations can have the same IP address.

Linux packages CSV file import tasks

Import – Generic Linux Packages Parser tasks import installed Linux packages data from user-generated CSV files to the current model.

Task properties

The properties that control **Import – Generic Linux Packages Parser** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Input File	The location of the CSV file containing the installed Linux packages data. An example of this file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_linuxPackages_csv.csv`
Mapping File	The location of the *mapping file*. The mapping file contains a map between the asset property names that Skybox uses and the column headers in **Input File**. An example of a mapping file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_linuxPackages_map.txt`
Config File	(Optional) The location of the *configuration file*. The configuration file contains a map between metadata that Skybox uses and metadata in **Input File**. An example of a configuration file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_linuxPackages_config.txt`
Advanced tab	
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.) The location of the debug log file. If this field is empty, the task does not save debug messages.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the assets whose Linux packages data is imported. **Note**: Use this property if different locations use the same set of IP addresses, so that assets at different locations can have the same IP address.

Network CSV file import tasks

Import – Generic Network CSV Parser tasks import network configuration data from user-generated CSV files to the current model.

Task properties

The properties that control **Import – Generic Network CSV Parser** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Input File	The location of the CSV file containing the network configuration data.

Property	Description
	An example of this file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_network_csv_input.csv`
Mapping File	The location of the *mapping file*. The mapping file contains a map between the network property names that Skybox uses and the column headers in **Input File**. An example of a mapping file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files\example_network_csv_mapping.txt`
Advanced tab	
Concatenate Location Names	
Merge assets by WINS name	Specifies whether to merge networks by name and not by IP address.
Location Hint	The location of the networks. **Note**: Use this property if different locations use the same set of IP addresses, so that networks at different locations can have the same IP address.

Raw configuration CSV file import tasks

Import – Raw Config tasks import raw configuration data from user-generated CSV files to the current model.

Task properties

The properties that control **Import – Raw Config** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Input Dir	The location of the CSV files containing the raw configuration data.
Advanced tab	
Hostname by file name	
Hostname by folder name	
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.) The location of the debug log file. If this field is empty, the task does not save debug messages.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the assets whose configuration data is imported.

Property	Description
	Note: Use this property if different locations use the same set of IP addresses, so that assets at different locations can have the same IP address.

JUNIPER SA FILES IMPORT TASKS

Import – Juniper SSL VPN Parser tasks import Juniper SA Series SSL VPN (now Pulse Connect Secure) appliance configuration data from user-generated XML files to the current model.

Task properties

The properties that control **Import – Juniper SSL VPN Parser** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Config File Folder	(Optional) The location of the *configuration file*. The configuration file contains a map between metadata that Skybox uses and metadata in **Input File**. An example of a configuration file is at `<Skybox_Home>\intermediate\bin\parsers\general\Example_Files`
Advanced tab	
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.) The location of the debug log file. If this field is empty, the task does not save debug messages.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the Juniper SA appliance. **Note**: Use this property if different locations use the same set of IP addresses, so that appliances at different locations can have the same IP address.

SCRIPT INVOCATION TASKS

Tools – Script Invocation tasks run a program on a Skybox machine (for example, on a machine running a Skybox Collector, a **Tools – Script Invocation** task could run a program to move data to a location from where Skybox can import it).

Task properties

The properties that control **Tools – Script Invocation** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the program.
Program	The full path to the program to be run; include the program name. See the note immediately following this table.
Arguments	A space-separated list of the arguments to use when the program is run. If **User** and **Password** are specified in the **Advanced** tab, use %u and %p in the string for these properties. If **Additional User** and **Additional Password** are specified in the **Advanced** tab, use %u2 and %p2 in the string for these properties. (Use %% if % is required in the argument string.)
Import iXML	Specifies whether the program produces an iXML file to import into the model.
iXML file path	This field is enabled only if you select **Import iXML**. The full path to the iXML file produced by the program.
Advanced tab	
Save output to file	Specifies whether to save the program's output to a file. If selected, Skybox saves the output to `<Skybox_Home>\data\collector\temp\SimpleExecution_<Skybox generated value>.txt`.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. Use this field if a user name is required as an argument for the specified program. The value in this field is represented by %u in the argument string passed to the program.
Password	This field is displayed if **Method** = **Device**. Use this field if a password is required as an argument for the specified program. The value in this field is represented by %p in the argument string passed to the program.
Additional Username	This field is displayed if **Method** = **Device**. Use this field if an additional user name is required as an argument for the specified program. The value in this field is represented by %u2 in the argument string passed to the program.
Additional Password	This field is displayed if **Method** = **Device**. Use this field if an additional password is required as an argument for the specified program. The value in this field is represented by %p2 in the

Property	Description
	argument string passed to the program.
Safe	This field is displayed if **Method** = **CyberArk**. Use this field if a user name is required as an argument for the specified program. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. Use this field if a user name is required as an argument for the specified program. The name of the CyberArk object that contains the user name and password. The user name is represented by %u in the argument string passed to the program. The password (if required) is represented by %p in the argument string passed to the program.
Additional Safe	This field is displayed if **Method** = **CyberArk**. Use this field if an additional user name is required as an argument for the specified program. The name of the CyberArk safe that contains the additional user authentication credential object.
Additional Object	This field is displayed if **Method** = **CyberArk**. Use this field if an additional user name is required as an argument for the specified program. The name of the CyberArk object that contains the additional user name and password. The user name is represented by %u2 in the argument string passed to the program. The password (if required) is represented by %p2 in the argument string passed to the program.
Task Status	
Task Exit Status	• **Error**: Exit codes listed in **Script Exit Codes** signify failure. All other exit codes signify success. • **Success**: Exit codes listed in **Script Exit Codes** signify success. All other exit codes signify failure.
Script Exit Codes	A comma-separated list of exit codes used by **Task Exit Status**.

Important: If you run a Skybox Collector as a service on Windows, you cannot use a mapped network drive when specifying the full path in the **Program** field.

Workaround: Use the Universal Naming Convention (UNC) name: `\\<server name>\<share name>\<directory>\<file name>`.

IMPORTING INTERFACE AND ROUTING CONFIGURATION

Note: We recommend that you use an **Import – Directory** task to import the configuration data; the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

On some assets (usually firewalls), the access rules and routing rules are controlled by different software. On Check Point firewalls, for example, firewall software manages the access rules but the operating system controls interfaces and routing.

You can import routing table and network interface information from the following operating systems:

- Windows
- Linux
- Solaris

The following files are required to import the configuration data:

- `ifconfig.txt`: The interfaces configuration report

  This file is the output of:

  - (Linux and Solaris) The `ifconfig -a` command
  - (Windows) The `ipconfig` command

- `netstat.txt`: The network status report

  This file is the output of:

  - (Linux and Solaris) The `netstat -rvn` command
  - (Windows) The `netstat -r` command

Chapter 4

Firewall configuration tasks

This chapter describes how to add firewall configuration data to the current model.

In this chapter

BLUE COAT PROXY

You can add or update configuration data from Blue Coat proxies to the current model:

- Using an online collection task:

- Configure the proxies (see page 64) to permit access from a Skybox Collector and create a task (see page 64) to collect the proxy configurations and add the configuration data to the model.

  The collection task can collect data from multiple proxies.

- Using an offline file import task:
  - Generate and retrieve proxy configuration files and import their data into the model (see page 65).

    The file import task can import the data of multiple proxies.

Configuring Blue Coat proxies for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure a Blue Coat proxy for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Proxy – Blue Coat Collection tasks use the SSH protocol to connect to Blue Coat proxies.

Commands sent to device

Proxy – Blue Coat Collection tasks send the following commands to Blue Coat proxies:

- `enable`
- `show configuration noprompts`
- `show ip-route-table`

Blue Coat collection tasks

Proxy – Blue Coat Collection tasks retrieve configuration data from Blue Coat proxies and add this data to the current model.

Task properties

The properties that control **Proxy – Blue Coat Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Blue Coat proxies. **Note**: A task can collect the configurations of multiple proxies only if the same authentication is used for all the proxies.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from

Property	Description
	CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the proxies.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Enable Password	The password for enable command privileges on the proxies. If a password is not required, leave this field blank.
Port	The port on which the firewalls listen. If you change the default port (22) on the proxies, the Skybox Collector must have permission to connect to the proxies on the port that you specify.
Advanced tab	
Override device prompt	The proxy prompt. If this field is empty, the default prompt is expected: **#$**.
Override password prompt	The password prompt. If this field is empty, the default prompt is expected: **[p|P]assword:\s$**.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the proxies. **Note**: Use this property if different locations use the same set of IP addresses, so that proxies at different locations can have the same IP address.

Importing Blue Coat configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Blue Coat firewall configuration:

- `*.txt` or `*.log`: The Blue Coat configuration file

  This file is the output of the Blue Coat `show configuration` command.

- (Optional) `route.txt`: Dump of the Blue Coat routing table

  This file is the output of the Blue Coat `show ip-route-table` command.

You can import the configurations of multiple firewalls; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

Note: To run an **Import – Collector** task or an **Import – Collector Advanced** task, the Skybox Collector specified for the task must reside on a Linux platform.

CHECK POINT FIREWALL-1 FIREWALL

Configuration data

You can add or update configuration data from Check Point FireWall-1 NG and NGX firewalls (R77 and lower) to the current model:

- Using an online collection task:
  - Configure the firewall Management Servers (see page 66) to permit access from a Skybox Collector and create a collection task (see page 74) to collect the firewall configurations and add the configuration data to the model.

    The collection task can collect data from multiple firewalls.
- Using an offline file import task:
  - Retrieve firewall configuration files and import their data into the model (see page 77).

    The file import task can import the data of multiple firewalls.

To add or update configuration data from Check Point FireWall-1 Management Servers (R80 and higher), see Check Point Security Management (on page 91).

To add or update configuration data from Check Point Provider-1 Domain Servers (CMAs), which can manage multiple Check Point FireWall-1 firewalls, see Check Point Provider-1 Domain Server (on page 79).

Installed hotfixes

You can add or update the hotfixes installed on Check Point FireWall-1 NG and NGX firewalls to the current model:

- Using an online collection task:
  - Configure the firewalls (see page 78) to permit access from a Skybox Collector and create a collection task (see page 78) to collect the installed hotfixes and add the hotfix data to the model.

    The collection task can collect data from multiple firewalls.
- Using an offline file import task:
  - Retrieve firewall hotfix and configuration files and import their data into the model (see page 79).

    The file import task can import the data of multiple firewalls.

Configuring FireWall-1 Management Servers for CPMI data collection

To configure a Check Point FireWall-1 Management Server (R77 and lower) so that Skybox can retrieve FireWall-1 configuration data:

- Create a Permissions Profile (see page 68) (read-only) for Skybox data collection.

  Note: For Skybox Change Manager to implement change requests automatically, create a *read-write* profile instead. (See the Configuring automatic implementation section in the Skybox Change Manager User Guide).

- Get the IP address of the firewall (see page 70).
- Configure the OPSEC application (see page 71).
- Configure the Management Server to permit collection using the OPSEC protocol (see page 73).

Note: If your network includes a standby Management Server, repeat these steps for the standby system.

To perform rule usage analysis, you must also collect firewall activity log data (see Check Point FireWall-1 activity log data (on page 163)). When you configure the Management Server, we recommend that you:

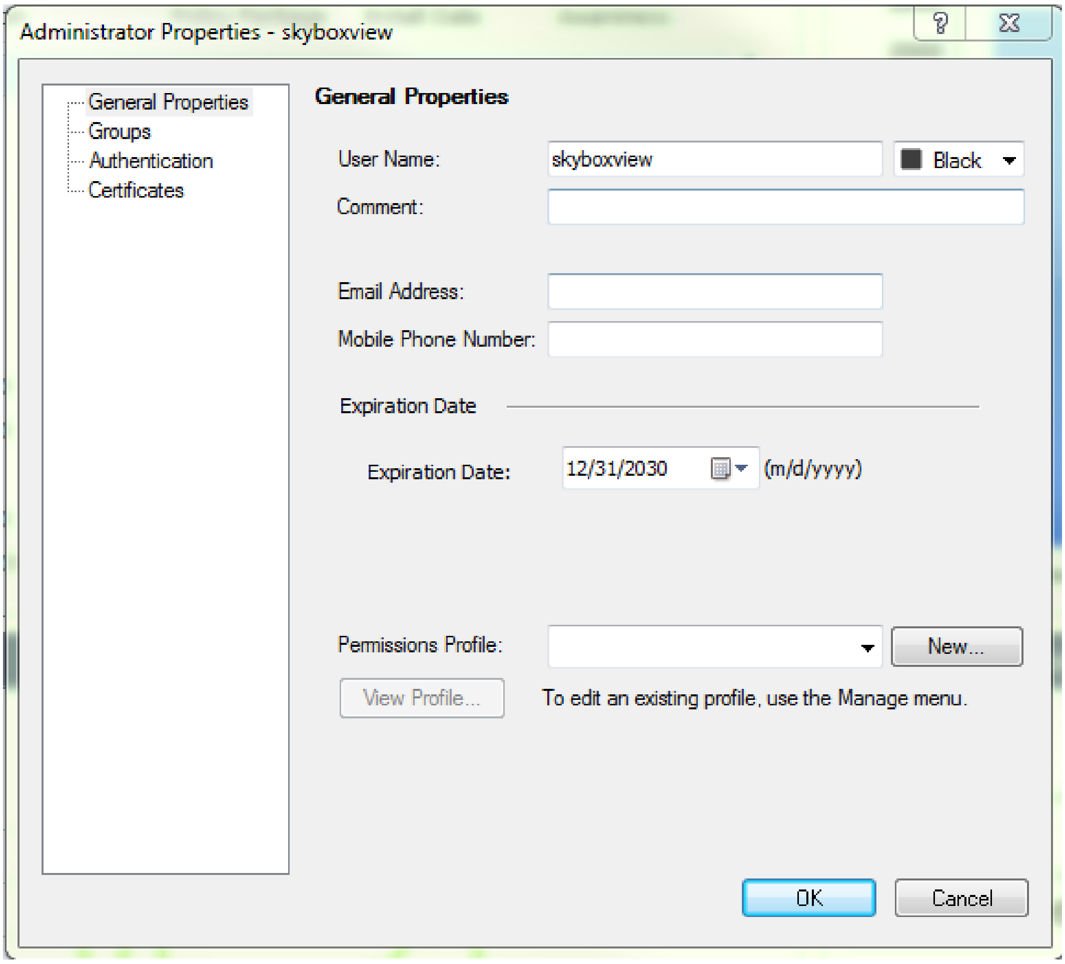
- Get the IP address of the device where the logs are stored (see page 74).
- (If the logs are on a log server) Install the OPSEC application database on the log server (see page 74).

Creating a Permissions Profile

To create a Permissions Profile

1 In Check Point SmartDashboard, select **Manage** > **Users and Administrators**.

2 Select **New** > **Administrator**.



Administrator Properties - skyboxview

General Properties

User Name: skyboxview

Black

Comment:

Email Address:

Mobile Phone Number:

Expiration Date

Expiration Date: 12/31/2030 (m/d/yyyy)

Permissions Profile:

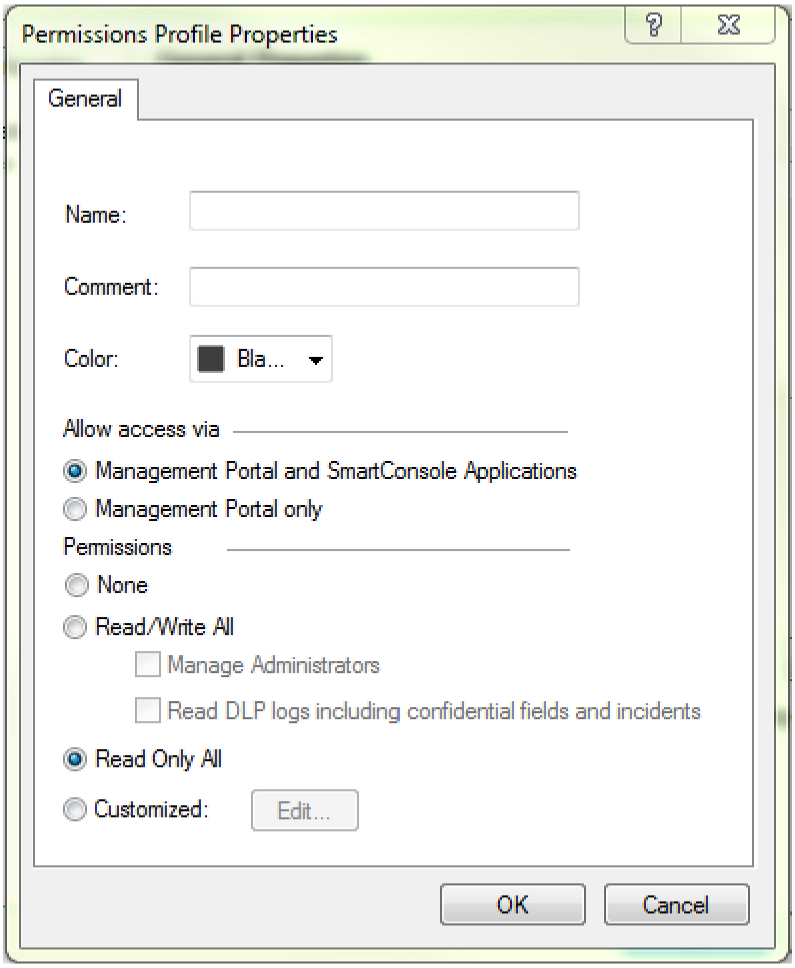
To edit an existing profile, use the Manage menu.

3 In the Administrator Properties dialog box, type **skyboxview** in the **Login Name** field.

4 Create a Permissions Profile:

a. Click **New**.

b. In the Permissions Profile Properties dialog box, fill in the fields.



Permissions Profile Properties

General

Name:

Comment:

Color: ■ Bla...

Allow access via

● Management Portal and SmartConsole Applications

○ Management Portal only

Permissions

○ None

○ Read/Write All

□ Manage Administrators

□ Read DLP logs including confidential fields and incidents

● Read Only All

○ Customized:

In the **Permissions** section:

- In general, select **Read Only All**.
- If you are working with Skybox Change Manager, select **Read / Write All** to permit Skybox Change Manager to implement change requests automatically.

  For additional information, see the Configuring automatic implementation section in the Skybox Change Manager User Guide.

c. Click **OK**.

5 Assign the Permissions Profile to the administrator:

a. Click the **Authentication** tab.

b. In the **Authentication Scheme** field, select **Check Point Password**.

c. Click **Enter Password**.

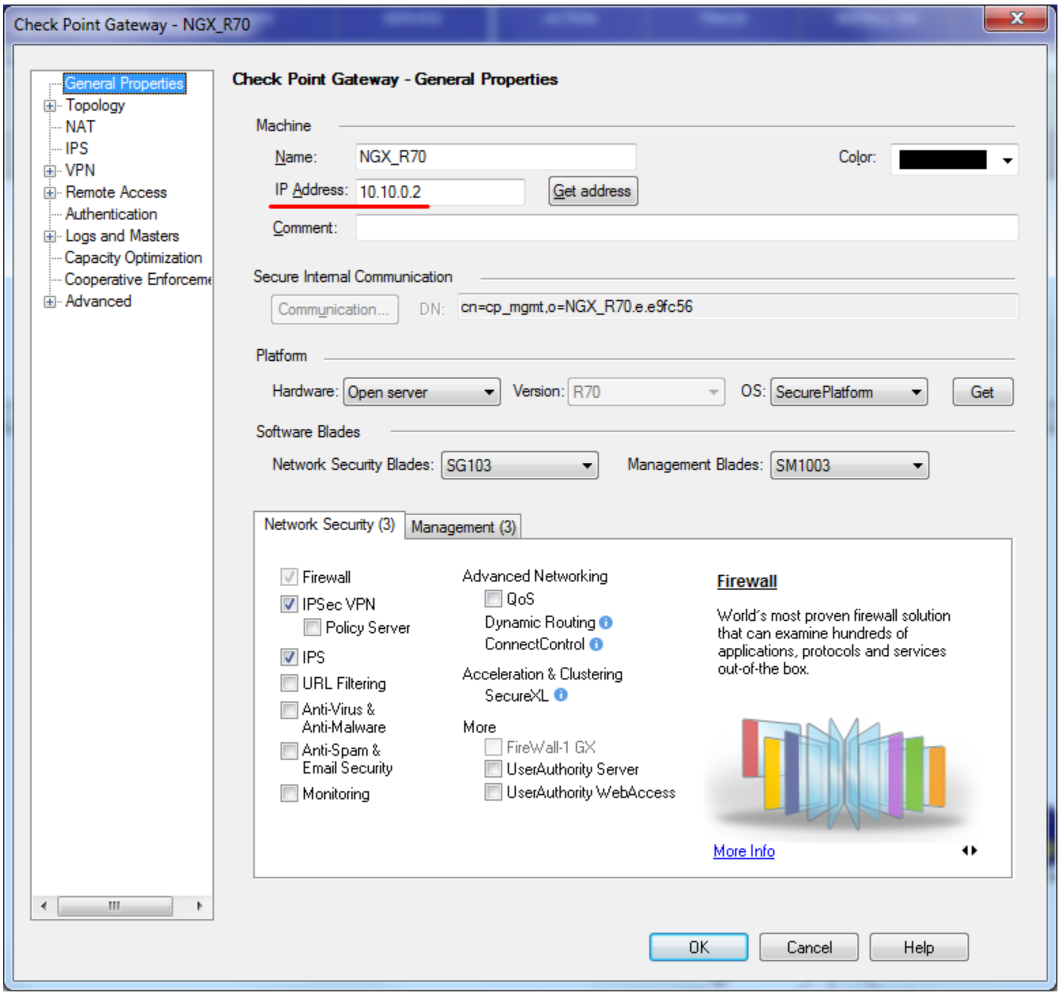
d. Type a password of your choice in the **Password** and **Confirm Password** fields and click **OK**.

6 Click **OK**.

Getting the IP addresses of FireWall-1 firewalls

To get the IP address of a firewall

1. In Check Point SmartDashboard, select **Manage** > **Network Objects**.
2. Select the FireWall-1 Management Server object from the drop-down list and click **Edit**.



Check Point Gateway - NGX_R70

Check Point Gateway - General Properties

Machine

Name: NGX_R70

IP Address: 10.10.0.2

Comment:

Color:

Secure Internal Communication

DN: cn=cp_mgmt,o=NGX_R70.e.e9fc56

Platform

Hardware: Open server

Version: R70

OS: SecurePlatform

Software Blades

Network Security Blades: SG103

Management Blades: SM1003

Network Security (3)

☑ Firewall
☑ IPSec VPN
□ Policy Server
☑ IPS
□ URL Filtering
□ Anti-Virus & Anti-Malware
□ Anti-Spam & Email Security
□ Monitoring

Advanced Networking
□ QoS
Dynamic Routing
ConnectControl

Acceleration & Clustering
SecureXL

More
□ FireWall-1 GX
□ UserAuthority Server
□ UserAuthority WebAccess

Firewall

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

3. Note the content of the **IP Address** field; you need this information when you create the firewall collection task.
4. Close the Properties dialog box.

Configuring OPSEC applications for FireWall-1

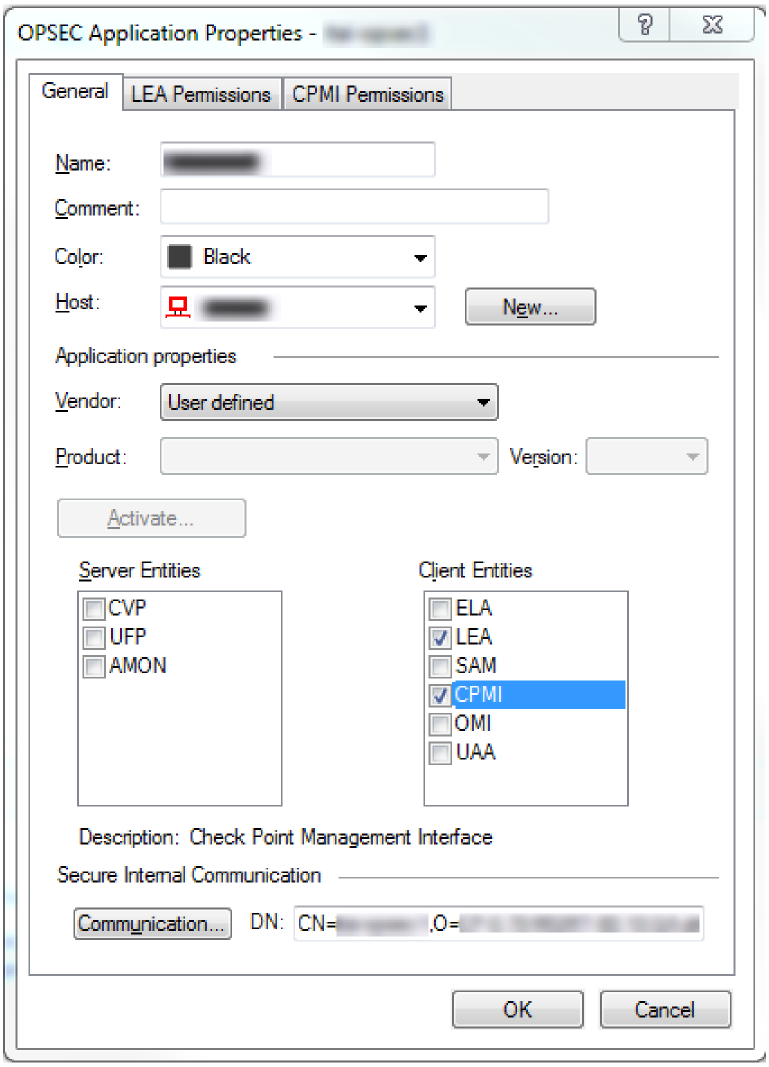
To configure the OPSEC application

1 Launch Check Point SmartDashboard.

2 Verify that the Skybox Collector machine is defined in SmartDashboard.

3 In SmartDashboard, select **Manage** > **Servers and OPSEC Applications**.

4 In the OPSEC Applications dialog box, click **New** and select **OPSEC Application**.



OPSEC Application Properties - [redacted]

Name: [redacted]

Comment:

Color: Black

Host: [redacted]

Application properties

Vendor: User defined

Product: Version:

Server Entities

□ CVP
□ UFP
□ AMON

Client Entities

□ ELA
☑ LEA
□ SAM
☑ CPMI
□ OMI
□ UAA

Description: Check Point Management Interface

Secure Internal Communication

DN: CN=[redacted],O=[redacted]

5 In the OPSEC Applications Properties dialog box:

a. Give the OPSEC application a name.

Note this name; you need it when you create the firewall collection task.

> Note: We recommend that you use **Skybox**—the default name that Skybox uses when retrieving a new certificate.

b. In the **Host** field, select the Skybox Collector machine.

c. In the **Client Entities** box:

i. Select **CPMI**.

ii. (Recommended—mandatory for rule usage analysis) Select **LEA**.

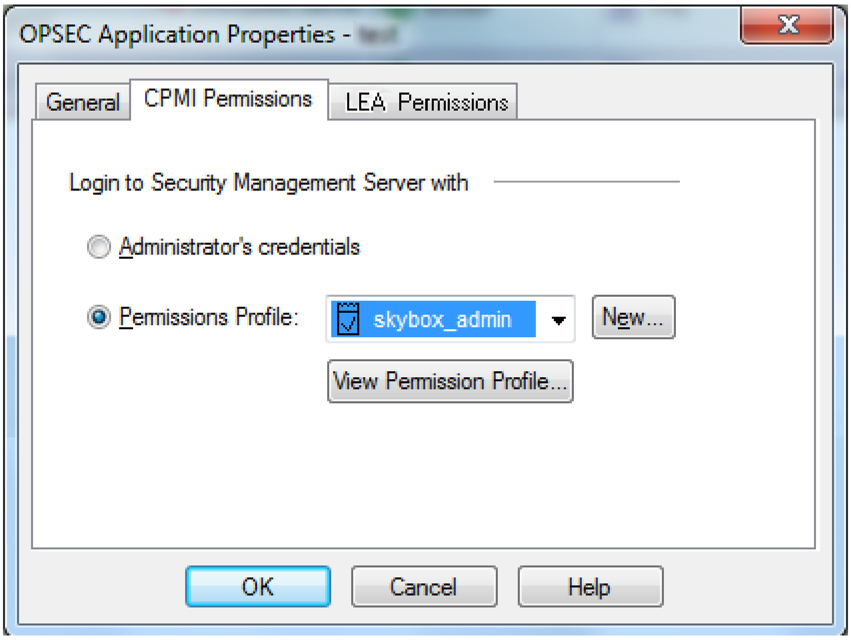
d. Click **Communications** and type an activation key.

The activation key is a one-time password that is used to create the certificate for authentication and encryption between the Skybox Collector and the Domain Server (CMA); you need the key when you create the firewall collection task.

e. Click **Initialize**.

f. Click **Close**.

g. Click the **CPMI Permissions** tab.



OPSEC Application Properties - [redacted]

Login to Security Management Server with

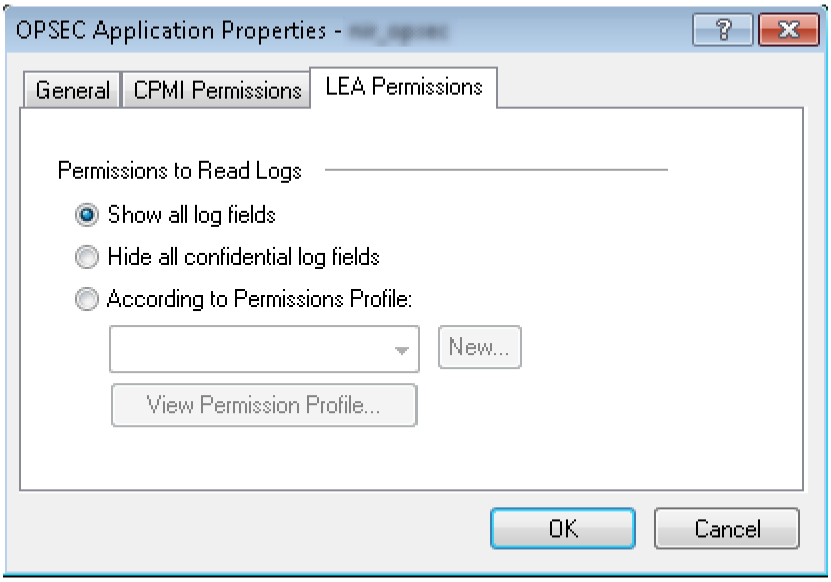
○ Administrator's credentials

● Permissions Profile: skybox_admin

h. Select the **Permissions Profile** that you created for the collection task (see Creating a Permissions Profile (on page 68)).

i. (Recommended—mandatory for rule usage analysis. Only available if you checked **LEA** at step **c2**.)

i. Click the **LEA Permissions** tab.



OPSEC Application Properties - [redacted]

Permissions to Read Logs

● Show all log fields

○ Hide all confidential log fields

○ According to Permissions Profile:

ii. Select **Show all log fields**.

j. Click **OK** to close the OPSEC Application Properties dialog box.

6 Click **Close** to close the OPSEC Applications dialog box.

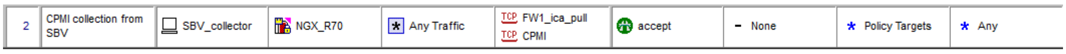
7 Save the changes.

Configuring FireWall-1 firewalls to permit collection

To configure a firewall to permit collection

1 Add an access rule in the firewall to permit the Skybox Collector to use the services required for the collection process.

> Note: This is only necessary if the connection between the Skybox Collector and the FireWall-1 Management Server is blocked by the firewall.



2	CPMI collection from SBV	SBV_collector	NGX_R70	Any Traffic	TCP FW1_ica_pull TCP CPMI	accept	- None	* Policy Targets	* Any

Use the following values for the access rule:

Source: Skybox Collector

Destination: FireWall-1 Management Server

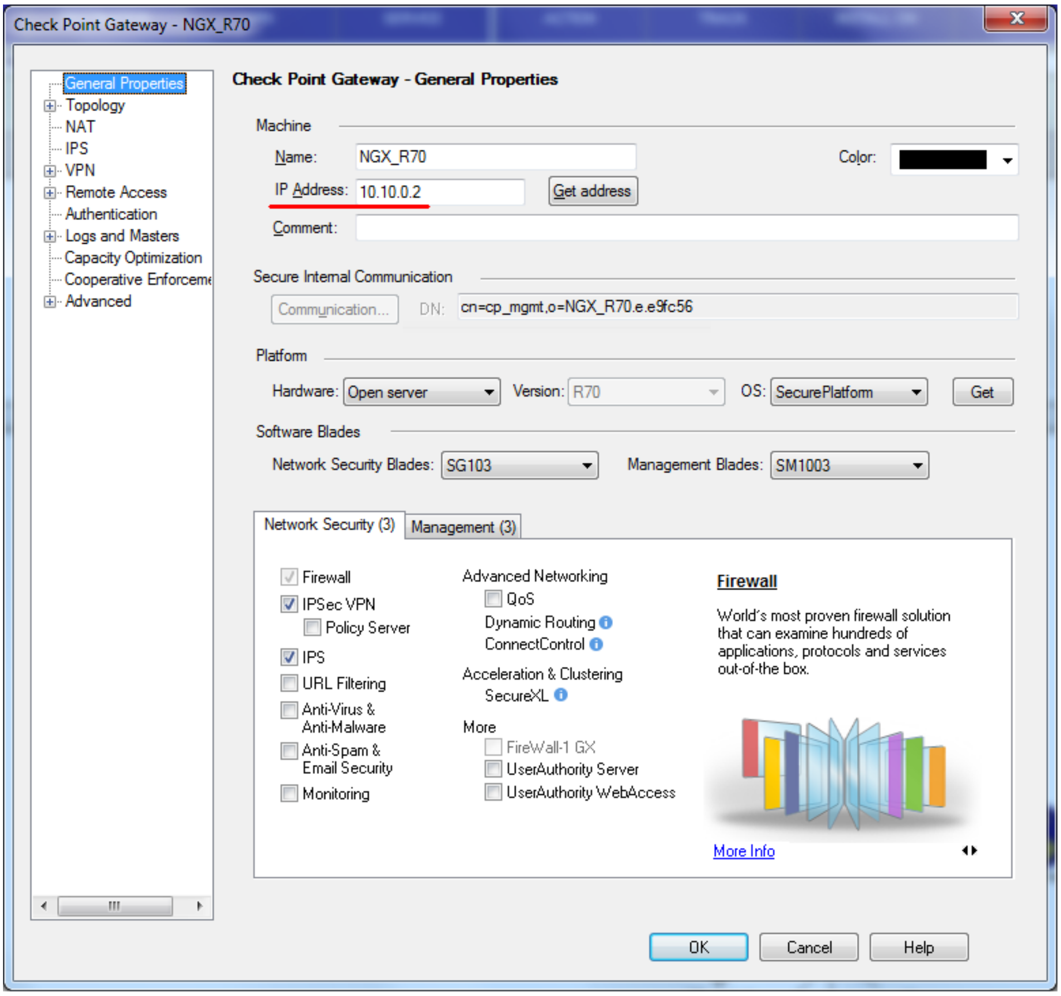
Services: FW1_ica_pull (18210/TCP), CPMI (18190/TCP), LEA (18184/TCP)

2 Install the policy on the firewall.

Getting the IP addresses of FireWall-1 log servers

To get the IP address of a device

1. In Check Point SmartDashboard, select **Manage** > **Network Objects**.
2. Select the device holding the logs (either the FireWall-1 Management Server object or the log server) from the drop-down list and click **Edit**.



Check Point Gateway - NGX_R70

Check Point Gateway - General Properties

Machine

Name: NGX_R70

IP Address: 10.10.0.2

Comment:

Color: ■

Secure Internal Communication

DN: cn=cp_mgmt,o=NGX_R70.e.e9fc56

Platform

Hardware: Open server

Version: R70

OS: SecurePlatform

Software Blades

Network Security Blades: SG103

Management Blades: SM1003

Network Security (3)

☑ Firewall
☑ IPSec VPN
□ Policy Server
☑ IPS
□ URL Filtering
□ Anti-Virus & Anti-Malware
□ Anti-Spam & Email Security
□ Monitoring

Advanced Networking
□ QoS
Dynamic Routing
ConnectControl

Acceleration & Clustering
SecureXL

More
□ FireWall-1 GX
□ UserAuthority Server
□ UserAuthority WebAccess

Firewall

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

3. Note the content of the **IP Address** field; you need this information when you create the firewall collection task.
4. Close the Properties dialog box.

Installing OPSEC application databases on log servers

To install an OPSEC application database on a log server

1. Launch Check Point SmartDashboard.
2. Select **Policy** > **Install Databases**.
3. Select the log server.
4. Click **Install**.

Check Point FireWall-1 CPMI collection tasks (FireWall-1)

Firewalls – Check Point FireWall-1 CPMI Collection tasks retrieve configuration data from a Check Point FireWall-1 Management Server (R77 and lower) and add this data to the current model.

- To retrieve configuration data from Check Point FireWall-1 Management Servers (R80 and higher), see Check Point R80 Security Management collection tasks (on page 96).

For VSX (virtual systems) firewalls, configuration data for all the virtual firewalls is retrieved.

Note: Create a separate CPMI collection task for each FireWall-1 Management Server.

Task properties

The properties that control **Firewalls – Check Point FireWall-1 CPMI Collection** tasks when collecting data from FireWall-1 Management Servers are described in the following table.

Property	**Description**
Basic tab	
Management Server	The IP address of the FireWall-1 Management Server. **Note**: Provide the IP address, not the asset name.
Firewall Filter	Specifies whether to collect configuration data of all (managed) firewalls, firewalls with a change event since the most recent collection (including new firewalls), or new firewalls only.
Initialize	
Certificate Issue Date	• If this field is empty, the connection to the Management Server is not initialized • <Timestamp>: The timestamp of the authentication certificate To retrieve an authentication certificate, click **Initialize Certificate** to open the Initialize Certificate dialog box (see page 77).
Authentication	If a Permissions Profile exists, the task uses the profile; any values entered in this section are ignored.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name of the administrator to access the Management Server.
Password	This field is displayed if **Method** = **Device**. The administrator password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the administrator authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the administrator name and password.
Collection	

Property	Description
Collect Active Policy	Specifies whether to collect the *active policy*. The active policy is the policy (rulebase) installed on the firewall.
Rulebase	This field is disabled if you select **Collect Active Policy**. The name of the policy to collect. • If you know the name of the policy, type it. • Click **Fetch** to retrieve a list of available policies from the Management Server.
Modules List	A comma-separated (or semicolon-separated) list of the names of FireWall-1 Enforcement Modules to collect.
SIC Name	The DN of the Management Server. Skybox displays the value from the authentication certificate that it retrieves when you initialize the connection. Do not change this value.
Advanced tab	
Location Hint	The location of the FireWall-1 Management Server. **Note**: Use this property if different locations use the same set of IP addresses, so that Management Servers at different locations can have the same IP address.
OPSEC Application	The name given to the OPSEC application when it was configured for Skybox (see Configuring OPSEC applications for FireWall-1 (on page 71)). Skybox displays the name that you provided when you initialized the connection.
SIC Name from MDS	Leave this check box cleared if you are collecting data from a FireWall-1 Management Server.
Do Not Merge	Specifies whether to collect configuration data but not merge it into the model. Configuration data files are saved under `<Skybox_Home>\data\collector\temp\`.
Secondary Management	The IP address of the standby FireWall-1 Management Server. **Note**: Provide the IP address, not the asset name.
Certificate Issue Date	• If this field is empty, the connection to the standby Management Server is not initialized • <Timestamp>: The timestamp of the authentication certificate To retrieve an authentication certificate, click **Initialize Certificate** to open the Initialize Certificate dialog box (see page 77).
Username	The user name of the administrator to access the standby Management Server.
Password	The standby administrator password.
Secondary SIC Name	The DN of the standby Management Server. Skybox displays the value in the authentication certificate it retrieves when you initialize the connection.

Initializing a certificate for FireWall-1

The Initialize Certificate dialog box properties are described in the following table.

Property	Description
Use existing certificate	Use the authentication certificate that Skybox retrieved previously from the OPSEC application.
OPSEC Application	The name given to the OPSEC application when it was configured for Skybox (see Configuring OPSEC applications for FireWall-1 (on page 71)).
Date	The date of the authentication certificate.
Retrieve new certificate	Retrieve a new authentication certificate from the OPSEC application.
OPSEC Application	The name given to the OPSEC application when it was configured for Skybox (see Configuring OPSEC applications for FireWall-1 (on page 71)).
Activation Key	The activation key created in SmartDashboard when configuring the OPSEC application (see Configuring OPSEC applications for FireWall-1 (on page 71)).

Importing Check Point FireWall-1 configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Check Point FireWall-1 configuration:

- `objects_5_0.c`: The network objects file contains objects (including assets, networks, and services) referenced in the access rules.
- `rulebases_5_0.fws`: The rulebase file contains the access rules.
- (Optional) `install_statuses.c`: The installed statuses file includes the name of the policy (the active policy) that is installed on the firewall.

  Note: If the Check Point configuration contains multiple policies, `install_statuses.c` is mandatory (it specifies the policy that is installed on each firewall).

- (Optional) `vsx_objects.c`: The VSX device objects file contains objects (including assets, networks, and services) referenced in the access rules of VSX (virtual systems) firewalls.

These files are in:

- (Windows) `C:\WINDOWS\FW1\<version#>\conf`
- (Linux) `/<FireWall-1 installation path>/CPfw1-<version#>/conf`

You also need:

- The name of the active policy on each firewall module
- (Optional—required to import VSX data) The output of the following commands from each firewall module:

- `ifconfig -a` (as `ifconfig.txt`)

> Note: Before running the `ifconfig -a` command, run vsenv `<VS ID>`

- `netstat –rnv` (as `netstat.txt`)

For Import – Basic tasks

When you copy files from the remote device, note the module names of the firewalls that you are importing.

You can import multiple firewalls managed by the same Management Server by specifying firewall names in the **Module List** field. Store the set of files from each Management Server in a separate 1st-level subdirectory of the specified directory.

Configuring FireWall-1 Management Servers for hotfix collection

To configure a FireWall-1 firewall for hotfix collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.
- Configure the firewall to permit collection. (The Skybox Collector must have permission to connect to the firewall using SSH.)
- (Version R76) Switch the firewall from clish mode to Expert mode.

Connection type

Firewalls – Check Point FireWall-1 Hotfix Collection tasks use the SSH protocol to connect to FireWall-1 firewalls.

Commands sent to device

Firewalls – Check Point FireWall-1 Hotfix Collection tasks send the following command to FireWall-1 firewalls:

- `cpinfo –y all`

Check Point FireWall-1 hotfix collection tasks

Firewalls – Check Point FireWall-1 Hotfix Collection tasks retrieve information about the running version and all the installed patches (hotfixes) from FireWall-1 firewalls and add this information to the current model.

> Note: For FireWall-1 firewalls running version R76, configure the firewall to run in Expert mode.

After running a **Firewalls – Check Point FireWall-1 Hotfix Collection** task, run an **Analysis – Vulnerability Detector for Network Devices** task to create the relevant vulnerability occurrences.

To view the hotfix information

- (In the Firewall Assurance workspace) Right-click the **All Firewalls** > **<firewall name>** > **Configuration Compliance** node and select **Patches**.
- (In the Model workspace) Select **All Network Devices** > **Firewalls**; select a firewall in the Table pane and then click the **Patches** tab in the Details pane.

Task properties

The properties that control **Firewalls – Check Point FireWall-1 Hotfix Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	(Read-only) The connection protocol to use.
SSH Port	The port on which the firewalls listen. If you change the default port (22) on the firewalls, the Skybox Collector must have permission to connect to the firewalls on the port that you specify.
Firewall Addresses	A comma-separated list of the IP addresses and IP address ranges of the FireWall-1 firewalls. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Firewall Filter	Specifies whether to collect all firewalls or only firewalls with a change event since the most recent collection.
Authentication	
Username	The user name to access the firewalls.
Password	The user password.
Advanced tab	
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

Importing Check Point FireWall-1 hotfix data

You can use an **Import – Directory** task to import Check Point FireWall-1 hotfix data.

The following files are required to import hotfixes:

- `cpinfo.txt`: The Check Point hotfix information
- `ifconfig.txt`: The interfaces configuration

CHECK POINT PROVIDER-1 DOMAIN SERVER

Check Point Provider-1 Domain Servers (CMAs) manage multiple Check Point FireWall-1 NG and NGX firewalls.

You can add or update configuration data of the Check Point FireWall-1 NG and NGX firewalls managed by a Check Point Provider-1 Domain Server to the current model:

- Using an online collection task:
  - Configure the Domain Server (see page 80) to permit access from a Skybox Collector and create a collection task (see page 86) to collect the firewall configurations and add them to the model.

The collection task can collect data from multiple Check Point FireWall-1 NG and NGX firewalls managed by 1 Domain Server.

- Using an offline file import task:
  - Retrieve Domain Server configuration files and import their data into the model (see page 88).

  The file import task can import the data of multiple Domain Servers.

To add or update configuration data from Check Point FireWall-1 Management Servers (R77 and lower), see Check Point FireWall-1 firewall (on page 66).

To add or update configuration data from Check Point FireWall-1 Management Servers (R80 and higher), see Check Point Security Management (on page 91).

Configuring Provider-1 for firewall data collection

To configure Check Point Provider-1 Domain Servers (CMAs) so that Skybox can retrieve FireWall-1 configuration data:

- Create a Domain Permission Profile (see page 80) for Skybox data collection.
- Get the IP addresses of the Domain Servers (see page 83).
- Configure the OPSEC applications (see page 83) (do this for each Domain Server).
- Configure each Domain Server to permit collection using the OPSEC protocol (see page 86).

Note: If your network includes a standby MDS, repeat these steps for the standby server.

To perform rule usage analysis, you must also collect firewall activity log data (see Check Point FireWall-1 activity log data (on page 163)). When you configure the Domain Servers, we recommend that you:

- Get the IP address of the device where the logs are stored (see page 74).
- (If the logs are on a log server) Install the OPSEC application database on the log server (see page 74).

Creating a Domain Permission Profile

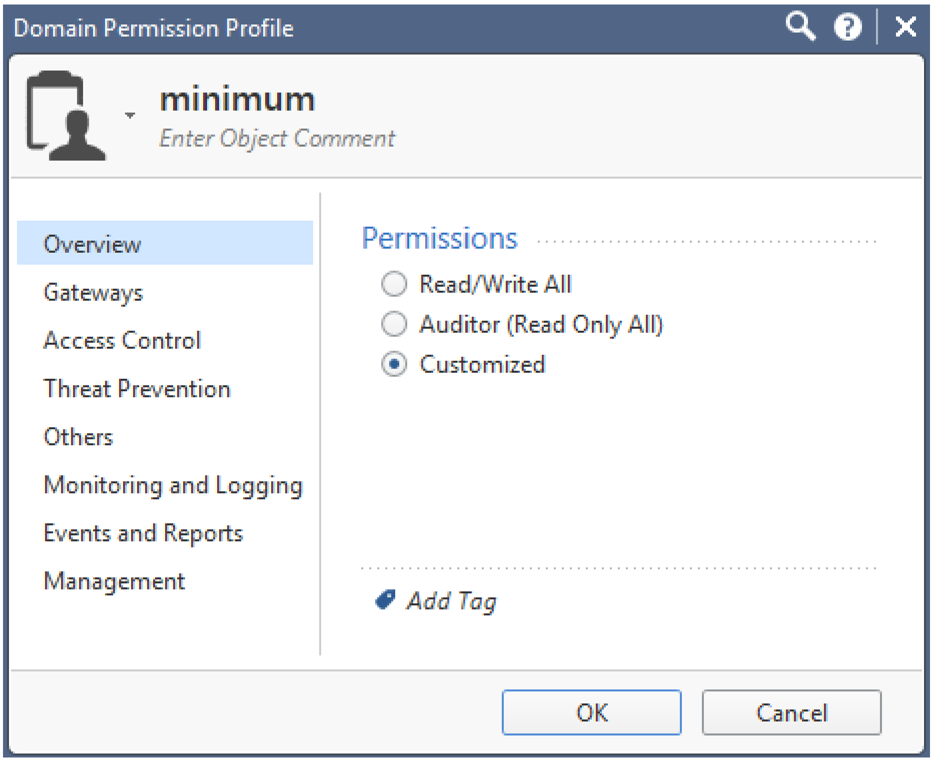
To retrieve Check Point firewall configuration data from Provider-1 Domain Servers (CMAs), you must create a customized Domain Permission Profile.

To create a Domain Permission Profile

1. Create a Domain Permission Profile and give it a name.

   (In the screen captures shown in this procedure, the Domain Permission Profile is named **minimum**.)

2 In the **Overview** tab of the Domain Permission Profile dialog box, set **Permissions** to **Customized**.



Domain Permission Profile

minimum

Enter Object Comment

Permissions

○ Read/Write All

○ Auditor (Read Only All)

● Customized

3 In the **Gateways** tab:

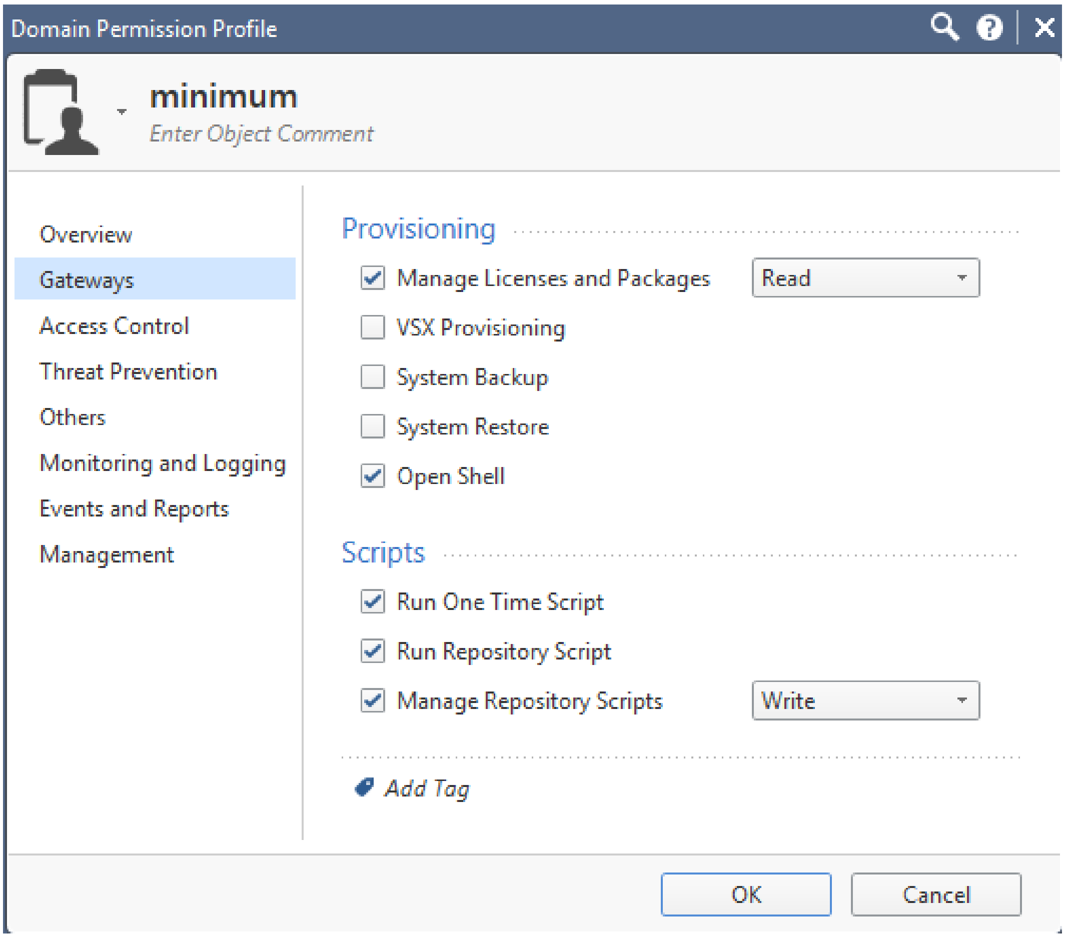
a. In the Provisioning area:

- Select **Manage Licenses and Packages** and set it to **Read**.
- Select **Open Shell**.

b. In the Scripts area:

- Select **Run One Time Script**, **Run Repository Script**, and **Manage Repository Scripts**.

– Set **Manage Repository Scripts** to **Write**.



Domain Permission Profile

minimum

Enter Object Comment

Provisioning

☑ Manage Licenses and Packages: Read

□ VSX Provisioning

□ System Backup

□ System Restore

☑ Open Shell

Scripts

☑ Run One Time Script

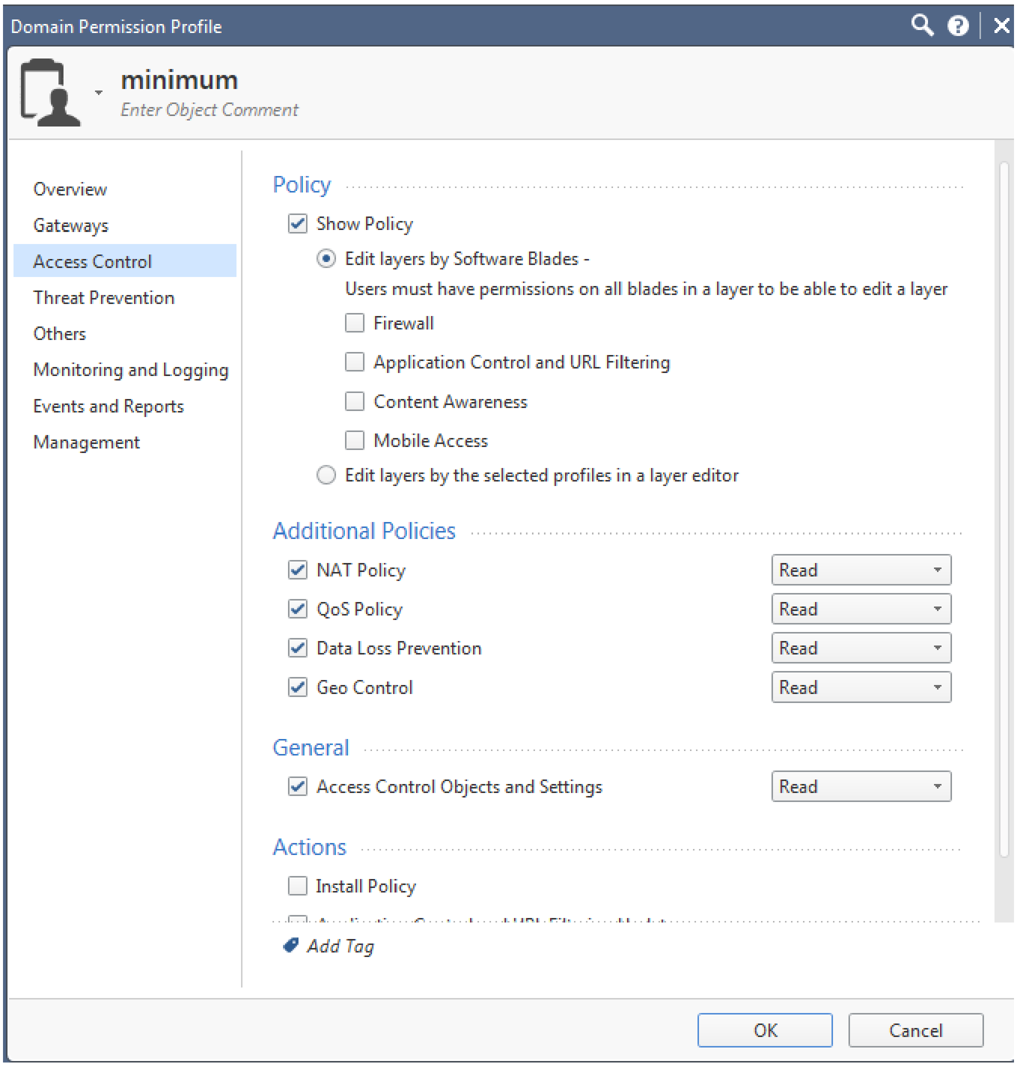
☑ Run Repository Script

☑ Manage Repository Scripts: Write

4 In the **Access Control** tab:

a. In the Policy area, clear all the Software Blades (as shown in the screen capture).

b. Select all the Additional Policies and set them to **Read**.



Policy

☑ Show Policy

● Edit layers by Software Blades -
Users must have permissions on all blades in a layer to be able to edit a layer

□ Firewall

□ Application Control and URL Filtering

□ Content Awareness

□ Mobile Access

○ Edit layers by the selected profiles in a layer editor

Additional Policies

☑ NAT Policy Read

☑ QoS Policy Read

☑ Data Loss Prevention Read

☑ Geo Control Read

General

☑ Access Control Objects and Settings Read

Actions

□ Install Policy

5 Click **OK** to save the new Domain Permission Profile.

Getting IP addresses of Domain Servers

To get the IP addresses of the Domain Servers (CMAs)

1 In the Check Point Provider-1 or SiteManager-1 UI, click the **General** icon.

2 Select **View** > **MDS Contents Mode**.

3 In the Provider-1 or SiteManager-1 tree, double-click each Domain Server and note its IP address; you need this information when you create the firewall collection task.

Configuring OPSEC applications for Provider-1

To configure the OPSEC applications

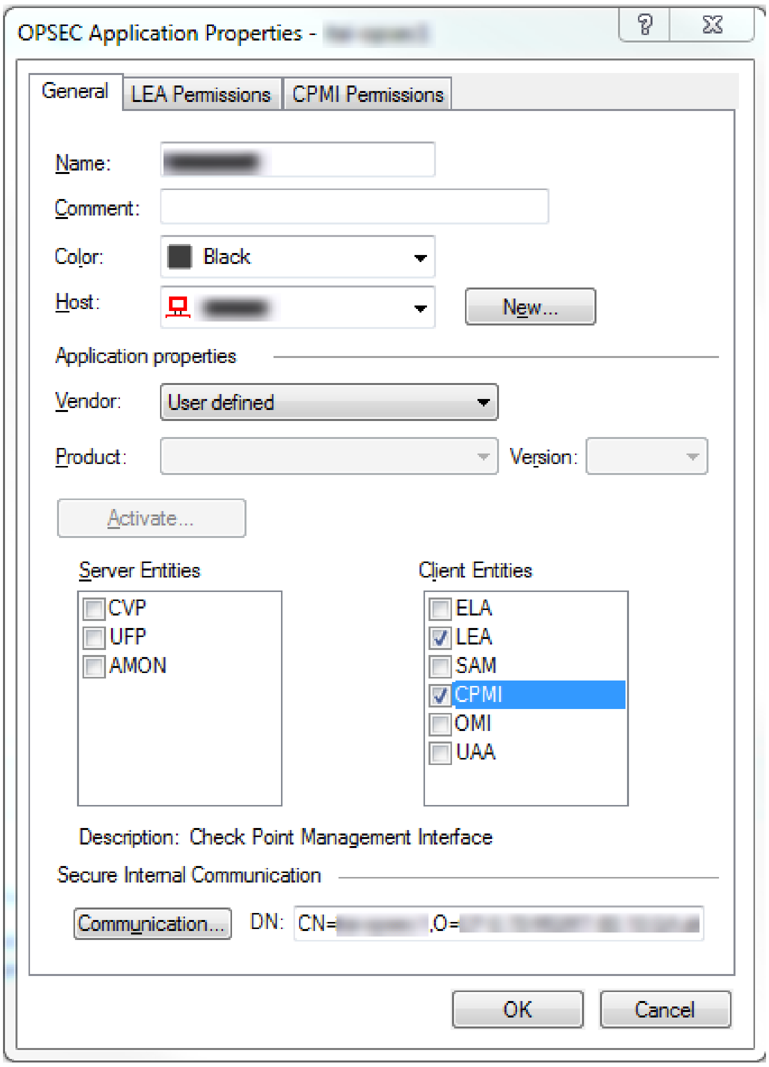
Note: Do the following for each Domain Server (CMA).

1 Launch Check Point SmartDashboard on the Domain Server.

2 Verify that the Skybox Collector machine is defined in SmartDashboard.

3 In SmartDashboard, select **Manage** > **Servers and OPSEC Applications**.

4 In the OPSEC Applications dialog box, click **New** and select **OPSEC Application**.



OPSEC Application Properties - [redacted]

Name: [redacted]

Comment:

Color: Black

Host: [redacted]

Application properties

Vendor: User defined

Product:

Version:

Server Entities

□ CVP
□ UFP
□ AMON

Client Entities

□ ELA
☑ LEA
□ SAM
☑ CPMI
□ OMI
□ UAA

Description: Check Point Management Interface

Secure Internal Communication

DN: CN=[redacted],O=[redacted]

5 In the OPSEC Applications Properties dialog box:

a. Give the OPSEC application a name.

Note this name; you need it when you create the firewall collection task.

Note: We recommend that you use **Skybox**—the default name that Skybox uses when retrieving a new certificate.

b. In the **Host** field, select the Skybox Collector machine.

c. In the **Client Entities** box:

i. Select **CPMI**.

ii. (Recommended—mandatory for rule usage analysis) Select **LEA**.

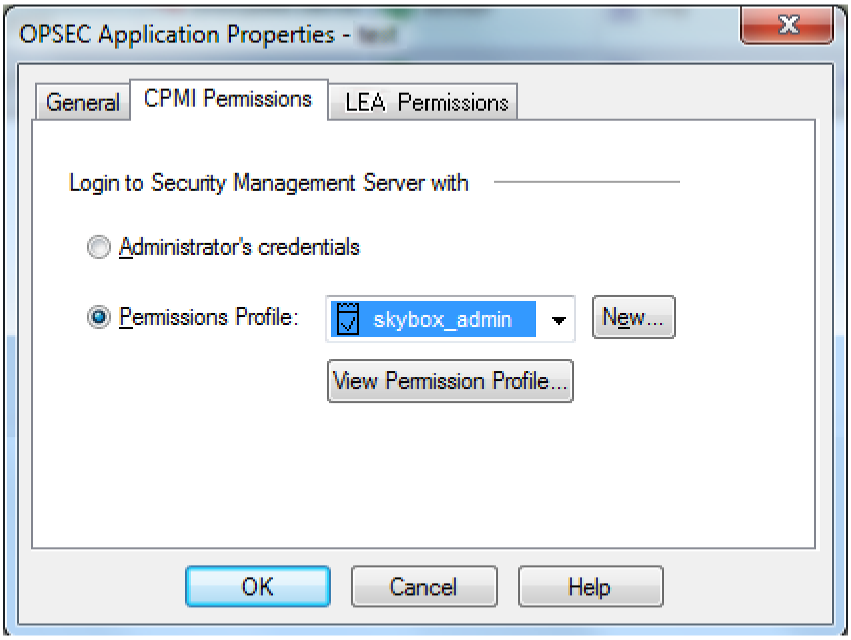
d. Click **Communications** and type an activation key.

The activation key is a one-time password that is used to create the certificate for authentication and encryption between the Skybox Collector and the Domain Server (CMA); you need the key when you create the firewall collection task.

e. Click **Initialize**.

f. Click **Close**.

g. Click the **CPMI Permissions** tab.



OPSEC Application Properties - [redacted]

Login to Security Management Server with

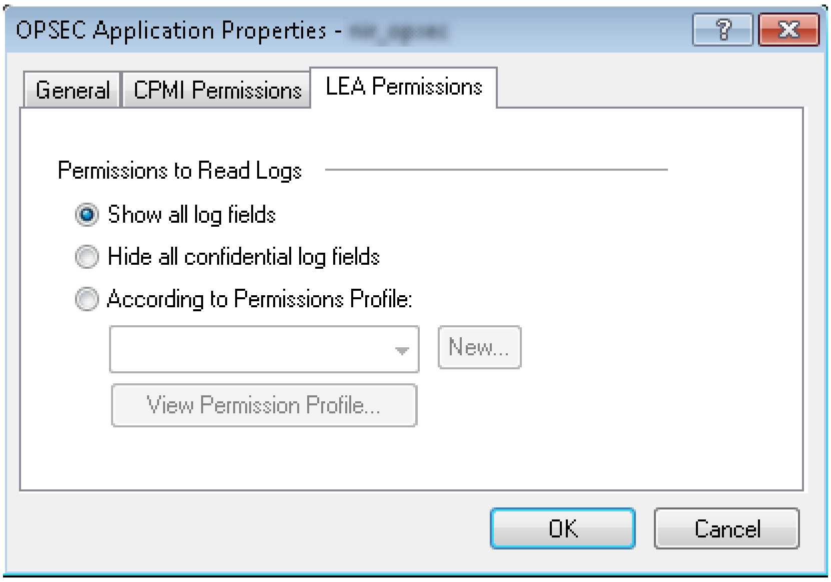
○ Administrator's credentials

● Permissions Profile: skybox_admin

h. Select the **Permissions Profile** that you created for the collection task (see Creating a Permissions Profile (on page 68)).

i. (Recommended—mandatory for rule usage analysis. Only available if you checked **LEA** at step **c2**.)

i. Click the **LEA Permissions** tab.



OPSEC Application Properties - [redacted]

Permissions to Read Logs

● Show all log fields

○ Hide all confidential log fields

○ According to Permissions Profile:

ii. Select **Show all log fields**.

j. Click **OK** to close the OPSEC Application Properties dialog box.

6 Click **Close** to close the OPSEC Applications dialog box.

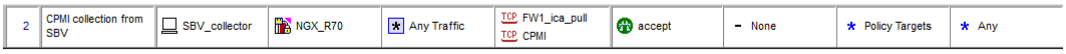
7 Save the changes.

Configuring Domain Servers to permit collection

To configure a Domain Server (CMA) to permit collection

1 Add an access rule in the Domain Server to permit the Skybox Collector to use the services required for the collection process.

Note: This is only necessary if the Skybox Collector and the Provider-1 Domain Server are not in the same segment.



2	CPMI collection from SBV	SBV_collector	NGX_R70	Any Traffic	TCP FW1_ica_pull TCP CPMI	accept	None	Policy Targets	Any

Use the following values for the access rule:

Source: Skybox Collector

Destination: Provider-1 Domain Server

Services: FW1_ica_pull (18210/TCP), CPMI (18190/TCP)

2 Install the policy on the Domain Server.

Check Point FireWall-1 CPMI collection tasks (Provider-1)

Firewalls – Check Point FireWall-1 CPMI Collection tasks retrieve the configuration data of Check Point FireWall-1 firewalls managed by a Check Point Provider-1 Domain Server (CMA) and add this data to the current model. For VSX (virtual systems) firewalls, configuration data for all the virtual firewalls is retrieved.

Note: Create a separate CPMI collection task for each Provider-1 Domain Server.

Task properties

The properties that control **Firewalls – Check Point FireWall-1 CPMI Collection** tasks when collecting data from Provider-1 Domain Servers are described in the following table.

Property	Description
Basic tab	
Management Server	The IP address of the Domain Server. (The Domain Server virtual IP address, not the MDS main IP address.) **Note**: Provide the IP address, not the name of the server.
Firewall Filter	Specifies whether to collect configuration data of all (managed) firewalls, firewalls with a change event since the most recent collection (including new firewalls), or new firewalls only.
Initialize	
Certificate Issue Date	• If this field is empty, the connection to the Domain Server is not initialized • <Timestamp>: The timestamp of the authentication certificate To retrieve an authentication certificate, click **Initialize Certificate** to open the Initialize Certificate dialog box (see page 88).

Property	Description
Authentication	If a Permissions Profile exists, the task uses the profile; any values entered in this section are ignored.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name of the MDS administrator to access the Domain Server.
Password	This field is displayed if **Method** = **Device**. The MDS administrator password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the MDS administrator authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the MDS administrator name and password.
Collection	
Collect Active Policy	Specifies whether to collect the *active policy*. The active policy is the policy (rulebase) installed on the firewall.
Rulebase	This field is disabled if you select **Collect Active Policy**. The name of the policy to collect. • If you know the name of the policy, type it. • Click **Fetch** to retrieve a list of available policies from the Domain Server.
Modules List	A comma-separated (or semicolon-separated) list of the names of FireWall-1 Enforcement Modules to collect.
SIC Name	The global DN of the Provider-1 Domain Server. Skybox displays the value from the authentication certificate that it retrieves when you initialize the connection. Do not change this value. **Note**: As an alternative to using each Domain Server SIC name, you can use the MDS SIC name. In this case, select **SIC Name from MDS** in the **Advanced** tab.
Advanced tab	
Location Hint	The location of the Domain Server. **Note**: Use this property if different locations use the same set of IP addresses, so that Domain Servers at different locations can have the same IP address.
OPSEC Application	The name given to the OPSEC application for this Domain Server when it was configured for Skybox (see Configuring OPSEC applications for Provider-1 (on page 83)). Skybox displays the name that you provided when you initialized the connection.

Property	Description
SIC Name from MDS	Specifies whether, exceptionally, **SIC Name** (in the **Basic** tab) is taken from the MDS rather than the Domain Server.
Do Not Merge	Specifies whether to collect device configuration data but not merge it into the model. Configuration data files are saved under `<Skybox_Home>\data\collector\temp\`.
Secondary Management	The IP address of the standby Domain Server. (The Domain Server virtual IP address, not the MDS main IP address.) **Note**: Provide the IP address, not the name of the server.
Certificate Issue Date	• If this field is empty, the connection to the standby Domain Server is not initialized • <Timestamp>: The timestamp of the authentication certificate To retrieve an authentication certificate, click **Initialize Certificate** to open the Initialize Certificate dialog box (see page 88).
Username	The user name of the MDS administrator to access the standby Domain Server.
Password	The standby MDS administrator password.
Secondary SIC Name	The global DN of the standby Domain Server. Skybox displays the value in the authentication certificate it retrieves when you initialize the connection.

Initializing a certificate for Provider-1

The Initialize Certificate dialog box properties are described in the following table.

Property	Description
Use existing certificate	Use the authentication certificate that Skybox retrieved previously from the OPSEC application.
OPSEC Application	The name given to the OPSEC application when it was configured for Skybox (see Configuring OPSEC applications for Provider-1 (on page 83)).
Date	The date of the authentication certificate.
Retrieve new certificate	Retrieve a new authentication certificate from the OPSEC application.
OPSEC Application	The name given to the OPSEC application when it was configured for Skybox (see Configuring OPSEC applications for Provider-1 (on page 83)).
Activation Key	The activation key created in SmartDashboard when configuring the OPSEC application (see Configuring OPSEC applications for Provider-1 (on page 83)).

Importing Check Point Provider-1 Domain Server configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Check Point Provider-1 Domain Server (CMA) configuration:

- `objects_5_0.c`: The global network objects file in the `/<installation path>/CPmds-<version#>/conf` directory.

  Note: You must rename this file to `g_objects_5_0.c`.

- `objects_5_0.c`: The Domain Server network objects file contains objects (including assets, networks, and services) referenced in the access rules.
- `rulebases_5_0.fws`: The Domain Server rulebase file contains the access rules.
- (Optional) `install_statuses.c`: The installed statuses file includes the name of the policy (the active policy) that is installed on the firewall.

  Note: If the Check Point configuration contains multiple policies, `install_statuses.c` is mandatory (it specifies the policy that is installed on each firewall).

- (Optional) `vsx_objects.c`: The VSX device objects file contains objects (including assets, networks, and services) referenced in the access rules of VSX (virtual systems) firewalls.

These files are in the `/<installation path>/CPmds-<version#>/customers/<customer name>/CPfw1-<version#>/conf` directory.

You also need:

- The name of the active policy on each firewall module
- (Optional—required to import VSX data) The output of the following commands from each firewall module:
  - `ifconfig -a` (as `ifconfig.txt`)

    Note: Before running the `ifconfig -a` command, run `vsenv <VS ID>`

  - `netstat –rnv` (as `netstat.txt`)

For Import – Basic tasks

When you copy files from the remote device, note the module names of the firewalls that you are importing and the running policy name.

You can import multiple firewalls managed by the same SmartCenter or Domain Server by specifying firewall names in the **Module List** field. Store the set of files from each Domain Server in a separate 1st-level subdirectory of the specified directory.

CHECK POINT GAIA FIREWALL

Note: Add the basic configuration data of each firewall to the current model (by running a Check Point FireWall-1 CPMI collection task (see page 74) or a Check Point R80 Security Management collection task (see page 96), as relevant) before running a **Firewalls – Check Point Gaia Collection** task for the first time.

You can add or update configuration data from Check Point firewalls running Gaia to the current model using an online collection task:

- Configure the firewall gateway (see page 90) to permit access from a Skybox Collector and create a collection task (see page 90) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple firewalls.

Note: Skybox's default Configuration Policies are not supported on Gaia firewalls.

Configuring Gaia firewall gateways for data collection

To configure a Gaia firewall gateway for data collection:

- Skybox data collection requires a superuser on the gateway device; we recommend that you create a separate user for this purpose.
- Configure the firewall policy to permit collection. (The Skybox Collector must have permission to connect to the firewall using SSH.)
- (Version R76) Switch the firewall from clish mode to Expert mode.

Connection type

Firewalls – Check Point Gaia Collection tasks use the SSH protocol to connect to Gaia firewalls.

Commands sent to device

Firewalls – Check Point Gaia Collection tasks send the following commands to gateways of Gaia firewalls:

- `show configuration`

Check Point Gaia collection tasks

Firewalls – Check Point Gaia Collection tasks retrieve Gaia firewall configuration data from gateways of a Gaia Management Server and add this data to the current model.

Note: For firewalls running version R76, configure the firewall to run in Expert mode.

Task properties

The properties that control **Firewalls – Check Point Gaia Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	(Read-only) The connection protocol to use.
SSH Port	The port on which the Management Server listens. If you change the default port (22) on the firewall, the Skybox Collector must have permission to connect to the firewall on the port that you specify.
Gateway Address	The IP address of the relevant gateway of the Gaia Management Server.

Property	Description
	Note: Provide the IP address, not the asset name.
Firewall Filter	Specifies whether to collect all firewalls or only firewalls with a change event since the most recent collection.
Authentication	
Username	The user name to access the gateway shell.
Password	The user password.
Advanced tab	
Location Hint	The location of the Management Server. **Note**: Use this property if different locations use the same set of IP addresses, so that gateways at different locations can have the same IP address.

CHECK POINT SECURITY MANAGEMENT

Check Point Security Management platforms manage multiple Check Point FireWall-1 NG and NGX firewalls (R80 and higher).

You can add or update configuration data of the Check Point FireWall-1 NG and NGX firewalls managed by a Check Point Security Management platform to the current model using an online collection task:

- Configure the Security Management (see page 91) to permit access from a Skybox Collector and create a collection task (see page 96) to collect the firewall configurations and add them to the model.

  The collection task can collect data of multiple Check Point FireWall-1 NG and NGX firewalls managed by 1 Security Management.

To add or update configuration data from Check Point FireWall-1 Management Servers (R77 and lower), see Check Point FireWall-1 firewall (on page 66).

Configuring Check Point Security Management for data collection

To configure a Check Point Security Management (R80 and higher) platform so that Skybox can retrieve FireWall-1 configuration data:

- Skybox data collection requires an administrator with a customized read-only Domain Permission Profile and a read-only Multi-Domain Permission Profile on the device; we recommend that you create a separate administrator for this purpose:
  - Create the Permission Profiles (see page 92) for Skybox data collection.
  - Create an administrator (see page 94)
- Activate the Security Management API and confirm that the API is running (see page 95).

To collect VSX routing rules from a Management Server (not required if you are collecting from a Multi-Domain Server):

- Create a Permissions Profile (see page 68) for Skybox data collection.
- Configure the OPSEC application (see page 71).

- Configure the Management Server to permit collection using the OPSEC protocol (see page 73).

Connection type

Firewalls – Check Point R80 Security Management – RESTful Collection tasks use a REST API to connect to Check Point Security Management platforms. (VSX routing rules are collected using CPMI; Check Point REST responses do not include routing rules for VSX firewalls and their components.)

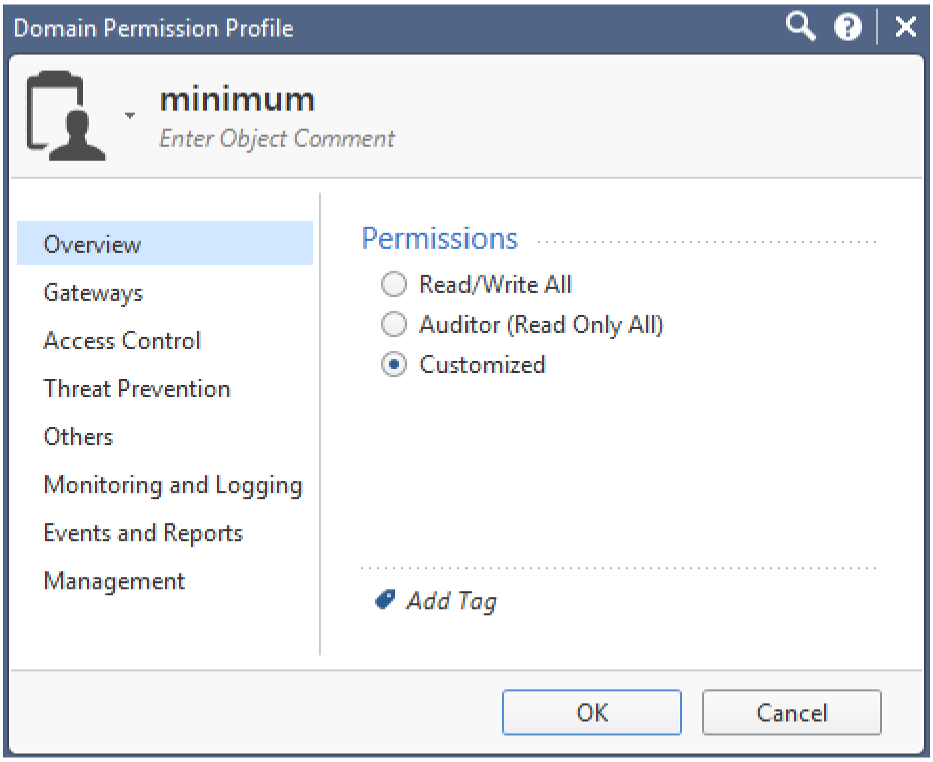
Creating a Permissions Profile

To create a Domain Permission Profile

1 Create a Domain Permission Profile and give it a name.

(In the screen captures shown in this procedure, the Domain Permission Profile is named **minimum**.)

2 In the **Overview** tab of the Domain Permission Profile dialog box, set **Permissions** to **Customized**.



minimum

Enter Object Comment

Permissions

○ Read/Write All

○ Auditor (Read Only All)

● Customized

3 In the **Gateways** tab:

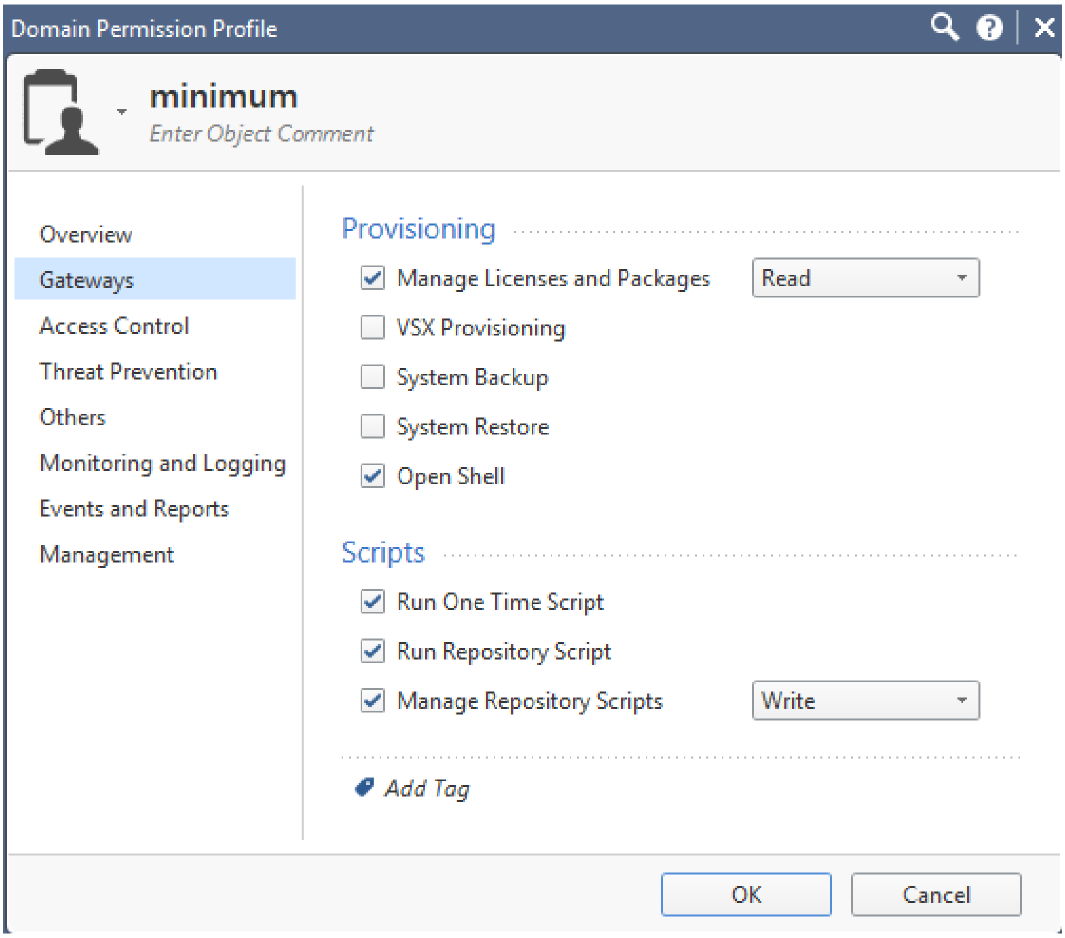
a. In the Provisioning area:

- Select **Manage Licenses and Packages** and set it to **Read**.
- Select **Open Shell**.

b. In the Scripts area:

- Select **Run One Time Script**, **Run Repository Script**, and **Manage Repository Scripts**.

- Set **Manage Repository Scripts** to **Write**.



Domain Permission Profile

minimum

Enter Object Comment

Provisioning

☑ Manage Licenses and Packages: Read

☐ VSX Provisioning

☐ System Backup

☐ System Restore

☑ Open Shell

Scripts

☑ Run One Time Script

☑ Run Repository Script

☑ Manage Repository Scripts: Write

4 Click **OK** to save the new Domain Permission Profile.

To create a Multi-Domain Permission Profile

1 Create a Multi-Domain Permission Profile:

a. Give it a name.

(In the screen capture shown in this procedure, the Domain Permission Profile is named **read only**.)

b. Give it **Manager** permission level.

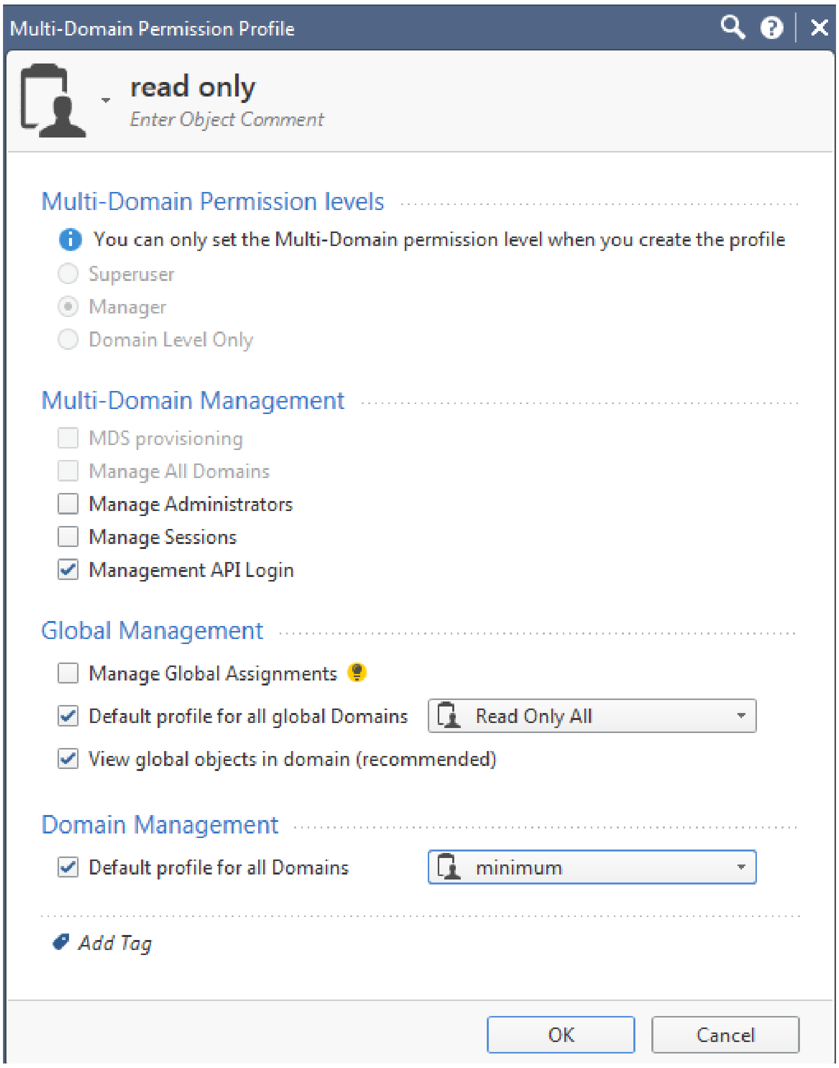
2 Define the profile:

a. In the Multi-Domain Management area, select **Management API Login**.

b. In the Global Management area:

- Select **Default profile for all global Domains** and set it to **Read Only All**.
- Select **View global objects in domain**.

c. In the Domain Management area, select **Default profile for all Domains** and set it to the Domain Permission Profile that you created in the preceding procedure (**minimum** in our example).



Multi-Domain Permission levels

You can only set the Multi-Domain permission level when you create the profile

○ Superuser
● Manager
○ Domain Level Only

Multi-Domain Management

□ MDS provisioning
□ Manage All Domains
□ Manage Administrators
□ Manage Sessions
☑ Management API Login

Global Management

□ Manage Global Assignments
☑ Default profile for all global Domains: Read Only All
☑ View global objects in domain (recommended)

Domain Management

☑ Default profile for all Domains: minimum

3 Click **OK** to save the new Multi-Domain Permission Profile.

Creating a FireWall-1 administrator (R80 Security Management)

To create an administrator

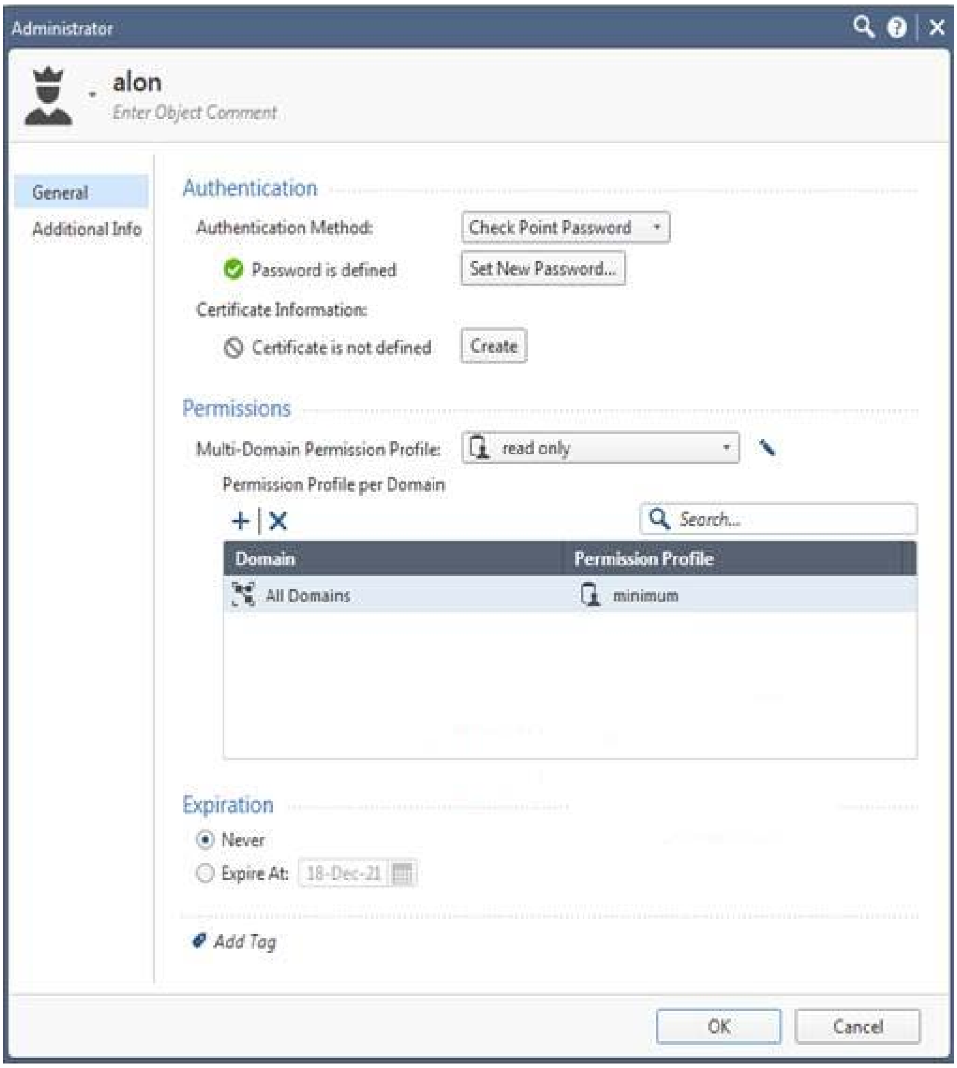
1 Create an Administrator and give it a name.

(In the screen capture shown in this procedure, the Domain Permission Profile is named **alon**.)

2 In the Permissions area:

a. Assign a **Multi-Domain Permission Profile** (in our example, **read only**).

b. In the **Permission Profile per Domain** table, assign a (Domain) **Permission Profile** to **All Domains** (in our example, **minimum**).



Administrator

alon

Enter Object Comment

Authentication

Authentication Method: Check Point Password

✓ Password is defined

Certificate Information:

Certificate is not defined

Permissions

Multi-Domain Permission Profile: read only

Permission Profile per Domain

Domain	Permission Profile
All Domains	minimum

Expiration

● Never

○ Expire At: 18-Dec-21

3 Click **OK** to save the new administrator.

Activating the Security Management API

To activate the Security Management API

1 Open the Check Point SmartDashboard and log in to Security Management.

2 Navigate to **Manage & Settings** > **Blades**.

3 (Directly beneath **Management API**) Click **Advanced Settings**.

4 In the Management API Setup dialog box:

- Select **Automatic start**.
- Select **All IP addresses**.

5 Click **OK** to close the Management API Setup dialog box.

6 Click **Publish** (at the top of the SmartDashboard window).

7 Log out of SmartDashboard.

8 Use an SSH client to connect to Security Management.

9 At the command prompt, run:

   a. `api reconf`

   b. `api status`

10 Verify:

   a. `Overall API Status` is `Started`

   b. `Test` is `SUCCESSFUL`

   The server is up and ready to receive connections.

   c. Under `API Settings`:

   `Accessibility` is set to `Allow from all`

11 Exit the SSH client.

To confirm that the Security Management API is running

1 Open `https://<Security Management IP address>/api_docs/`.

2 Accept the self-signed SSL certificate warning.

The 1st page of the *Management API Reference* is displayed; the Security Management API server is up and running.

Check Point R80 Security Management collection tasks

Firewalls – Check Point R80 Security Management – RESTful Collection tasks retrieve configuration data from a Check Point FireWall-1 Management Server (R80 and higher) and add this data to the current model.

Note: Create a separate R80 Security Management collection task for each FireWall-1 Management Server.

› To retrieve configuration data from Check Point FireWall-1 Management Servers (R77 and lower), see Check Point FireWall-1 CPMI collection tasks (FireWall-1) (on page 74).

Note: Single clusters are supported for all versions of Check Point R80; multiple clusters require Check Point R80.10 and higher.

For VSX (virtual systems) firewalls, configuration data for all the virtual firewalls is retrieved.

Note: Check Point REST responses do not include anti-spoofing configuration data for clusters, or for VSX firewalls and their components.

Task properties

The properties that control **Firewalls – Check Point R80 Security Management – RESTful Collection** tasks when collecting data from FireWall-1 Management Servers are described in the following table.

Property	Description
Basic tab	
Management server	The IP address of the FireWall-1 Management Server or Multi-Domain Server (MDS). **Note**: Provide the IP address, not the asset name.
Firewall Filter	Specifies whether to collect configuration data of all (managed) firewalls, firewalls with a change event since the most recent collection (including new firewalls), or new firewalls only.
Authentication	If a Permissions Profile exists, the task uses the profile; any values entered in this section are ignored.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name of the administrator created for the task (see Creating a FireWall-1 administrator (R80 Security Management) (on page 94)).
Password	This field is displayed if **Method** = **Device**. The administrator password.
Domain	(If **Management server** is an MDS) A comma-separated list of MDS domains. Use the characters **?** and ***** for standard pattern matching.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Location Hint	The location of the FireWall-1 Management Server. **Note**: Use this property if different locations use the same set of IP addresses, so that Management Servers at different locations can have the same IP address.
Collect VSX routing rules(CPMI)	(Only required if **Management server** is an MDS and you are collecting a subset of the CMAs.)
Certificate Issue Date	• If this field is empty, the connection to the Management Server is not initialized • <Timestamp>: The timestamp of the authentication certificate To retrieve an authentication certificate, click **Initialize Certificate** to open the Initialize Certificate dialog box (see page 77).

Property	Description
SIC Name	The DN of the Management Server. Skybox displays the value from the authentication certificate that it retrieves when you initialize the connection. Do not change this value.
OPSEC Application	The name given to the OPSEC application when it was configured for Skybox (see Configuring OPSEC applications for FireWall-1 (on page 71)). Skybox displays the name that you provided when you initialized the connection.

CISCO FIREPOWER MANAGEMENT CENTER

Cisco Firepower Management Centers (FMCs) manage multiple Cisco Firepower Threat Defense firewalls.

You can add or update configuration data of Firepower Threat Defense firewalls (version 6.2.3-build 83 and higher) managed by an FMC to the current model using an online collection task:

- Configure the FMC (see page 98) to permit access from a Skybox Collector and create a collection task (see page 98) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data of multiple Firepower Threat Defense firewalls managed by 1 FMC.

Configuring Cisco Firepower Management Center for data collection

Note: Firepower collection is supported for version 6.2.3-build 83 and higher.

To configure an FMC for data collection:

- Skybox data collection requires a user with **Security Approver** permissions on the device; we recommend that you create a separate user for this purpose.
- For multi-domain environments the user must be configured for the global domain.

Connection type

Firewalls – Cisco Firepower Management Center Collection tasks use a REST API to connect to FMCs.

Cisco Firepower Management Center collection tasks

Firewalls – Cisco Firepower Management Center Collection tasks retrieve configuration data of Cisco Firepower Threat Defense firewalls managed by a Cisco Firepower Management Center (FMC) and add this data to the current model.

Task properties

The properties that control **Firewalls – Cisco Firepower Management Center Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	The name or IP address of the FMC. If you are using IPv6, enclose the address in brackets: **https://[xxxx::x]**
Firewall Filter	Specifies whether to collect configuration data of all (managed) firewalls, firewalls with a change event since the most recent collection (including new firewalls), or new firewalls only.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the FMC.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Location Hint	The location of the FMC. **Note**: Use this property if different locations use the same set of IP addresses, so that FMCs at different locations can have the same IP address.

CISCO PIX/ASA/FWSM FIREWALL

You can add or update configuration data from Cisco PIX/ASA/FWSM firewalls to the current model:

- Using an online collection task:
  - Configure the firewalls (see page 100) to permit access from a Skybox Collector and create a collection task (see page 102) to collect the firewall configurations and add the configuration data to the model.

    The collection task can collect data from multiple firewalls.
- Using an offline file import task:
  - Retrieve firewall configuration files and to import their data into the model (see page 104).

    The file import task can import the data of multiple firewalls.

Configuring Cisco PIX/ASA/FWSM firewalls for data collection

To configure a Cisco PIX/ASA/FWSM firewall so that Skybox can retrieve its configuration data:

- In the firewall, create an admin user with level 5 privileges.

> Note: If the user name that you use to log in to the firewall has sufficient permissions, you do not need to create an admin user.
> The method described here creates an admin user that does not have login permissions; you need another user name to log in to the firewall.

- Enable access to the firewall from the Skybox Collector:
  - If access rules are configured on the firewall, configure a rule to permit either SSH or Telnet access from the Skybox Collector IP address to the firewall.
- (ASA only) Add the supported SSH protocol and algorithm.

To create a user if you are using Cisco's authentication mechanism (basic or AAA)

1 Add a user with level 5 privileges:

```
# username skybox password skybox privilege 5
```

2 Configure a password for this user.

You need the user name and password when you create the firewall collection task.

3 Execute the following commands to grant this user permissions to the PIX/ASA/FWSM `show conf` and `show route` commands:

```
# conf term
# aaa authentication ssh console LOCAL
# aaa authorization command LOCAL
# privilege show level 5 command route
# privilege show level 5 command running-config
# privilege configure level 5 command ["terminal page" | "no pager"]
# write mem
```

4 (ASA only) Add the supported SSH protocol and algorithm:

```
# ssh key-exchange group dh-group1-sha1
```

To create a user if you are using TACACS or RADIUS

1 Configure a level 5 user on the TACACS or RADIUS.

2 Configure a password for this user.

You need the user name and password when you create the firewall collection task.

3 Execute the following commands to grant this user permissions to the PIX/ASA/FWSM `show conf` and `show route` commands:

```
# conf term
# privilege show level 5 command route
# privilege show level 5 command running-config
# privilege configure level 5 command ["terminal page" | "no pager"]
# write mem
```

4 (ASA only) Add the supported SSH protocol and algorithm:

```
# ssh key-exchange group dh-group1-sha1
```

Commands sent to Cisco PIX/ASA/FWSM firewalls

Connection type

Firewalls – Cisco PIX/ASA/FWSM Collection tasks use the SSH protocol to connect to PIX/ASA/FWSM firewalls.

Commands sent to device

Firewalls – Cisco PIX/ASA/FWSM Collection tasks send the following commands to PIX/ASA/FWSM firewalls:

- One of:
  - `enable`
  - `login`

  depending on the value of **Enabling Command** in the **Advanced** tab of the task
- `sh mode`
- `terminal pager 0`
- `no pager`
- One of:
  - `wr terminal`
  - `show conf` *and* `show ver`
  - `show run`
  - `show run all`
  - `more system:running-config`
  - `show startup-config` (this command is also sent if you select **Collect Startup Configuration** in the **Advanced** tab of the task)

  depending on the value of **Get Configuration Command** in the **Advanced** tab of the task
- `show route`
- `show access-list`

  This command is sent only if you select **Collect hit counts** in the **Basic** tab of the task.

If the output of sh mode is **Security context mode: multiple**, the task also sends the following commands to the firewall:

- `changeto system`
- `sh hostname`
- `show context`
- `changeto context <context>`

Cisco PIX / ASA / FWSM collection tasks

Firewalls – Cisco PIX / ASA / FWSM Collection tasks retrieve configuration data from Cisco PIX/ASA/FWSM firewalls and add this data to the current model.

Note: If a firewall is configured in L2 (transparent) mode, you must define segments and assign them to the interfaces after ingesting the firewall configuration data.

Task properties

The properties that control **Firewalls – Cisco PIX / ASA / FWSM Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	The connection protocol to use.
SSH Port	If **Connection Protocol** = **ssh**, the port on which the firewalls listen. If you change the default port (22) on the firewalls, the Skybox Collector must have permission to connect to the firewalls on the port that you specify.
Addresses	A comma-separated list of the IP addresses and IP address ranges of the PIX/ASA/FWSM firewalls. To collect configurations of all contexts from a firewall with *multiple contexts* (that is, virtual firewalls), type the IP address of the admin context. (To collect the configuration of 1 context, type the IP address of the context.) **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Firewall Filter	Specifies whether to collect all firewalls or only firewalls with a change event since the most recent collection.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewalls.
Password	This field is displayed if **Method** = **Device**.

Property	Description
	The user password.
Admin Username	This field is displayed if **Method** = **Device**. The user name of an administrator on the firewalls. After logging in with **Username**, Skybox runs `set user` on the firewalls using **Admin Username**. **Note**: If **Username** has sufficient permissions, you can leave this field empty; otherwise, it is mandatory.
Admin Password	This field is displayed if **Method** = **Device**. The administrator password. **Note**: Only required if you provide **Admin Username** (see previous note).
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Admin Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the administrator authentication credential object. **Note**: If the user specified in **Object** has sufficient permissions, you can leave this field empty; otherwise, it is mandatory.
Admin Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the administrator name and password. **Note**: Only required if you provide **Admin Safe** (see previous note).
Enable Setting	
Enabling Command	The command to use for user authentication if you provide: • (**Method** = **Device**) **Admin Username** and **Admin Password** • (**Method** = **CyberArk**) **Admin Object**
Enable Privilege	This field is enabled only if **Enabling Command** = **enable**. The privilege to append when sending the `enable` command. (If this field is empty, the `enable` command is sent with no value appended.)
Collection Setting	
Collect hit counts	Specifies whether to retrieve the hit counts of the access rules. If selected, rule usage analysis is available immediately; you do not need to run a **Change Tracking Events – Syslog Import** task.

Property	Description
Advanced tab	
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.
Get Configuration Command	The command to send to the firewalls to retrieve the configuration. **Note**: If you select **Collect Startup Configuration**, do not select **sh conf**.
Collect Startup Configuration	This field is disabled if **Get Configuration Command** = **show startup-config**. Specifies whether to collect the startup configuration. If selected, you can compare the startup configuration and the running configuration. For information about making this comparison, see the Cisco configuration diffs topic in the Skybox Firewall Assurance User Guide.
Use config routes only	Specifies whether to skip the parsing of the dynamic routing file. Select this option if the dynamic routing file uses names rather than IP addresses.

Importing Cisco PIX/ASA/FWSM configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Cisco PIX/ASA/FWSM firewall configuration:

- `run.txt`: The PIX/ASA/FWSM configuration file

  This file is the output of the PIX/ASA/FWSM show `run` command.

  - (Optional) Hit counts are imported if you append the output of the show `access-list` command to `run.txt`.

- (Optional) `route.txt`: Dump of the PIX/ASA/FWSM routing table

  This file is the output of the PIX/ASA/FWSM show `route` command.

  Note: If you cannot extract routing rules in device native format, you can manually append the rules to the end of the device configuration file. See Appending routing information to device configuration (on page 43).

If `route.txt` is included, its routing rules overwrite routing rules from `run.txt` because its information is more extensive and includes static and dynamic routing rules.

You can import the configurations of multiple firewalls; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

CISCO SECURITY MANAGER

Cisco Security Managers (CSMs) manage multiple Cisco firewalls.

You can add or update configuration data of the Cisco firewalls managed by a CSM to the current model:

- Using an online collection task:
  - Configure the CSM (see page 105) to permit access from a Skybox Collector and create a collection task (see page 105) to collect the firewall configurations and add the configuration data to the model.

    The collection task can collect data of multiple Cisco firewalls managed by 1 CSM.
- Using an offline file import task:
  - Generate and retrieve a CSM source file and import its data into the model (see page 107).

    The file import task can import the data of multiple CSMs.

To add or update configuration data from Cisco firewalls see Cisco PIX/ASA/FWSM firewall (on page 99).

Configuring Cisco Security Manager for data collection

To configure a CSM for data collection:

- Configure the CSM to permit collection. (The Skybox Collector must have permission to connect to the CSM device using HTTPS on port 8443.)
- Skybox data collection requires a user with a **Network Operator** role on the device; we recommend that you create a separate user for this purpose.

Licensing data collection

To collect data from a CSM, you must install 2 API licenses on the CSM device:

- A developer license: The developer license is a 90-day license for developers who are integrating their products with CSM
- A production license: The production license is required by end users who use 3rd-party products.

For information about CSM licensing, see http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.3/installation/guide/licensing.html

Connection type

Firewalls – Cisco Security Manager Collection tasks use a web service to connect to CSMs.

Cisco Security Manager collection tasks

Firewalls – Cisco Security Manager Collection tasks retrieve configuration data of Cisco firewalls managed by a Cisco Security Manager (CSM) and add this data to the current model.

Task properties

The properties that control **Firewalls – Cisco Security Manager Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	The name or IP address of the CSM.
Firewall Filter	Specifies whether to collect configuration data of all (managed) firewalls, firewalls with a change event since the most recent collection (including new firewalls), or new firewalls only.
Authentication	
Method	- **Device**: Use the authentication credentials provided here. - **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the CSM.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Collection	
Limit by device names	A comma-separated list of the names of Cisco devices (managed by the CSM) for which to collect configuration data. You can use ***** as a wildcard in the device names.
Limit by groups	A comma-separated list of device groups (on the CSM) for which to collect configuration data.
Exclude groups	A comma-separated list of device groups and subgroups to exclude from the devices included in **Limit by groups**.
Collect only firewalls	Specifies whether to collect configuration data for firewalls only or for all devices as specified in the preceding 3 fields.
Advanced tab	
Location Hint	The location of the CSM. **Note**: Use this property if different locations use the same set of IP addresses, so that CSMs at different locations can have the same IP address.

Importing CSM-managed Cisco firewalls configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data.

The following file is required to import the configuration of Cisco firewalls managed by a Cisco Security Manager (CSM):

- `*.xml`: The CSM source file

  This file is retrieved using a web service.

You can import the source file of multiple CSMs.

DELL SONICWALL FIREWALL

You can add or update configuration data from Dell SonicWALL firewalls to the current model using an online collection task:

- Configure the firewalls (see page 107) to permit access from a Skybox Collector and create a collection task (see page 107) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple firewalls.

Configuring SonicWALL firewalls for data collection

To configure a SonicWALL firewall for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Note: SonicWALL version 5.9 does not support the collection method. If you need a workaround, contact Skybox Support.

Connection type

Firewalls – SonicWALL Collection tasks use a web service to connect to SonicWALL firewalls.

Dell SonicWALL collection tasks

Firewalls – SonicWALL Collection tasks retrieve configuration data from SonicWALL firewalls and add this data to the current model.

Note: SonicWALL version 5.9 does not support the collection method. If you need a workaround, contact Skybox Support.

Task properties

The properties that control **Firewalls – SonicWALL Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of IP addresses of SonicWALL firewalls, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 443.

Property	Description
	Note: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewalls.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
SSL	Specifies whether to connect to the firewalls over HTTPS (SSL) rather than HTTP.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

DIONIS FIREWALL

You can add or update configuration data from DioNIS firewalls to the current model using an online collection task:

- Configure the firewalls (see page 108) to permit access from a Skybox Collector and create a collection task (see page 109) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple firewalls.

Configuring DioNIS firewalls for data collection

To configure a DioNIS firewall for data collection:

- Install the DioNIS agent software in `<Skybox_Home>\intermediate\bin\collectors\firewalls\DioNIS\DiAgent`
- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Firewalls – DioNIS Collection tasks use a proprietary DioNIS API to connect to DioNIS firewalls.

DioNIS collection tasks

Firewalls – DioNIS Collection tasks retrieve configuration data from DioNIS firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – DioNIS Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the DioNIS firewalls. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Username	The user name to access the firewalls.
Password	The user password.
Enable Password	The password for enable command privileges on the firewalls.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

DPTECH FIREWALL

You can add or update configuration data from DPtech firewalls to the current model using an online collection task:

- Configure the firewalls (see page 109) to permit access from a Skybox Collector and create a collection task (see page 110) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple firewalls.

Configuring DPtech firewalls for data collection

To configure a DPtech firewall for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Firewalls – DPtech Collection tasks use the SSH protocol to connect to DPtech firewalls.

Commands sent to device

Firewalls – DPtech Collection tasks send the following commands to DPtech firewalls:

- `no page`
- `show run`
- `show ip route`

DPtech collection tasks

Firewalls – DPtech Collection tasks retrieve configuration data from DPtech firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – DPtech Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the DPtech firewalls. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewalls.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log.

Property	Description
	If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

FORCEPOINT NGFW APPLIANCE

You can add or update firewall configuration data from Forcepoint NGFW appliances to the current model using an online collection task:

- Configure the appliance (see page 111) to permit access from a Skybox Collector and create a collection task (see page 111) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple firewalls from a single appliance.

Configuring Forcepoint NGFW appliances for data collection

To configure a Forcepoint appliance for data collection:

- Install the Python smc-python package.
- Skybox data collection requires a Superuser on the device; we recommend that you create a separate Superuser for this purpose.

To download and install the Python smc-python package on Skybox

- Download and install the smc-python package from https://pypi.python.org/pypi/smc-python/

Connection type

Firewalls – Forcepoint NGFW Collection tasks use a REST API to connect to Forcepoint appliances.

Forcepoint collection tasks

Firewalls – Forcepoint NGFW Collection tasks retrieve firewall configuration data from a Forcepoint NGFW appliance and add this data to the current model.

Task properties

The properties that control **Firewalls – Forcepoint NGFW Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Management IP	The IP address of the appliance, with the format

Property	Description
	`nnn.nnn.nnn.nnn[:<port>]`. The default port is 8082.
API-key	The *API-key* of the Superuser accessing the appliance.
Firewalls	A comma-separated list of the names of the firewalls whose configuration data is to be collected.
Advanced tab	
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system `Temp` directory.
Separate config per host	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the appliance. **Note**: Use this property if different locations use the same set of IP addresses, so that appliances at different locations can have the same IP address.

FORTINET FORTIGATE FIREWALL

You can add or update configuration data from Fortinet FortiGate firewalls to the current model:

- Using an online collection task:
  - Configure the firewalls (see page 112) to permit access from a Skybox Collector and create a collection task (see page 114) to collect the firewall configurations and add the configuration data to the model.

    The collection task can collect data from multiple firewalls.
- Using an offline file import task:
  - Generate and retrieve firewall configuration files and import their data into the model (see page 116).

    The file import task can import the data of multiple firewalls.

Configuring FortiGate firewalls for data collection

To configure a FortiGate firewall for data collection:

- Skybox data collection requires an admin user on the device; we recommend that you create a separate user for this purpose.

  To collect all VDOMs, assign this user global permissions.
- Configure the firewall to permit collection. (The Skybox Collector must have permission to connect to the firewall using either SSH or Telnet.)

To assign global permissions to a user

1 Log in to the firewall via SSH.

2 Create an access profile by running the following commands:

```
config global
config system accprofile
edit <Skybox profile>
```

<Skybox profile> is the name of the profile that you are creating for the admin user

3 Grant the profile read-only permissions by running the following commands:

```
set scope global
set mntgrp read
set admingrp read
set updategrp read
set authgrp read
set sysgrp read
set netgrp read
set loggrp read
set routegrp read
set fwgrp read
set vpngrp read
set utmgrp read
set wanoptgrp read
set endpoint-control-grp read
set wifi read
```

4 Assign the user to the profile by running the following commands:

```
config system admin
edit <admin name>
set accprofile <Skybox profile>
```

Change tracking events

To import firewall change event log data (syslog data) from a FortiGate firewall (for a **Change Tracking Events – Syslog Import** task):

1 Set the FortiGate **Log Level** to **informational** (or higher).

2 Configure the firewall to send syslog messages to a Skybox Appliance or Collector; send the following commands to the server:

```
config log syslogd setting
set facility local7
set port 514
set server <IP address>
set status enable
end
```

For additional information about configuring the firewall, see *Logging to a Syslog server* at https://help.fortinet.com/fos40hlp/43/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=logging_storing%20logs.34.9.html

For information about **Change Tracking Events – Syslog Import** tasks, see Syslog change events (on page 170).

Connection type

Firewalls – FortiGate Collection tasks use the SSH protocol to connect to FortiGate firewalls.

Commands sent to device

Firewalls – FortiGate Collection tasks send the following commands to FortiGate firewalls:

- a

  This ‘command’ is sent to retrieve the command prompt.

- `get system status`
- `get system interface`
- `config global`

  If the device version does not support VDOMs or if VDOMS are disabled, `config system global` is sent instead of `config global`.

- `config system console`
- `set output standard`
- One of:
  - `show`
  - `show full-configuration`

  depending on the value of **Get Configuration Command** in the **Advanced** tab of the task

- `config vdom`
- `edit <VDOM>`
- `show system interface`
- `get system ha status`
- `get router info routing-table`
- `get router info routing-table all`

Fortinet FortiGate collection tasks

Firewalls – FortiGate Collection tasks retrieve configuration data from FortiGate firewalls and add this data to the current model.

Note: If the firewall is working in VDOM Method, the task does not check for “missing explicit Deny rule” (see the Rule Check types topic in the Skybox Firewall Assurance User Guide).

Task properties

The properties that control **Firewalls – FortiGate Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	The connection protocol to use.
SSH Port	If **Connection Protocol** = **ssh**, the port on which the firewalls listen. If you change the default port (22) on the firewalls, the Skybox Collector must have permission to connect to the firewalls on the port that you specify.
FortiGate Addresses	A comma-separated list of the IP addresses and IP address ranges of the FortiGate firewalls. To collect configurations of Virtual Domains, type an IP address for each physical firewall only. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Firewall Filter	Specifies whether to collect all firewalls or only firewalls with at least 1 change event since the most recent collection.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewalls.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.
Do Not Collect Routing Table	If selected, specifies that the routing table is not collected. Select this option if the firewall is working in VDOM (Virtual Domains) Method.

Property	Description
Do Not Collect IPS Rule Groups	If selected, specifies that the IPS rule groups are not collected. If cleared, the IPS rule properties show the associated Vulnerability Definitions with severity and CVE information.
Get Configuration Command	The command to send to the firewalls to retrieve the configuration.
Import BGP Routes	Specifies whether to import BGP routing rules. • **System default**: Use the value of `fortigate_ignore_BGP_routing_rules` in `<Skybox_Home>\server\conf\sb_common.properties` (this property has a default value of `true`)

Importing FortiGate configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a FortiGate firewall configuration:

- `config.txt`: The FortiGate configuration file

  To create this file, run the following FortiGate commands:

  1. `get system status` (the output of this command includes the FortiGate version)

     Save the output of this command to a new text file, `config.txt`.

  2. `config system console`
  3. `set output standard`
  4. `show` (the output of this command is the FortiGate configuration)

     Append the output of this command to the file created in step **1** and save the file.

- (Optional) `route.txt`: Dump of the FortiGate routing table

  This file is the output of the FortiGate `get router info routing-table` command.

  Note: If you cannot extract routing rules in device native format, you can manually append the rules to the end of the device configuration file. See Appending routing information to device configuration (on page 43).

You can import the configurations of multiple firewalls; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

FORTINET FORTIMANAGER SECURITY MANAGEMENT APPLIANCE

Fortinet FortiManager Security Management appliances manage multiple Fortinet FortiGate firewalls.

You can add or update configuration data of the FortiGate firewalls managed by a FortiManager Security Management appliance to the current model using an online collection task:

- Configure the FortiManager Security Management appliance (see page 117) to permit access from a Skybox Collector and create a collection task (see page 118) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data of multiple FortiGate firewalls managed by a single FortiManager Security Management appliance.

To add or update configuration data from Fortinet FortiGate firewalls see Fortinet FortiGate firewall (on page 112).

Configuring FortiManager Security Management appliances for data collection

To configure a FortiManager Security Management appliance for data collection:

- For collection using the FortiManager XML API:
  - Create a separate super user administrator account on the appliance for Skybox tasks
  - Enable the API
- For collection using the FortiManager JSON API:
  - Create a separate read-only user on the appliance for Skybox tasks

    Note: For Skybox Change Manager to implement change requests automatically, create a *read-write* profile instead. (See the Configuring automatic implementation section in the Skybox Change Manager User Guide).

  - Confirm that the user that you created has the correct permissions.
  - Enable the API

  Note: If you use the JSON API, the task cannot collect users or the Central NAT, due to limitations of the FortiManager API.

- Configure the FortiManager Security Management appliance to permit collection. (The Skybox Collector must have permission to connect to the Security Management appliance using HTTPS on port 8080.)

To create an account

1. In the FortiManager Web-based Manager, select **System Settings** > **Admin** > **Administrator**.
2. Select **Create New**.
3. In the New Administrator dialog box:
   - (For the XML API) In the **Admin Profile** field, select **Super_User**.
   - (For the JSON API) In the **Admin Profile** field, select **Read Only User**.

     For automatic implementation of change requests, select **Super_User**.
4. Click **OK** to create the new account.

To confirm that the new user has permissions (JSON API)

1 Connect to FortiManager via SSH.

2 Run the following commands:

```
config system admin user
edit <name>
show
```

3 Search the response for the line `set rpc-permit read` (or `set rpc-permit read-write`).

4 If the line is not present:

a. Run the following commands:

```
set rpc-permit read (or set rpc-permit read-write)
end
```

b. Repeat steps **2** and **3** to confirm that the permission was applied.

To enable the FortiManager API

1 In the FortiManager Web-based Manager, select **System Settings** > **Network**.

2 Select **Web Service**.

Connection type

Firewalls – FortiManager Collection tasks use (depending on the value of **Collection Method** in the **Basic** tab of the task) either a combination of a SOAP API and the SSH protocol, or a REST API to connect to FortiManager Security Management appliances.

Commands sent to device

Firewalls – FortiManager Collection tasks send the following SSH commands to FortiManager Security Management appliances:

- `get system status`
- `get system interface`
- `diagnose dvm device list`

Fortinet FortiManager Security Management appliance collection tasks

Firewalls – FortiManager Collection tasks retrieve configuration data of FortiGate firewalls managed by a Fortinet FortiManager Security Management appliance and add this data to the current model.

Task properties

The properties that control **Firewalls – FortiManager Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	The name or IP address of the FortiManager Security Management appliance.

Property	Description
Firewall Filter	Specifies whether to collect configuration data of all (managed) firewalls, firewalls with at least 1 change event since the most recent collection (including new firewalls), or new firewalls only.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The super user name to access the FortiManager Security Management appliance.
Password	This field is displayed if **Method** = **Device**. The super user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Collection	
Device ADOMS	A comma-separated list of administrative domains in which the firewalls, whose data is collected, exist.
Import Specific Devices	Specifies whether to collect data for specific firewalls in the specified administrative domains of the FortiManager Security Management appliance. If cleared, data for all firewalls in the specified domains is collected.
Device Names	This field is enabled only if you select **Import Specific Devices**. A comma-separated list of the names of firewalls for which to collect configuration data. You can use ***** as a wildcard in the device names.
Collection Method	Specifies the method that the task uses to connect to the appliance. **Note**: If you select **JSON API**, the task *cannot* collect users or the Central NAT. **Note**: For FortiGate firewalls running versions lower than 5.4, not all information is available if you select **XML API**.
Advanced tab	
HTTPS Port	The port on which the FortiManager Security Management appliance listens. If you change the default port (8080) on the Security Management appliance, the Skybox Collector must have permission to connect to the Security Management appliance using HTTPS on the port that you specify.

Property	Description
Location Hint	The location of the FortiManager Security Management appliance. **Note**: Use this property if different locations use the same set of IP addresses, so that Security Management appliances at different locations can have the same IP address.
Do Not Collect Routing Table	If selected, specifies that the routing table of each firewall is not collected. Select this option if the firewalls are working in VDOM (Virtual Domains) Method.
Do Not Collect IPS Rule Groups	If selected, specifies that the IPS rule groups of each firewall are not collected. If cleared, the IPS rule properties show the associated Vulnerability Definitions with severity and CVE information.
Import BGP Routes	Specifies whether to import BGP routing rules. • **System default**: Use the value of `fortigate_ignore_BGP_routing_rules` in `<Skybox_Home>\server\conf\sb_common.properties` (this property has a default value of `true`)

GENBAND FIREWALL

You can add or update configuration data from Genband firewalls to the current model:

- Using an online collection task:
  - Configure the firewalls (see page 120) to permit access from a Skybox Collector and create a collection task (see page 121) to collect the firewall configurations and add the configuration data to the model.

    The collection task can collect data from multiple firewalls.
- Using an offline file import task:
  - Generate and retrieve firewall configuration files and import their data into the model (see page 122).

    The file import task can import the data of multiple firewalls.

Configuring Genband firewalls for data collection

To configure a Genband firewall for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Firewalls – Genband Collection tasks use either the SSH protocol or the SCP protocol (depending on the value of **SCP Config Dir** in the **Advanced** tab of the task) to connect to Genband firewalls.

Commands sent to device

Firewalls – Genband Collection tasks send the following SSH commands to Genband firewalls:

- `cli cr list | cat\r`
- `nxconfig.pl -S\r`
- `cli realm list | cat\r`
- `cli db export filename.xml\r`
- `nxconfig.pl -M\r`
- `cli cp list bindings | cat\r`
- `cli vnet list | cat\r`
- `cli iedge list | cat\r`
- `cat filename.xml\r`
- `cat new-mdevices.xml\r`

Genband collection tasks

Firewalls – Genband Collection tasks retrieve configuration data from Genband firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – Genband Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Genband firewalls. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewalls.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system Temp directory.
Connection Mode	The protocol to use to connect to the firewalls.

Property	Description
SCP Config Dir	(Only relevant if **Connection Mode** = **SCP**) The full path to the directory that is to hold the downloaded configuration files.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

Importing Genband configuration data

You can use an **Import – Directory** task to import Genband configuration data.

Note: If you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

You can import the configurations of multiple firewalls; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

HUAWEI EUDEMON FIREWALL

You can add or update configuration data from Huawei Eudemon firewalls to the current model using an online collection task:

- Configure the firewalls (see page 122) to permit access from a Skybox Collector and create a collection task (see page 123) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple firewalls.

Configuring Eudemon firewalls for data collection

To configure a Huawei Eudemon firewall for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Firewalls – Huawei Eudemon Collection tasks use SSH to connect to Eudemon firewalls.

Commands sent to device

Firewalls – Huawei Eudemon Collection tasks send the following commands to Eudemon firewalls:

- `screen-length 0 temporary`
- `dis current-configuration`
- `dis version`
- `dis ip routing-table`

Huawei Eudemon collection tasks

Firewalls – Huawei Eudemon Collection tasks retrieve configuration data from Eudemon firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – Huawei Eudemon Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Eudemon firewalls. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
SSH Port	The port on which the routers listen. If you change the default port (22) on the routers, the Skybox Collector must have permission to connect to the routers on the port that you specify.
Username	The user name to access the firewalls.
Password	The user password.
Advanced tab	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

JUNIPER NETWORKS JUNOS FIREWALL

You can add or update configuration data from Juniper Networks Junos firewalls to the current model:

- Using an online collection task:
  - Configure the firewalls (see page 124) to permit access from a Skybox Collector and create a collection task (see page 125) to collect the firewall configurations and add the configuration data to the model.

    The collection task can collect data from multiple firewalls.
- Using an offline file import task:

- Generate and retrieve firewall configuration files and import their data into the model (see page 126).

  The file import task can import the data of multiple firewalls.

Note: These tasks can also add or update configuration data from Juniper Networks MX routers.

Configuring Junos firewalls for data collection

To configure a Junos firewall for data collection:

- Create a separate user on the device with set permission for Skybox data collection.
- Configure the firewall to permit collection. (The Skybox Collector must have permission to connect to the firewall using either SSH or Telnet.)

To import firewall activity log data (syslog data) from a Junos firewall:

- Configure the firewall to output log messages in structured-data format. (This requires Junos version 8.3 or higher.)

  For information about configuring the firewall, see http://www.juniper.net/techpubs/en_US/junos10.0/information-products/topic-collections/syslog-messages/directing_log_file.html#Logging_msgs_structured_data_format

To import firewall change event log data (syslog data) from a Junos firewall (for a **Change Tracking Events – Syslog Import** task):

- Configure the firewall to send syslog messages to a Skybox Appliance or Collector.

  For information about configuring the firewall, see https://kb.juniper.net/InfoCenter/index?page=content&id=KB10132

  For information about **Change Tracking Events – Syslog Import** tasks, see Syslog change events (on page 170).

Connection type

Firewalls – Junos Collection tasks use the SSH protocol to connect to Junos firewalls.

Commands sent to device

Firewalls – Junos Collection tasks send the following commands to Junos firewalls:

- `set cli screen-width 1000`
- `show chassis hardware | no-more`
- `show configuration | display inheritance | no-more`
- Any 1, or the first 2, of:
  - `show route logical-system all | no-more`
  - `show route all | no-more`
  - `show route extensive active-path | no more | display xml`

depending on the value of **Get Routing Table Command** in the **Advanced** tab of the task

- `show route logical-system all | no-more`

  If there are no logical systems so that this command returns an error, the following command is also sent:

  `show route all | no-more`

- `show configuration | display set | no-more`

  This command is sent only if you select **Collect Deactivated Policies** in the **Advanced** tab of the task

Juniper Networks Junos collection tasks

Firewalls – Junos Collection tasks retrieve configuration data from Junos firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – Junos Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	The connection protocol to use.
SSH Port	If **Connection Protocol** = **ssh**, the port on which the firewalls listen. If you change the default port (22) on the firewalls, the Skybox Collector must have permission to connect to the firewalls on the port that you specify.
Addresses	A comma-separated list of the IP addresses and IP address ranges of the Junos firewalls. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Firewall Filter	Specifies whether to collect all firewalls or only firewalls with at least 1 change event since the most recent collection.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewalls.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user

Property	Description
	authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.
Do Not Collect Routing Table	If selected, specifies that the routing table is not collected.
Get Routing Table Command	The command to send to the firewalls to create the routing table. • **automatic**: Send `show route logical-system all`; if there are no logical systems so that this command returns an error, send `show route all`.
Import BGP Routes	Specifies whether to import BGP routing rules: • **System default**: Use the value of `junos_ignore_BGP_routing_rules` in `<Skybox_Home>\server\conf\sb_common.properties` (this property has a default value of `true`)
Collect Deactivated Policies	Specifies whether to also collect deactivated policies.

Importing Junos configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Junos firewall configuration:

- `config.txt`: The Junos configuration file

  This file is the output of the Junos command `show configuration | display inheritance | no-more`

  If you are working with a cluster of Junos firewalls, prepend the output of the Junos command `show chassis hardware | no-more`

- (Optional) `route.txt`: Dump of the Junos routing table

  This file is the output of the Junos command `show route logical-system all | no-more` (if there are no logical systems, use `show route all | no-more`)

  Note: If you cannot extract routing rules in device native format, you can manually append the rules to the end of the device configuration file. See Appending routing information to device configuration (on page 43).

You can import the configurations of multiple firewalls; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

If you need only the Junos configuration file, you can retrieve it via HTTP.

To retrieve the configuration file of a Junos firewall

1. In your browser, log in to the Juniper Web Device Manager.
2. Click the **Configure** tab and select **CLI Tools** > **CLI Viewer**.
3. Save the configuration to a text file and name the file `config.txt`.

JUNIPER NETWORKS JUNOS SPACE NETWORK MANAGEMENT PLATFORM

Juniper Networks Junos Space Network Management Platforms manage multiple Juniper Networks Junos firewalls. You can add or update configuration data of the Junos firewalls managed by a Junos Space platform to the current model using an online collection task:

- Configure the Junos Space platform (see page 127) to permit access from a Skybox Collector and create a collection task (see page 127) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data of multiple Junos firewalls managed by a Junos Space platform.

To add or update configuration data from Juniper Networks Junos firewalls see Juniper Networks Junos firewall (on page 123).

Configuring Junos Space Network Management Platform for data collection

To configure a Junos Space Network Management Platform for data collection:

- Create a separate global domain Device Manager account on the platform for Skybox tasks.
- Configure the Junos Space platform to permit collection. (The Skybox Collector must have permission to connect to the Junos Space platform server using HTTPS on port 8443.)

Connection type

Firewalls – Junos Space Collection tasks use a proprietary Juniper API to connect to Junos Space platforms.

Junos Space Network Management Platform collection tasks

Firewalls – Junos Space Collection tasks retrieve configuration data of Juniper Networks Junos firewalls managed by a Juniper Networks Junos Space Network Management Platform and add this data to the current model.

Note that:

- Dynamic routing rules cannot be collected from Junos Space platforms.
- There is a difference between the information available via SSH commands (in **Firewalls – Junos Collection** tasks) and that available via REST APIs (in

Firewalls – Junos Space Collection tasks). This may cause differences in the way the devices are represented in the model.

Task properties

The properties that control **Firewalls – Junos Space Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	The name or IP address of the Junos Space platform.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the Junos Space platform.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Collection	
Device Domains	A comma-separated list of logical domains in which the firewalls, whose data is collected, exist. **Note**: Use the *full* domain name (as it appears in the Junos Space UI)—**global/<domain name>**—and not just the domain name.
Import Specific Devices	Specifies whether to collect data for specific firewalls in the specified logical domains of the Junos Space platform. If cleared, data for all firewalls in the specified domains is collected.
Device Names	This field is enabled only if you select **Import Specific Devices**. A comma-separated list of the names of firewalls for which to collect configuration data. You can use * as a wildcard in the device names.
Advanced tab	
Location Hint	The location of the Junos Space platform. **Note**: Use this property if different locations use the same set of IP addresses, so that Junos Space platforms at different locations can have the same IP address.

JUNIPER NETWORKS NETSCREEN FIREWALL

You can add or update configuration data from Juniper Networks NetScreen firewalls to the current model:

- Using an online collection task:
  - Configure the firewalls (see page 129) to permit access from a Skybox Collector and create a collection task (see page 130) to collect the firewall configurations and add the configuration data to the model.

    The collection task can collect data from multiple firewalls.
- Using an offline file import task:
  - Generate and retrieve firewall configuration files and import their data into the model (see page 131).

    The file import task can import the data of multiple firewalls.

Configuring NetScreen firewalls for data collection

To configure a NetScreen firewall for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.
- Configure the firewall to permit collection. (The Skybox Collector must have permission to connect to the firewall using either SSH or Telnet.)

To import firewall change event log data (syslog data) from a NetScreen firewall (for a **Change Tracking Events – Syslog Import** task):

- Configure the firewall to send syslog messages to a Skybox Appliance or Collector; send the following commands to the server:

  ```
  set syslog config <IP address> facilities local0 local0
  ```

Connection type

Firewalls – NetScreen Collection tasks use the SSH protocol to connect to NetScreen firewalls.

Commands sent to device

Firewalls – NetScreen Collection tasks send the following commands to NetScreen firewalls:

- `set console page 0`
- `get vr all`
- `get hostname`
- `get config all`
- `get nsrp`
- `get system`
- `get vsys`
- `get route`
- `enter vsys <vsys>`

Juniper NetScreen collection tasks

Firewalls – NetScreen Collection tasks retrieve configuration data from NetScreen firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – NetScreen Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	The connection protocol to use.
SSH Port	If **Connection Protocol** = **ssh**, the port on which the firewalls listen. If you change the default port (22) on the firewalls, the Skybox Collector must have permission to connect to the firewalls on the port that you specify.
NetScreen Addresses	A comma-separated list of the IP addresses and IP address ranges of the NetScreen firewalls. To collect configurations of Virtual Systems, type an IP address for each physical firewall only. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Vsys List	A comma-separated list of names of Virtual Systems. If this field is empty, the configurations of all Virtual Systems are collected.
Firewall Filter	Specifies whether to collect all firewalls or only firewalls with at least 1 change event since the most recent collection.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewalls.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Location Hint	The location of the firewalls.

Property	Description
	Note: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

Importing NetScreen configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a NetScreen firewall configuration:

- `config.txt`: The NetScreen configuration file

  This file is the output of the NetScreen `get config all` command.

- (Optional) `route.txt`: Dump of the NetScreen routing table

  This file is the output of the NetScreen `get route` command.

You can import the configurations of multiple firewalls; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

If you need only the NetScreen configuration file, you can retrieve it via HTTP or TFTP.

To retrieve the configuration file of a NetScreen firewall via HTTP

1. In your browser, log in to the NetScreen web management tool.
2. From the menu on the left, select **Configuration** > **Update** > **Config File**.
3. Select **Save To File** and specify `config.txt`.
4. Use an SSH client to connect to the device CLI.
5. In a Command Prompt window, run the following command to get the version data: `get system`
6. Append the version data to the `config.txt` file saved at step 3.

To retrieve the configuration file of a NetScreen firewall via TFTP

1. Log in to the NetScreen firewall, using either Telnet or the firewall console.
2. Ensure that the TFTP server is running.
3. In a Command Prompt window, run:
   - `get config all > tftp <save file IP address> config.txt`
   - `get system > tftp <save file IP address> config_version.txt`
4. Append the content of `config_version.txt` to `config.txt`.

JUNIPER NETWORKS NETWORK AND SECURITY MANAGER

Juniper Networks Network and Security Managers (NSMs) manage multiple Juniper Networks NetScreen and Juniper Networks Junos firewalls.

You can add or update configuration data of the NetScreen and Junos firewalls managed by an NSM to the current model using an online collection task:

- Configure the NSM (see page 132) to permit access from a Skybox Collector and create a collection task (see page 132) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data of multiple NetScreen and Junos firewalls managed by an NSM.

To add or update configuration data from Juniper Networks NetScreen firewalls see Juniper Networks NetScreen firewall (on page 129).

To add or update configuration data from Juniper Networks Junos firewalls see Juniper Networks Junos firewall (on page 123).

Configuring Network and Security Manager for data collection

To configure a Network and Security Manager (NSM) for data collection:

- Create a separate global domain Read-Only Administrator account on the device for Skybox tasks.
- Configure the NSM to permit collection. (The Skybox Collector must have permission to connect to the NSM server using HTTPS on port 8443.)

Connection type

Firewalls – Juniper Networks NSM Collection tasks use a proprietary Juniper API to connect to NSMs.

Juniper Networks NSM collection tasks

Firewalls – Juniper Networks NSM Collection tasks retrieve configuration data of Juniper Networks firewalls managed by a Juniper Networks Network and Security Manager (NSM) and add this data to the current model.

Task properties

The properties that control **Firewalls – Juniper Networks NSM Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	The name or IP address of the NSM.
Port Number	The port on which the NSM listens. If you change the default port (8443) on the NSM, the Skybox Collector must have permission to connect to the NSM server using HTTPS on the port that you specify.
Firewall Filter	Specifies whether to collect configuration data of all (managed) firewalls, firewalls with at least 1 change event since the most recent collection (including new firewalls), or new firewalls only.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from

Property	Description
	CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the NSM.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Login Domain	The name of the domain to which **Username** and **Password** log in. If you are logging in to a subdomain, use **global.<subdomain name>**. If this field is empty, the task uses the **global** domain.
Collection	
Device Domains	A comma-separated list of logical domains in which the firewalls, whose data is collected, exist.
Import Specific Devices	Specifies whether to collect data for specific firewalls in the specified logical domains of the NSM. If cleared, data for all firewalls in the specified domains is collected.
Device Names	This field is enabled only if you select **Import Specific Devices**. A comma-separated list of the names of firewalls for which to collect configuration data. You can use ***** as a wildcard in the device names.
Device Type	Specifies whether to collect configuration data for NetScreen firewalls, Junos firewalls, or all Juniper firewalls.
Advanced tab	
Location Hint	The location of the NSM. **Note**: Use this property if different locations use the same set of IP addresses, so that NSMs at different locations can have the same IP address.

LINUX IPTABLES FIREWALL

You can add or update configuration data from Linux iptables firewalls to the current model using an offline file import task:

- Retrieve firewall configuration files and import their data into the model (see page 134).

  The file import task can import the data of multiple firewalls.

Importing Linux iptables configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Linux iptables firewall configuration:

- `ifconfig.txt`: The iptables interfaces configuration report

  This file is the output of the iptables `ifconfig -a` command.

- `filter.txt`: The iptables filter table

  This file is the output of the iptables `iptables -t filter -L -n -v` command.

- `nat.txt`: The iptables NAT table

  This file is the output of the iptables `iptables -t nat -L -n -v` command.

- `mangle.txt`: The iptables mangle table

  This file is the output of the iptables `iptables -t mangle -L -n -v` command.

- (If you are using ipset) `ipset.xml`: The iptables ipset table

  This file is the output of the iptables `ipset list -output xml` command.

You can import the configurations of multiple firewalls; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

MCAFEE ENTERPRISE (SIDEWINDER) FIREWALL

You can add or update configuration data from McAfee Enterprise (Sidewinder) firewalls to the current model using an online collection task:

- Configure the firewalls (see page 134) to permit access from a Skybox Collector and create a collection task (see page 135) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple firewalls.

Configuring McAfee Enterprise firewalls for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure a McAfee Enterprise firewall for data collection:

- Skybox data collection requires a user with admin permissions on the device; we recommend that you create a separate user for this purpose.

Connection type

Firewalls – McAfee Enterprise Collection tasks use the SSH protocol to connect to McAfee Enterprise firewalls.

Commands sent to device

Firewalls – McAfee Enterprise Collection tasks send the following commands to McAfee Enterprise firewalls:

- `cf service q`
- `cf host q`
- `cf iprange q`
- `cf netgroup q`
- `cf policy q`
- `cf route q`
- `cf appdb list verbose=on`
- `cf config version`
- `cf adminuser q`
- `cf policy q`
- `cf package list`
- `cf servicegroup q`
- `cf ipaddr q`
- `cf subnet q`
- `cf interface q`
- `cf static q`
- `cf netmap q`
- `cf application q`
- `cf ntp q`
- `cf hostname q`
- `cf cron q`
- `cf appgroup q`

Note: Not all commands are supported on all versions of the firewall.

McAfee Enterprise collection tasks

Firewalls – McAfee Enterprise Collection tasks retrieve configuration data from McAfee Enterprise firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – McAfee Enterprise Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the McAfee Enterprise firewalls. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewalls.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.

Property	Description
Port	The port on which the firewalls listen. If you change the default port (22) on the firewalls, the Skybox Collector must have permission to connect to the firewalls on the port that you specify.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

MICROSOFT AZURE FIREWALL

You can add or update configuration data from Microsoft Azure firewalls to the current model using an online collection task:

- Configure the firewalls (see page 136) to permit access from a Skybox Collector and create a collection task (see page 137) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple firewalls.

Configuring Azure firewalls for data collection

To retrieve data from Azure firewalls:

1. You must have an Azure subscription.
2. **Firewalls – Azure Collection** tasks requires credentials based on Azure Active Directory service principal functionality.

   Get these credentials from the Azure UI.
3. You need **Log Analytics Reader** (or higher) permissions for your app.

To get Azure credentials from the Azure UI

1. Log in to the Azure UI.
2. Get the **Application ID** by creating an app registration:

   a. Select **App registrations** > **New application registration**.

   b. Fill in the fields in the Create pop-up:

   - **Name**: The name of your app (for example, **Skybox–Collection**)
   - **Application Type**: Always set to **Web App/API**
   - **Sign-on URL**: The URL where you sign in to use the app (you can change this later)

   c. Click **Create**.

   Information about the **Skybox–Collection Registered app** is displayed.

   d. Copy the value of the **Application ID** and paste it into the **Client** field of the **Firewalls – Azure Collection** task that you are creating.

3 Get the app **Key**:

   a. From **Skybox–Collection Registered app**, select **Settings** > **Keys**.

   b. Fill in the fields in the Passwords pop-up:

   – **Description**: Your description of the key

   – **Expires**: The duration of the key

   c. Click **Save**.

   The key is displayed in the **Value** field.

   d. Copy the key and paste it into the **Key** field of the **Firewalls – Azure Collection** that you are creating.

   Important: Copy this key; after you leave the pop-up, the value is hidden.

4 Get the **Directory ID**:

   a. From **Skybox–Collection Registered app**, select **Azure Active Directory** > **Properties**.

   b. Copy the value of the **Directory ID** and paste it into the **Tenant** field of the **Firewalls – Azure Collection** task that you are creating.

5 (Optional) If you are collecting data from 1 subscription, get the **Subscription ID**:

   a. From the main menu, select **Subscription**.

   A list of all subscriptions is displayed.

   b. Copy the value of the relevant **Subscription ID** and paste it into the **Subscription** field of the **Firewalls – Azure Collection** task that you are creating.

To assign permissions to your app

1 Log in to the Azure UI.

2 Select **Subscription** > **<Subscription Name>** > **Access control (IAM)**.

3 Fill in the fields in the Add permissions pop-up:

   a. **Role**: The permissions to assign to your app (select **Log Analytics Reader** (or higher))

   b. **Select**: The name of your app (select from the drop-down list)

   The app is added to the **Selected members** list.

4 Click **Save**.

Connection type

Firewalls – Azure Collection tasks use the Azure SDK to connect to Azure firewalls.

Microsoft Azure collection tasks

Firewalls – Azure Collection tasks retrieve configuration data from Azure firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – Azure Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Tenant	Take values for these properties (*Directory ID*, *Application ID*, and *Key* respectively) from the Azure service principal-based authentication file that you created for the task (see Configuring Azure firewalls for data collection (on page 136)).
Client	
Key	
Subscription	If **Collect all subscriptions** is cleared, collect data from this *Subscription ID* (see Configuring Azure firewalls for data collection (on page 136)).
Collect all subscriptions	Specifies whether to collect data for all subscriptions.
Advanced tab	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system Temp directory.
Use Proxy	Specifies whether to use HTTP proxy settings.
Proxy Username	Only required if you select **Use Proxy**. Configuration of the proxy that the task must use to connect to the firewalls.
Proxy Password	
Proxy Host	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

PALO ALTO NETWORKS FIREWALL

You can add or update configuration data (including IPS data) from Palo Alto Networks firewalls to the current model:

- Using an online collection task:
  - Configure the firewalls (see page 139) to permit access from a Skybox Collector and create a collection task (see page 139) to collect the firewall configurations and add the configuration data to the model.

    The collection task can collect data from multiple firewalls.
- Using an offline file import task:

- Generate and retrieve firewall configuration files and import their data into the model (see page 140).

  The file import task can import the data of multiple firewalls.

Configuring Palo Alto firewalls for data collection

To configure a Palo Alto firewall for data collection:

- Skybox data collection requires a Super User on the device; we recommend that you create a separate Super User for this purpose.
- Configure the firewall to permit collection. (The Skybox Collector must have permission to connect to the firewall using HTTPS on port 443, and either SSH or Telnet.)

Connection type

Firewalls – Palo Alto Networks Collection tasks use a combination of a REST API and the SSH protocol to connect to Palo Alto firewalls.

Commands sent to device

Firewalls – Palo Alto Networks Collection tasks send the following SSH commands to Palo Alto firewalls:

- `show system info`
- `set cli pager off`
- `show routing route`

Palo Alto Networks collection tasks

Firewalls – Palo Alto Networks Collection tasks retrieve configuration data (including IPS rules) from Palo Alto firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – Palo Alto Networks Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	A comma-separated list of the names or IP addresses and IP address ranges of the Palo Alto firewalls.
Import specific vsys	Specifies whether to collect configuration data for specific virtual systems running on the device. If cleared, configuration data for all virtual systems on the device is collected.
Vsys list	This field is enabled only if you select **Import specific vsys**. A comma-separated list of the names of virtual systems for which to collect configuration data. You can use ***** as a wildcard in the names.
Firewall Filter	Specifies whether to collect all firewalls or only firewalls with at least 1 change event since the most recent collection.

Property	Description
Authentication	
Method	- **Device**: Use the authentication credentials provided here. - **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewall.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Https port	The port on which the firewall listens. If you change the default port (443) on the firewall, the Skybox Collector must have permission to connect to the firewall using HTTPS on the port that you specify.
Connection Protocol	The connection protocol to use.
SSH Port	If **Connection Protocol** = **ssh**, the port on which the firewall listens.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

Importing Palo Alto configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Palo Alto firewall configuration:

- An XML file containing the Palo Alto configuration data.
- (Optional) `route.txt`: A file containing the Palo Alto dynamic routing table

Important: The Palo Alto API calls return raw XML. You must encode special characters before running the **Import – Directory** task (for example, replace & with &amp). If you need assistance, contact Skybox Professional Services.

You can import the configurations of multiple firewalls; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

To create a file containing the firewall configuration

1. Generate and save the API key required for authenticating API calls. You need the key in subsequent steps of this procedure.

   The API key is returned by the following URL request:

   - `https://<IP address of firewall>/api/?type=keygen&user=<admin name>&password=<password>`

2. Create a file in a text editor.
3. Add the line `<?xml version="1.0" encoding="UTF-8" ?>` to the file.
4. Add the tags `<response status="success">` and `</response>`.
5. Inside these tags:

   a. Add the line `<palo_alto_xml_config/>`.

   b. Add the tag pair `<result>` and `</result>`.

6. Add the response to the following URL request (replace `<key>` with the API key generated at step **1**) inside the `<result>` tag pair. Discard the `<response>`, `</response>`, `<result>` and, `</result>` tags in the response but include the content inside the tags.

   - `https://<IP address of firewall>/api/?type=config&action=show&key=<key>`

   This adds the configuration data.

7. Add the responses to the following URL requests (replace `<key>` with the API key generated at step **1**) *in this order* inside the `<shared>` tag pair. Discard the `<response>`, `</response>`, `<result>` and, `</result>` tags in the response but include the content inside the tags.

   - Predefined applications: `https://<IP address of firewall>/api/?type=config&action=get&xpath=/config/predefined/application&key=<key>`
   - Application filters: `https://<IP address of firewall>/api/?type=config&action=get&xpath=/config/devices/entry/vsys/entry/application-filter&key=<key>`
   - Application groups: `https://<IP address of firewall>/api/?type=config&action=get&xpath=/config/devices/entry/vsys/entry/application-group&key=<key>`
   - Services: `https://<IP address of firewall>/api/?type=config&action=get&xpath=/config/predefined/service&key=<key>`
   - Threats (IPS signatures on the device): `https://<IP address of firewall>/api/?&type=config&action=get&xpath=/config/predefined/threats/vulnerability&key=<key>`
   - Dynamic address group: `https://<IP address of firewall>/api/?type=op&action=get&cmd=<show><object><dynamic-address-group><all></all></dynamic-address-group></object></show>&key=<key>`
   - High Availability: `https://<IP address of firewall>/api/?type=op&action=get&cmd=<show><high-`

availability><state></state></high-availability></show>&key=<key>

- System: https://<IP address of firewall>/api/?type=op&action=get&cmd=<show><system><info></info></system></show>&key=<key>
- Layer 3 interfaces: https://<IP address of firewall>/api/?type=op&action=get&cmd=<show><interface>all</interface></show>&target=<target>&key=<key>

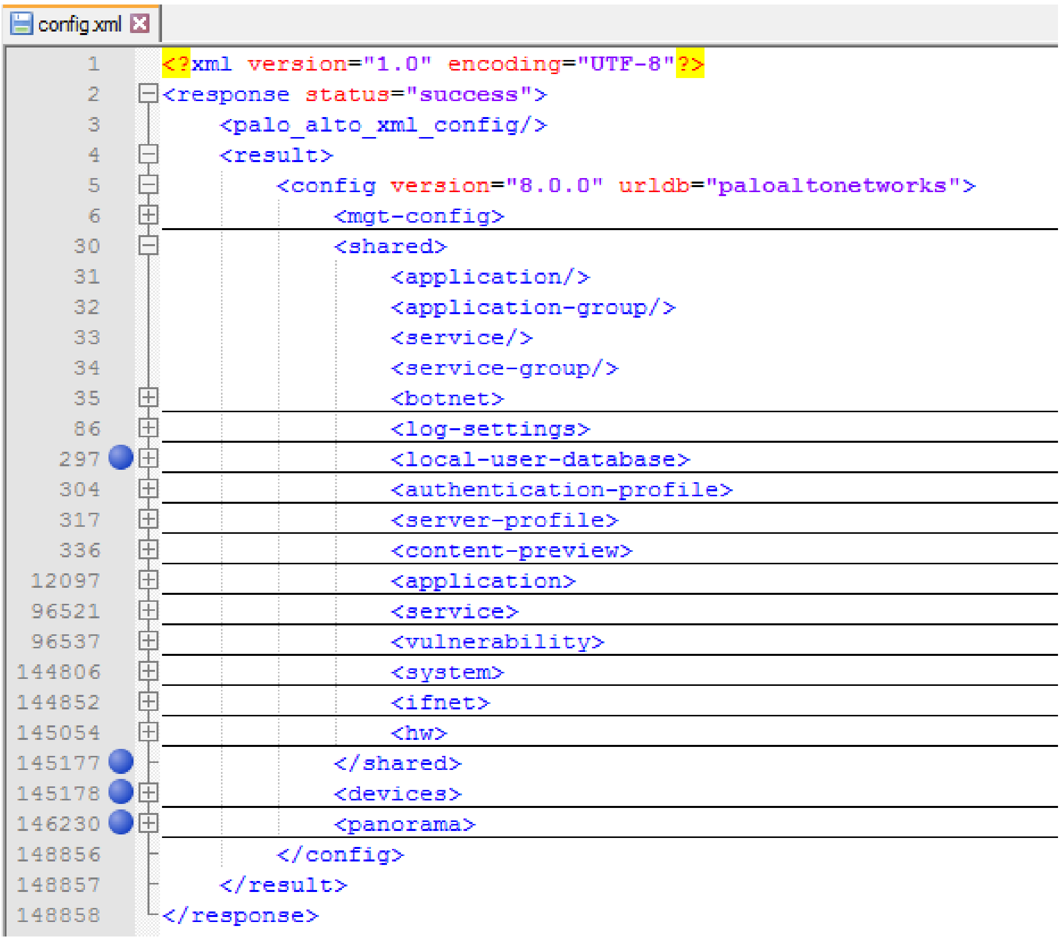
8 Add the response to the following URL request (replace <key> with the API key generated at step **1**) immediately after the </devices> tag. Discard the <response>, </response>, <result> and, </result> tags in the response but include the content inside the tags.

- https://<IP address of firewall>/api/?type=config&action=get&&xpath=/config/panorama&key=<key>

This adds the Panorama Pre Rules and Post Rules.

9 Save the file.

The following figure shows the (collapsed) structure of the file.



```
<?xml version="1.0" encoding="UTF-8"?>
<response status="success">
    <palo_alto_xml_config/>
    <result>
        <config version="8.0.0" urldb="paloaltonetworks">
            <mgt-config>
            <shared>
                <application/>
                <application-group/>
                <service/>
                <service-group/>
                <botnet>
                <log-settings>
                <local-user-database>
                <authentication-profile>
                <server-profile>
                <content-preview>
                <application>
                <service>
                <vulnerability>
                <system>
                <ifnet>
                <hw>
            </shared>
            <devices>
            <panorama>
        </config>
    </result>
</response>
```

10 Issue the `show system info` command to the firewall via Telnet or SSH and append the output to the file.

11 Save the file.

To create a file containing the dynamic routing table

- Issue the following commands to the firewall via Telnet or SSH:
  - `set cli pager off`
  - `show routing route`

Importing external dynamic lists (EDLs) of IP addresses

An EDL is a text file that a firewall uses to import objects.

You can import EDLs of type **IP Address** with the rest of the firewall configuration. (EDLs of type **URL** and type **Domain** are not supported.)

To add EDLs to a file containing the firewall configuration

Note: You need the API key that you generated in the previous procedure.

1 Add the tag pair <edls> and </edls> before the </config> tag (following the </panorama> tag) in the XML file containing the Palo Alto configuration data.

2 Add the tag pair <vsys> and </vsys> inside the <edls> tag pair.

3 Change the target to a vsys of the firewall by sending the following URL request (replace <key> with the API key generated at step **1** of the previous procedure; replace <vsys-name> with the name of a vsys):

   - `https://<IP address of firewall>/api/?type=op&action=get&cmd=<set><system><setting><target-vsys><vsys-name></target-vsys></setting></system></set>&key=<key>`

4 Retrieve the list of EDLs in this vsys by sending the following URL request (replace <key> with the API key generated at step **1** of the previous procedure):

   - `https://<IP address of firewall>/api/?type=op&action=get&cmd=<request><system><external-list><show><type><predefined-ip><name></name></predefined-ip></type></show></external-list></system></request>&key=<key>`

5 For each EDL, add the response to the following URL request (replace <key> with the API key generated at step **1** of the previous procedure; replace <edl-name> with the name of an EDL) inside the <vsys> tag pair.

   - `https://<IP address of firewall>/api/?type=op&action=get&cmd=<request><system><external-list><show><type><ip><name><edl-name></name></ip></type></show></external-list></system></request>&key=<key>`

6 Repeat steps **3** to **5** for each vsys.

   The structure of this part of the file should look like this:

```
<edls>
   <vsys>
```

```
      <entry name=" vsys1">
         <external-list>
            <entry name="{edl1}">
               CONTENT
            </entry>
            <entry name="{edl2}">
               CONTENT
            </entry>
            ...
         </external-list>
      </entry>
      <entry name=" vsys2">
         <external-list>
            ...
         </external-list>
      </entry>
      ...
   </vsys>
</edls>
```

PALO ALTO NETWORKS PANORAMA

Palo Alto Networks Panoramas manage multiple Palo Alto Networks firewalls.

You can add or update configuration data of the Palo Alto Networks firewalls managed by a Panorama to the current model using an online collection task:

- Configure the Panorama (see page 144) to permit access from a Skybox Collector and create a collection task (see page 145) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data of multiple Palo Alto Networks firewalls managed by a Panorama.

To add or update configuration data from Palo Alto Networks firewalls see Palo Alto Networks firewall (on page 138).

Configuring Panorama for data collection

To configure a Panorama for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

  The user that accesses the device *must* have permissions for the following modules:

  - Configuration
  - Operational Requests
  - Commit

  Note: The Commit module requires write permissions, but this is only necessary if automatic implementation is enabled and changes are made to the configuration on the device during Panorama device collection. For information about automatic implementation, see the Configuring automatic implementation section in the Skybox Change Manager User Guide.

- Configure the device to permit collection. (The Skybox Collector must have permission to connect to the device using HTTPS on port 443.)

Connection type

Firewalls – Panorama Collection tasks use a REST API to connect to Panoramas.

Palo Alto Networks Panorama collection tasks

Firewalls – Panorama Collection tasks retrieve configuration data (including IPS rules) from Palo Alto Networks firewalls managed by a Palo Alto Networks Panorama and add this data to the current model.

Task properties

The properties that control **Firewalls – Panorama Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	The name or IP address of the Panorama.
Firewall Filter	Specifies whether to collect configuration data of all (managed) firewalls, firewalls with at least 1 change event since the most recent collection (including new firewalls), or new firewalls only.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the firewall.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Collection	
Device Groups	A comma-separated list of device groups from which to collect Palo Alto Networks firewall configuration data.
Import Specific Devices	Specifies whether to collect configuration data of specified Palo Alto Networks firewalls instead of collecting the data of all the Palo Alto Networks firewalls in the device groups.
Device Names	This field is enabled only if you select **Import Specific Devices**. A comma-separated list of Palo Alto Networks firewall names.

Property	Description
Advanced tab	
Https port	The port on which the Panorama listens. If you change the default port (443) on the Panorama, the Skybox Collector must have permission to connect to the Panorama server using HTTPS on the port that you specify.
Location Hint	The location of the Panorama. **Note**: Use this property if different locations use the same set of IP addresses, so that Panoramas at different locations can have the same IP address.

SIDEWINDER G2 (MCAFEE ENTERPRISE) FIREWALL

You can add or update configuration data from Sidewinder G2 (McAfee Enterprise) firewalls to the current model using an offline file import task:

- Generate, retrieve, and parse firewall configuration files and import their data into the model (see page 146).

  The file import task can import the data of multiple firewalls.

Importing Sidewinder G2 configuration data

To import Sidewinder G2 firewall configurations

1 Generate and retrieve the required Sidewinder G2 configuration files (see Generating Sidewinder G2 configuration files (on page 146)).

2 Parse the configuration files using the Skybox Sidewinder G2 parser (see Parsing Sidewinder G2 configuration files (on page 147)).

3 In the Skybox Operational Console:

a. Create a task.

b. Set **Task Type** to **Import – Directory** (see Import directory tasks (on page 39)).

c. In the **Directory** field, specify the location of the iXML file created in step **2**.

Note: You can import the configurations of multiple firewalls; give a different name to each file created by the parser.

4 Launch the task.

Generating Sidewinder G2 configuration files

To generate Sidewinder configuration files

1 Connect to the Sidewinder firewall.

a. Log in as admin (the `cf` command must be executed by a system administrator).

b. Issue the `srole` command at the shell prompt to enter the administration shell.

2 Generate the required files by running the following commands from the Sidewinder command-line interface:

   - (Optional) burb definition: `cf burb query > /tmp/burbQuery.txt`
   - ipfilter data: `cf ipfilter query > /tmp/ipfilterQuery.txt`
   - Proxy rules data: `cf acl query > /tmp/aclQuery.txt`
   - Interfaces and burbs: `cf interface query > /tmp/interfaceQuery.txt`
   - Proxy services definitions: `cf proxy query > /tmp/proxyQuery.txt`
   - (Optional) Routing information: `netstat -nr > /tmp/routingInfo.txt`

Parsing Sidewinder G2 configuration files

Skybox includes a parser that creates an iXML file from Sidewinder G2 firewall configuration files. This iXML file can then be imported into Skybox.

The Skybox Sidewinder G2 parser supports the following Sidewinder features:

- IP filtering: A simple stateful packet filter that inspects the source and destination IP addresses, port, and protocol (Layers 3 and 4).
- Transparent proxy: The firewall intercepts every connection attempt and opens the connection on the user’s behalf. The firewall makes all internet connections so that the internal network does not communicate directly with the internet. Access to the proxy services of the firewall is controlled by an access rule, which is similar to the IP filtering feature. However, in addition to an accept or drop action, authentication and application layer inspection might be required.
- Application firewall: The firewall enforces a positive policy that specifies the actions that are permitted.

The Skybox Sidewinder G2 parser is `<Skybox_Home>\intermediate\bin\parsers\firewalls\sidewinder\SideWinderParser.pl`

Syntax

```
SideWinder.pl -h <host name> -i <interfaces file> -f <ipfilter file>
              -a <acl file> -p <proxies file>
              [-r <routing information file>] [-b <burbs file>]
              [-v silent | standard | debug] -o <output XML file>
```

The Skybox Sidewinder G2 parser arguments are described in the following table.

Argument	Value
-h	Host name of the Sidewinder firewall **Note**: Ignored if you provide the `cf burb query` output file (**-b** argument)
-i	`cf interface query` output file
-f	`cf ipfilter query` output file
-a	`cf acl query` output file
-p	`cf proxy query` output file
-r	`netstat -nr` output file

Argument	Value
-b	cf burb query output file
-v	Verbose level (silent, standard, or debug)
-o	File name to store parsing results

SOPHOS UNIFIED THREAT MANAGEMENT FIREWALLS

You can add or update configuration data of Sophos UTM firewalls to the current model using an online collection task:

- Configure the firewalls (see page 148) to permit access from a Skybox Collector and create a collection task (see page 148) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect the configuration data from multiple firewalls.

Configuring Sophos UTM firewalls for data collection

To configure a Sophos UTM firewall for data collection:

- Skybox data collection requires a read-only user on the firewall; we recommend that you create a separate user for this purpose.

Connection type

Firewalls – Sophos UTM Collection tasks use a REST API to connect to UTM firewalls.

Sophos UTM collection tasks

Firewalls – Sophos UTM Collection tasks retrieve configuration data from Sophos firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – Sophos UTM Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of IP addresses of Sophos UTM firewalls, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 4444. **Note**: A task can collect the configurations of multiple firewalls only if the same authentication is used for all the firewalls.
Username	The user name to access the firewalls.
Password	The user password.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls.

Property	Description
	Note: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

VMWARE VSHIELD EDGE FIREWALL

You can add or update configuration data from VMware vShield Edge firewalls to the current model using an online collection task:

- Configure the firewall manger (see page 149) to permit access from a Skybox Collector and create a collection task (see page 149) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data from multiple virtual firewalls on a device.

Configuring VMware vShield Edge firewalls for data collection

To configure a vShield Edge firewall for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Firewalls – VMware vShield Edge Collection tasks use a web service to connect to vShield Edge firewalls.

VMware vShield Edge collection tasks

Firewalls – VMware vShield Edge Collection tasks retrieve configuration data from vShield Edge firewalls and add this data to the current model.

Task properties

The properties that control **Firewalls – VMware vShield Edge Collection** tasks are described in the following table.

Property	Description
Basic tab	
vShield Management IP	The IP address of the vShield Edge Manager.
Username	The user name to access the vShield Edge Manager.
Password	The user password.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

ZSCALER CLOUD SECURITY PLATFORMS

Zscaler Cloud Security Platforms manage multiple Zscaler Cloud Firewalls.

You can add or update configuration data of the Zscaler Cloud Firewall managed by a Zscaler Cloud Security Platform to the current model using an online collection task:

- Configure the Zscaler Cloud Security Platform (see page 150) to permit access from a Skybox Collector and create a collection task (see page 150) to collect the firewall configurations and add the configuration data to the model.

  The collection task can collect data of multiple Zscaler Cloud Firewalls managed by a Zscaler Cloud Security Platform.

Configuring Zscaler Cloud Security Platforms for data collection

To configure a Zscaler Cloud Security Platform for data collection:

- Skybox data collection requires a read-only user on the platform; we recommend that you create a separate user for this purpose.
- You need a Zscaler API key for the task to access the configuration data.

To obtain a Zscaler API key

1. Log in to the Zscaler Cloud Security Platform.
2. Navigate to **Administration** > **API Key Management**.
3. Note the API key; you need it when you create the **Secure Web Gateway – Zscaler** task.

Connection type

Secure Web Gateway – Zscaler tasks use a Zscalar cloud web service API over HTTPS to connect to Zscaler Cloud Security Platforms.

Zscaler collection tasks

Secure Web Gateway – Zscaler tasks retrieve Zscaler Cloud Firewall configuration data from Zscaler Cloud Security Platforms and add this data to the current model.

Task properties

The properties that control **Secure Web Gateway – Zscaler** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Cloud	The name of the Zscaler Cloud Security Platform containing the configuration data of your Zscaler Cloud Firewalls.
Username	The user name to access the Zscaler Cloud Security Platform.
Password	The user password.
API Key	The user API key for the Zscaler Cloud Security Platform.
Advanced tab	
Use Proxy	Specifies whether to use HTTP proxy settings.

Property	Description
Proxy Username	Only required if you select **Use Proxy**. Configuration of the proxy that the task must use to connect to the Platform.
Proxy Password	
Proxy Host	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the firewalls. **Note**: Use this property if different locations use the same set of IP addresses, so that firewalls at different locations can have the same IP address.

FIREWALLS IMPLEMENTED IN SOFTWARE

You can add or update configuration data from firewalls implemented in software to the current model:

- Using an online collection task:
  - Configure the firewalls (see page 151) to permit access from a Skybox Collector and create a collection task (see page 152) to collect the firewall configurations and add the configuration data to the model.

    Network State Collection tasks can collect configuration data from firewalls running on the following platforms:

    - Nokia
    - Linux
    - SPLAT
    - Solaris

    Each task can collect data from a single platform type only.
- Using an offline file import task:
  - See Importing interface and routing configuration (on page 60) for information.

Configuring software firewalls for data collection

To configure a device running a firewall implemented in software for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.
- Configure the device to permit collection. (The Skybox Collector must have permission to connect to the firewall application using either SSH or Telnet.)

SPLAT

To run a **Network State Collection** task to collect data from a firewall running on a SPLAT platform:

- (Recommended) Create a special user in the Bash shell (instead of cpshell).

Platform-dependent commands

The `ifconfig` and `netstat` commands that **Network State Collection** tasks run for the different supported platforms are listed in the following table.

Platform	ifconfig	netstat
Nokia	ifconfig -a	netstat -nr
Linux	ifconfig -a	netstat -nrv
SPLAT	/bin/save_ifconfig	/bin/netstat -nrv
Solaris	ifconfig -a	netstat -nrv

Network state collection tasks

Network State Collection tasks collect configuration data (routing rules and network interface) from firewalls that are implemented in software on top of an operating system.

Task properties

The properties that control **Network State Collection** tasks are described in the following table.

Property	Description
Basic tab	
Platform	The platform from which to collect the configuration data.
Connection Protocol	The connection protocol to use.
SSH Port	If **Connection Protocol** = **ssh**, the port on which the firewall listens. If you change the default port (22) on the device, the Skybox Collector must have permission to connect to the device on the port that you specify.
Device Addresses	A comma-separated list of the IP addresses and IP address ranges of the devices whose routing rules are collected.
Device prompt	The prompt for devices specified in **Device Addresses**. **Note**: If the prompt ends with the 2 characters **]#** (a right bracket followed by a hash sign), you can leave this field empty.
Authentication	
Username	The user name of a user of the device.
Password	The user password.
Advanced tab	
Get Network Interfaces Command	This field is enabled only if **Platform** = **Linux** in the **Basic** tab.
Location Hint	The location of the destination network. **Note**: Use this property if different locations use the same set of IP addresses, so that networks at different

Property	Description
	locations can have the same IP address.

Chapter 5

Firewall rule usage analysis tasks

This chapter describes how to add firewall log data for rule usage analysis to the current model.

In this chapter

SYSLOG TRAFFIC EVENTS

You can add or update syslog-formatted activity log data to the current model using an online collection task. The following device types are supported:

- Check Point FireWall-1
- Cisco Firepower
- Cisco IOS
- Cisco PIX/ASA/FWSM
- Forcepoint (StoneGate)
- Fortinet FortiGate
- Juniper Networks Junos
- Juniper Networks NetScreen
- McAfee Enterprise (Sidewinder)
- Palo Alto Networks

To add syslog traffic events

1 Before running a **Traffic Events – Syslog Import** task for the 1st time, add the configuration data of the device to the current model by running the relevant task:

   - Firewalls – Check Point FireWall-1 CPMI Collection (FireWall-1) (see page 74) or Firewalls – Check Point FireWall-1 CPMI Collection (Provider-1) (see page 86)
   - Firewalls – Cisco Firepower Management Center Collection (see page 98)
   - Routers – Cisco IOS Collection (see page 192)
   - Firewalls – Cisco PIX/ASA/FWSM Collection (see page 102)
   - Firewalls – Forcepoint NGFW Collection (see page 111)

- Firewalls – FortiGate Collection (see page 114)
- Firewalls – Junos Collection (see page 125)
- Firewalls – NetScreen Collection (see page 130)
- Firewalls – McAfee Enterprise Collection (see page 135)
- Firewalls – Palo Alto Networks Collection (see page 139)

2 Configure the logged devices to permit access from a Skybox Collector. Configuring devices is described in:

- For Check Point firewalls, configure the firewall to forward activity data to a syslog server (the task then collects the logs from the syslog server):

  Configuring Check Point firewalls to send activity logs to a syslog server (see page 156)
- Configuring Cisco Firepower Management Center for data collection (see page 98)
- Configuring Cisco IOS routers for data collection (see page 189)
- Configuring Cisco PIX/ASA/FWSM firewalls for data collection (see page 100)

  We recommend that you enable logging using syslog messages 10610x (see page 155)
- Configuring Forcepoint NGFW appliances for data collection (see page 111)
- Configuring FortiGate firewalls for data collection (see page 112)
- Configuring Junos firewalls for data collection (see page 124)
- Configuring NetScreen firewalls for data collection (see page 129)
- Configuring McAfee Enterprise firewalls for data collection (see page 134)
- Configuring Palo Alto Networks firewalls for data collection (see page 139)

3 If you are collecting CEF formatted syslog, modify `pa_log_rules.txt` to match your CEF syslog records. See Using CEF-formatted syslog (see page 157) for information about this file.

4 Create a collection task (see page 161) to collect the logs and add their data to the model.

Skybox uses activity log data for rule usage analysis, which is described in the Skybox Firewall Assurance User Guide.

Note: Alternatively, log data from Check Point firewalls for rule usage analysis can be collected and added using Check Point FireWall-1 LEA collection tasks (see page 164). However, we recommend that you use Check Point Log Exporter whenever possible.

Configuring Cisco firewalls to log using syslog messages 10610x

We recommend that you configure Cisco PIX/ASA/FWSM firewalls to log using syslog messages 106100 and 106102:

› If a firewall is configured to send a syslog message for every event and the firewall is attacked, the number of syslog messages for denied packets can be very large. Syslog message 106100, which provides statistics per access rule, limits the number of syslog messages produced. Syslog message 106102 is the VPN/AAA filter equivalent of message 106100.

- For information about configuring ACL logging on Cisco firewalls, see http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/acl_logging.html#51687

Note: Access rules are named access control entries (ACEs) by Cisco.

- For information about syslog messages 106100 and 106102, see https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog/syslogs1.html#con_4769049

- **Traffic Events – Syslog Import** tasks filter records from the log. Only messages 10610x (that is, 106100-106103) are parsed and their data added to the model.

Configuring Check Point firewalls to send activity logs to a syslog server

Check Point Log Exporter

We recommend that you use Check Point Log Exporter whenever possible.

To get syslog records via Check Point Log Exporter

1. Configure the Check Point devices to forward syslog traffic logs to Skybox Collectors in syslog format.

   Check Point Log Exporter installation instructions are available at:

   https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323

2. Configure a task of type **Traffic Events – Syslog Import** to import the logs (see Syslog traffic events collection tasks (on page 161)).

Alternative methods

You can add or update firewall activity log data from Check Point FireWall-1 NG and NGX firewalls to the current model using a **Firewalls – Check Point FireWall-1 LEA Collection** task (see Check Point FireWall-1 activity log data (on page 163)). To retrieve this data a Skybox Collector must have permission to access the Check Point device holding the firewall activity logs.

If access to the Check Point device is not permitted, you can collect and add log data for rule usage analysis using a **Traffic Events – Syslog Import** task. In this case, configure the Check Point device to forward the activity data to a syslog server.

How to forward activity logs to a syslog server

1. On the Check Point Management Server or Multi-Domain Server (MDS), add the following line to /etc/syslog.conf

```
local4.info[tab character]@<IP address of the syslog server>
```

2. Modify /etc/rc.local:

   - (Management Server architecture) On the log server add the following line

```
fw log -ftnlp 2> /dev/null | awk 'NF' | logger -p local4.info -t Firewall &
```

- (Provider-1 architecture) For each Domain Server (CMA) in the MDS add the following 2 lines

```
mdsenv cmaname ; $FWDIR/bin/fw log -ftnlp fw.adtlog | logger -t "cma name "
-p local4.info &
mdsenv cmaname ; $FWDIR/bin/fw log -ftnlp fw.log | logger -t "Provider
cmaname " -p local4.info &
```

For additional information about the `fw log` command, refer to the *fw log* entry (https://sc1.checkpoint.com/documents/R77/CP_R77_CLI_ReferenceGuide_WebAdmin/html_frameset.htm) in the *Command Line Interface R77 Reference Guide*.

3 Reboot the device running the Check Point log server.

Note: You must reboot the device; it is not sufficient to use the `cpstop` and `cpstart` commands.

4 Enable communication from the Check Point log server to the syslog server on port UDP 514.

Examples of the required format of Check Point syslog records

- Check Point Management Server architecture:

```
2013-01-02 10:17:06 Local4.Info     62.90.0.2  Firewall: 2Nov2012
8:08:44 accept 62.90.0.2 >eth1 rule: 1; rule_uid: {5AB2ED5F-16FF-
4F66-8BAF-736BF620EC81}; service_id: TCP-7800; src: 192.168.30.2;
dst: 192.168.80.198; proto: tcp; product: VPN-1 & FireWall-1;
service: 7800; s_port: 56266; product_family: Network;
```

- Check Point Provider-1 architecture:

```
2013-01-06 17:05:09 Local4.Info     10.20.0.2  cma1: 16Sep2012
16:51:08 accept 10.12.0.2 >eth0 rule: 1; rule_uid: {42B0B1D4-73B6-
4FEC-97D0-9BBE0AF18742}; service_id: telnet; src: 192.168.80.159;
dst: 10.12.0.2; proto: tcp; product: VPN-1 & FireWall-1; service:
23; s_port: 54143; product_family: Network;
```

Using CEF-formatted syslog

If you are using CEF-formatted syslog, modify `<Skybox_Home>\collector\conf\collector_commands\pa_log_rules.txt` on the Skybox Collector machine before running the **Traffic Events – Syslog Import** task.

This file contains multiple key sets that check each line in the syslog file for traffic events.

- See here (on page 159) for an explanation of the fields in the file.
- See here (on page 160) to view the default file.

For example, if you made any changes to names of properties on the device, change the key values in this file accordingly.

How the parsing procedure finds traffic events

The parsing procedure (in **Traffic Events – Syslog Import** tasks) checks all lines in the syslog file to find traffic events.

- Lines from the syslog file are only matched if they contain one of the hints.
- The following fields are mandatory:
  - Timestamp (FULL_DATE)

    You must also configure DATE_FORMAT in the key set
  - Source (SOURCE_PAT)
  - Destination (DESTINATION_PAT)
  - GUID (POLICY_ID_PAT): The GUID of the ACL, which is retrieved from the device (and then searched for when trying to do the match)
  - Device ID (SERIAL_ID_PAT)
- If a mandatory field that appeared in the 1st key set does not appear in a subsequent key set, the value of that field is based on the 1st key set.
- The following delimiter separates between a field name and its pattern: "__-__".
- Spaces in a pattern are considered as part of the pattern. For example, for the field "SERIAL_ID_PAT__-__orig= ", the parser looks for "orig= "; it does not ignore the space.
- Each key set is delimited by "__-__end of set__-__"
- You can add more fields and more key sets as necessary (some are controlled via ArcSight).

  You can add fields that contain an underscore ("_") in their name even if they start with an underscore.

The parsing procedure is:

1. Each syslog line is checked against the 1st key set.
2. If the line being compared does not match all the fields in the key set, the search continues with the next key set.
3. The following error message is written if any of the following is missing: `Header doesn't contain needed values which are defined under HINT. Skipping this set`
4. Without the above fields, a line is marked automatically as invalid. However, it is not sufficient to find them in syslog to get a match as this is between parsed syslog and a matched ACL.

Sample line in a syslog file

The following line is parsed as a traffic event by the default version of `pa_log_rules.txt` because it contains the strings `CEF:` and `traffic`.

```
private static final String LINE = "Apr  7 16:23:55 pa-2020 CEF:0|Palo Alto
Networks|PAN-OS|4.1.0|end|TRAFFIC|1|rt=Apr 07 2014 13:23:55 GMT
deviceExternalId=0004C101384 src=192.168.80.220 dst=172.20.0.250
sourceTranslatedAddress=0.0.0.0 destinationTranslatedAddress=0.0.0.0
cs1Label=Rule cs1=cleanup suser= duser= app=my ICMP cs3Label=Virtual System
cs3=vsys1 cs4Label=Source Zone cs4=trust cs5Label=Destination Zone
cs5=trust deviceInboundInterface=ethernet1/1
deviceOutboundInterface=ethernet1/1 cs6Label=LogProfile cs6=log_profile
cn1Label=SessionID cn1=63687 cnt=3 spt=0 dpt=0 sourceTranslatedPort=0
destinationTranslatedPort=0 flexString1Label=Flags flexString1=0x0
proto=icmp act=allow flexNumber1Label=Total bytes flexNumber1=354 in=180
out=174 cn2Label=Packets cn2=6 PanOSPacketsReceived=3 PanOSPacketsSent=3
start=Apr 07 2014 13:23:49 GMT cn3Label=Elapsed time in seconds cn3=0
cs2Label=URL Category cs2=any externalId=645104"
```

Fields for matching CEF formatted syslog

Typical fields that can be included in pa_log_rules.txt are described in the following table.

Field	Mandatory	Description
POLICY_ID_PAT	Yes	The GUID of the ACL, retrieved from the device
SOURCE_PAT	Yes	Traffic source IP
SOURCE_PORT_PAT		Traffic source port
DESTINATION_PAT	Yes	Traffic destination IP
DESTINATION_PORT_PAT		Traffic destination port
SERIAL_ID_PAT	Yes	Device host name or IP address
FULL_DATE	Yes	Traffic timestamp (according to the selected date format)
DATE_FORMAT		Date format The following date formats are supported: - yyyy/MM/dd HH:mm:ss - yyyy-MM-dd HH:mm:ss - yyyy-dd-MM HH:mm:ss - dd-MM-yyyy HH:mm:ss - MM-dd-yyyy HH:mm:ss - MMM d yyyy HH:mm:ss - EEE, MMM d, ''yy HH:mm:ss - EEE, d MMM yyyy HH:mm:ss Z - MMM dd HH:mm:ss - yyyy-MM-dd'T'HH:mm:ssZ - yyyy-MM-dd'T'HH:mm:ss.SSS - yyyy-MM-dd: HH:mm:ss - ddMMMyyyy HH:mm:ss - yyyy/dd/MM HH:mm:ss - yyyyMMdd`HH:mm:ss - yyyyMMdd HHmmss - Unix epoch format is automatically recognized for parsing purposes; select any format for this field
SERVICE_PAT		Protocol and port
PROTOCOL_PAT		Protocol
LOG_ID_PAT		Log file ID

Field	Mandatory	Description
HINT	Yes	Text that indicates that this line is in CEF format The default hint is `HINT__-__traffic&&CEF`: This means that the strings `traffic` and `CEF:` must appear in the line. If these strings are not used in your syslog files, choose a unique text for the lines in the file that are to be considered for CEF checking. **Note**: If necessary, use || for OR.
ICMP_TYPE_PAT		
VD_PAT		
APPLICATION		
VSYS		
USER		
SERIAL_ID_PAT		

Default version of pa_log_rules.txt

```
# Explanation:
# This file enables the configuration of multiple key sets for each line in
the syslog file.
# Each syslog line is checked by one key set. If the mandatory fields
(time/src/dst/dst port/guid/device id) don’t match, the line is checked by
the next key set.
# Each key set should be delimited by "__-__end of set__-__"
# If a property that appeared in the first key set does not appear in a
subsequent key set, the value of that property is taken from the first key
set.

POLICY_ID_PAT__-__cs1=
SERVICE_PAT__-__service=
ICMP_TYPE_PAT__-__icmp type=
PROTOCOL_PAT__-__proto=
SOURCE_PAT__-__src=|srcip=
DESTINATION_PAT__-__dst=|dstip=
SOURCE_PORT_PAT__-__spt=
DESTINATION_PORT_PAT__-__dpt=
LOG_ID_PAT__-__log_id=|logid=
VD_PAT__-__vd=
APPLICATION__-__app=
VSYS__-__cs3=
USER__-__suser=
FULL_DATE__-__start=
DATE_FORMAT__-__MMM d yyyy HH:mm:ss
SERIAL_ID_PAT__-__deviceExternalId=
HINT__-__TRAFFIC&&CEF:

__-__end of set__-__

POLICY_ID_PAT__-__policy_id=
SERIAL_ID_PAT__-__shost=
DATE_FORMAT__-__yyyy/MM/dd HH:mm:ss
VSYS__-__
HINT__-__traffic&&CEF:

__-__end of set__-__
```

```
POLICY_ID_PAT__-__ad.policy-name=
FULL_DATE__-__art=
SERIAL_ID_PAT__-__ahost=
VSYS__-__
HINT__-__CEF:
```

Syslog traffic events collection tasks

Traffic Events – Syslog Import tasks retrieve syslog-formatted activity logs and add the relevant data from the logs to the current model. The following device types are supported:

- Check Point FireWall-1
- Cisco Firepower
- Cisco IOS
- Cisco PIX/ASA/FWSM
- Forcepoint (StoneGate)
- Fortinet FortiGate
- Juniper Networks Junos
- Juniper Networks NetScreen
- McAfee Enterprise (Sidewinder)
- Palo Alto Networks

For Palo Alto Network firewalls, Check Point firewalls, Juniper Networks Junos firewalls, Juniper Networks NetScreen, and Fortinet FortiGate firewalls, both standard syslog and ArcSight CEF-formatted syslog (see page 157) are supported.

Note: CEF syslog is not yet supported when using Check Point Log Exporter.

Note: Log data can be added to the model only for devices that exist in the model and have the same rules and objects as those used in the log; if the policy has changed, update the device in the model before running the **Traffic Events – Syslog Import** task.

Note: For logs with a great deal of information, a **Traffic Events – Syslog Import** task can take time to import all the data.

Filtering records from the logs

- For standard syslog, the task checks each log record for the following strings to decide whether to parse the record and add its data to the model:
  - PIX/ASA/FWSM: `10610`
  - Junos:
    - `RT_FLOW_SESSION_CLOSE`
    - `RT_FLOW_SESSION_CREATE`

    Note: The log must be in structured-data format (see Configuring Junos firewalls for data collection (on page 124))
  - NetScreen: `00257`

- FortiGate: `traffic`
- Palo Alto Networks: `TRAFFIC`
- Check Point: `Firewall` or `cma`
- Forcepoint (StoneGate): `Connection_Allowed`
- McAfee Enterprise: `t_nettraffic`

For examples of syslog records that Skybox uses for rule usage analysis, see Examples of syslog records for rule usage analysis (on page 167).

› For CEF formatted syslog, use the `HINT` key in `pa_log_rules.txt` to filter the records. See Using CEF-formatted syslog (see page 157) for information about this file.

Task properties

The properties that control **Traffic Events – Syslog Import** tasks are described in the following table.

Property	Description
Basic tab	
Files Directory Path	The full path to the directory containing the syslog files to collect.
Modules	A list of the modules (devices) for which to collect logs. **Note**: All modules must be of the same type.
Collection Period	The time frame for which to collect activity logs. • **Custom**: Select **Specific** or **Relative** start and end times. If (in the **Advanced** tab) **Date Format** = **Automatic**, this value must be between 1 and 30 days.
Filter by Type	This field is disabled if you select **Collect CEF logs only** in the **Advanced** tab. (CEF logs can contain records from multiple devices of different types.) A list of the device types for which to collect logs.
Actual Rule Usage tab	
Trace Scope	A list of firewalls and firewall folders for which to collect actual usage (trace) information.
Trace Criteria for Actual Rule Usage	Actual usage information is collected when any of the criteria are met.
Advanced tab	
Re-collect Time Frames Already in Database	Force (re)collection of log data that is already in the Skybox database. **Note**: This option is useful if there is a gap in collected data. The Skybox database holds the date of the most recently collected log and, unless this option is selected, the task considers anything earlier as already collected.
Date Format	This field is disabled if you select **Collect CEF logs only**. (Records from different devices can have different date formats. Permitted date formats are listed in `pa_log_rules.txt`. See Using CEF formatted syslog (see

Property	Description
	page 157) for information about this file.) The format of the message date in the `start_time` field of the syslog message. If the required format is not listed, add a row with the format to the file `<Skybox_Home>\server\conf\collector_commands\date_patterns.txt`. If **Date Format** = **Automatic**: • The task attempts to identify the format of the date for each of the syslog files under the input directory • **Collection Period** (in the **Basic** tab) must have a value between 1 and 30 days
Date Position in Log Record (Cisco/Junos)	This field is disabled if **Date Format** = **Automatic**. (Cisco and Junos devices only) The position of the message date in the syslog message header. (Position is defined as the nth word from the beginning of the line—the 1st word is **1** (not **0**) and words are separated by any whitespace.)
Device ID Position in Log Record (Cisco/Junos)	This field is disabled if **Date Format** = **Automatic**. (Cisco and Junos devices only) The position of the device ID in the syslog message header. (Position is defined as the nth word from the beginning of the line—the 1st word is **1** (not **0**) and words are separated by any whitespace.)
Limit Log lines	The number of lines to parse in each log file.
Collect CEF logs only	(Palo Alto, Check Point, Junos, NetScreen, and FortiGate firewalls only) Specifies whether to limit collection to CEF syslog format logs only. Select this option if you are using CEF logs only; the task runs significantly faster. If selected, standard syslog format logs are marked as *invalid*. **Note**: Skybox does not yet support CEF format when using the Check Point Log Exporter.

CHECK POINT FIREWALL-1 ACTIVITY LOG DATA (LEA COLLECTION)

Note: We recommend that you use Check Point Log Exporter whenever possible and import the log using a **Traffic Events – Syslog Import** task (see Syslog traffic events collection tasks (on page 161)).

You can add or update firewall activity log data from Check Point FireWall-1 NG and NGX firewalls to the current model using an online collection task:

- Configure the device holding the firewall activity logs (see page 164) to permit access from a Skybox Collector and create a collection task (see page 164) to collect the logs and add their data to the model.

Note: Add the configuration data of each firewall to the current model (by running a Check Point FireWall-1 CPMI collection task (see page 74)) before running a **Firewalls – Check Point FireWall-1 LEA Collection** task for the 1st time.

Skybox uses activity log data for rule usage analysis, which is described in the Skybox Firewall Assurance User Guide.

Note: Alternatively, you can collect and add log data for rule usage analysis using a Traffic Events – Syslog Import task (see page 154). (If you use this task, the Skybox Collector does not need access to the device; you configure the device to forward the activity data to a syslog server.)

Configuring devices for FireWall-1 log collection

The logs generated by a Check Point FireWall-1 firewall can be either on the Check Point FireWall-1 Management Server that manages the firewall or on a dedicated log server.

Note: We recommend that you use Check Point Log Exporter whenever possible (see Configuring Check Point firewalls to send activity logs to a syslog server (on page 156)). If you do so, this procedure is unnecessary.

To enable Skybox to collect FireWall-1 logs (if you did not do so when configuring the OPSEC application to permit CPMI collection):

1. Get the IP address of the device where the logs are stored (see page 74).
2. Configure the OPSEC application to permit LEA collection (see page 71).
3. (If the logs are on a Check Point FireWall-1 Management Server) Configure the Management Server to permit collection using the OPSEC protocol (see page 73).
4. (If the logs are on a log server) Install the OPSEC application database on the log server (see page 74).

Check Point FireWall-1 LEA collection tasks

Note: We recommend that you use Check Point Log Exporter whenever possible and import the log using a **Traffic Events – Syslog Import** task (see Syslog traffic events collection tasks (on page 161)).

Firewalls – Check Point FireWall-1 LEA Collection tasks retrieve firewall activity logs from Check Point FireWall-1 Management Servers (or from dedicated log servers) and add the log data to the current model. Create a separate LEA collection task for each FireWall-1 Management Server. For VSX (virtual systems) firewalls, configuration data for all the virtual firewalls is retrieved.

Note: Skybox supports log hit count collection for access rules with Log as their Track Option.

You can create a **Firewalls – Check Point FireWall-1 LEA Collection** task in 2 ways:

- Right-click a **Firewalls – Check Point FireWall-1 CPMI Collection** task and select **Create Task for Activity Log Collection**.

A **Firewalls – Check Point FireWall-1 LEA Collection** task is created, with relevant property values copied from the Check Point FireWall-1 CPMI collection task.

Note: If you create the **Firewalls – Check Point FireWall-1 LEA Collection** task from a Provider-1 CPMI collection task, a warning message is displayed and **SIC Name** is not copied.

- Create a task and set **Task Type** to **Firewalls – Check Point FireWall-1 LEA Collection**.

You can add log data to the model only for firewalls that exist in the model and have the same rules and objects as those used in the log; if the policy changes, update the firewall in the model before running the LEA collection task. (For FireWall-1 NG firewalls, update the firewall in the model every time that the policy in the firewall changes so that rule usage analysis can work as accurately as possible; this is not necessary for FireWall-1 NGX firewalls.)

Note: For large log files, a **Firewalls – Check Point FireWall-1 LEA Collection** task can take several hours. You can view progress messages in the **Messages** tab of the task; a message is added, by default, every 60 seconds. You can change the frequency that messages are added by changing the value of `lea_progress_interval` in `<Skybox_Home>\server\conf\sb_server.properties`

To minimize collection time, if data for part of the **Collection Period** was collected previously, that data is not (by default) collected again.

Task properties

The properties that control **Firewalls – Check Point FireWall-1 LEA Collection** tasks are described in the following table.

Property	**Description**
Basic tab	
Management Server	The IP address of the FireWall-1 Management Server. **Note**: Provide the IP address, not the name of the server. **Note**: Authentication is against the FireWall-1 Management Server, even if it is managed by a Provider-1 Domain Server (CMA).
Initialize	
Certificate Issue Date	• If this field is empty, the connection to the Management Server is not initialized • <Timestamp>: The timestamp of the authentication certificate To retrieve an authentication certificate, click **Initialize Certificate** to open the Initialize Certificate dialog box (see page 77).
Authentication	If a Permissions Profile exists, the task uses the profile; any values entered in this section are ignored.
Username	The user name of the administrator to access the Management Server.
Password	The administrator password.

Property	Description
Collection	
Collect From Log Server	Specifies whether the activity logs are collected from a log server. If cleared, the activity logs are collected from the Management Server.
Log Server	This field is enabled only if you select **Collect From Log Server**. The IP address of the log server. If there is a secondary server, add the IP address of the secondary server (separated by a comma or space); if the primary server is down or inaccessible, the task collects the logs from the secondary server. To collect logs from the log server, install the OPSEC application database on the log server (see Configuring devices for FireWall-1 log collection (on page 164)).
Modules	A list of the modules (firewalls and firewall folders) for which to collect logs.
Collection Period	The time frame for which to collect activity logs. • **Custom**: Select **Specific** or **Relative** start and end times. **Note**: The time frame must not be more than 100 days.
SIC Name	The DN of the location of the activity logs. Skybox displays the value from the authentication certificate that it retrieves when you initialize the connection. Do not change this value. If you specified a secondary server in **Log Server**, the DN of the secondary server is also displayed.
Actual Rule Usage tab	
Trace Scope	The firewalls and firewall folders for which to collect actual usage (trace) information.
Trace Criteria for Actual Rule Usage	Actual usage information is collected when any of the criteria are met.
Advanced tab	
OPSEC Application	The name given to the OPSEC application when it was configured for Skybox (see Configuring devices for FireWall-1 log collection (on page 164)).
Clear Mode	Specifies whether the Management Server or log server works in clear mode. Clear this option if the Management Server or log server works in encrypted mode rather than clear mode.
Port	The port to use on the Management Server or log server. **Note**: If the Management Server is working in encrypted mode and uses a non-default port (a port other than 18184), modify `fwopsec.conf` and `cpmad_opsec.conf`.
Excluded Log Files	A comma-separated list of log files that the task does not collect. By default, `fw.log` is displayed. We recommend that you

Property	Description
	do *not* delete this (that is, do *not* collect fw.log).
Re-collect Time Frames Already in Database	Force (re)collection of log data that is already in the Skybox database. **Note**: This option is useful if there is a gap in collected data. The Skybox database holds the date of the most recently collected log and, unless this option is selected, the task considers anything earlier as already collected.
Device Time Zone offset	The 3-letter code for the time zone to use for timestamps in the log. If this field is empty, Skybox uses the local time zone.
Limit Log Lines	Specifies whether to stop the task after collecting the specified number of log lines. All retrieved logs are saved.

EXAMPLES OF SYSLOG RECORDS FOR RULE USAGE ANALYSIS

Examples of syslog records for rule usage analysis

- Check Point FireWall-1

```
Dec 23 12:44:25 1-1-1-1 Firewall: 31Oct2012  0:01:55 accept
1.1.1.1  >eth1 rule: 1; rule_uid: {E1A963D8-20D1-42F4-BFD5-
AF010A5B25B5}; rule_name: 2; src: 192.168.1.1; dst: 192.168.2.2;
proto: tcp; product: VPN-1 & FireWall-1; service: 7800; s_port:
20658; product_family: Network;
```

- Check Point Domain Server (Provider-1)

```
2013-01-06 16:07:55        Local4.Info         10.1.1.1
cma1: 16Sep2012 15:53:54 accept 10.2.2.2  >eth0 rule: 1; rule_uid:
{42B0B1D4-73B6-4FEC-97D0-9BBE0AF18742}; service_id: ssh_version_2;
src: 192.168.1.1; dst: 10.2.2.2; proto: tcp; product: VPN-1 &
FireWall-1; service: 22; s_port: 53753; product_family: Network;
```

- Cisco PIX/ASA/FWSM

This example is for ASA; PIX and FWSM are similar.

```
Feb 17 03:13:29 firewallASA1 %ASA-6-106100: 10.0.1.1 access-list
outbound denied tcp inside/192.168.1.1(59004) ->
Outside/10.32.1.1(80) hit-cnt 2 300-second interval [0x5abd3815,
0x0]
```

- Juniper Networks Junos

```
Oct  1 03:02:42 10.1.1.1 1 2011-10-01T00:51:59.582 abcdefghijklm11
RT_FLOW - RT_FLOW_SESSION_CLOSE [junos@1.1.1.1.1.1 reason="unset"
source-address="10.2.2.2" source-port="57623" destination-
address="10.3.3.3" destination-port="53" service-name="junos-dns-
udp" nat-source-address="1.1.1.1" nat-source-port="57623" nat-
destination-address="1.1.1.2" nat-destination-port="53" src-nat-
rule-name="None" dst-nat-rule-name="None" protocol-id="17" policy-
name="9" source-zone-name="SourceZone" destination-zone-
name="DestZone" session-id-32="100110617" packets-from-client="1"
bytes-from-client="72" packets-from-server="1" bytes-from-
server="147" elapsed-time="60"]
```

- Juniper Networks NetScreen

```
2014-09-19 10:38:24        Local0.Notice     192.168.30.2
Vlab-ns: NetScreen device_id=Vlab-ns  [Root]system-notification-
00257(traffic): start_time=\"2014-09-19 10:38:24\" duration=1
policy_id=8 service=SSH proto=6 src zone=Trust dst zone=Untrust
action=Permit sent=78 rcvd=64 src=192.168.32.2 dst=192.168.80.167
src_port=1030 dst_port=22 src-xlated ip=192.168.30.2
port=1061<000>
```

- Fortinet FortiGate

```
itime=1265626137 cluster_id=123456789ABCDE00_CID date=2010-02-08
time=09:26:44 devname=ABCDEFGH01 device_id=123456789ABCDE00
log_id=0021010001 type=traffic subtype=allowed pri=notice vd=root
SN=741011340 duration=135 user=N/A group=N/A policyid=53 proto=6
service=80/tcp app_type=N/A status=accept src=1.1.1.1
srcname=1.1.1.1 dst=2.2.2.2 dstname=2.2.2.2 src_int=port2
dst_int=port3 sent=1690 rcvd=580 sent_pkt=6 rcvd_pkt=5
src_port=60309 dst_port=80 vpn=N/A tran_ip=0.0.0.0 tran_port=0
dir_disp=org tran_disp=noop
```

- Palo Alto Networks

```
Apr  7 16:23:55 pa-2020 CEF:0|Palo Alto Networks|PAN-
OS|4.1.0|end|TRAFFIC|1|rt=Apr 07 2014 13:23:55 GMT
deviceExternalId=00011111111 src=192.168.1.1 dst=172.1.1.1
sourceTranslatedAddress=0.0.0.0
destinationTranslatedAddress=0.0.0.0 cs1Label=Rule cs1=cleanup
suser= duser= app=my ICMP cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=trust cs5Label=Destination Zone cs5=trust
deviceInboundInterface=ethernet1/1
deviceOutboundInterface=ethernet1/1 cs6Label=LogProfile
cs6=log_profile cn1Label=SessionID cn1=63687 cnt=3 spt=0 dpt=0
sourceTranslatedPort=0 destinationTranslatedPort=0
flexString1Label=Flags flexString1=0x0 proto=icmp act=allow
flexNumber1Label=Total bytes flexNumber1=354 in=180 out=174
cn2Label=Packets cn2=6 PanOSPacketsReceived=3 PanOSPacketsSent=3
start=Apr 07 2014 13:23:49 GMT cn3Label=Elapsed time in seconds
cn3=0 cs2Label=URL Category cs2=any externalId=645104
```

- Forcepoint (StoneGate)

```
Oct 13 12:27:09 192.168.88.27 kernel:
CEF:0|Stonesoft|Firewall|5.5.6|70018|Connection_Allowed|0|spt=4993
2 deviceExternalId=Fw node 1 dst=1.1.1.1 app=Remote Desktop rt=Oct
13 2014 12:27:04 deviceFacility=Packet filter act=Allow proto=6
dpt=3389 src=2.2.2.2 dvc=3.3.3.3 dvchost=4.4.4.4 cs1Label=RuleId
cs1=13339.3
```

- McAfee Enterprise

```
Jul 17 07:03:54 10.8.179.19 auditd: date="2014-07-17 12:03:54
+0000",fac=f_kernel_ipfilter,area=a_general_area,type=t_nettraffic
,pri=p_major,hostname=ho-ban.dummy.com,event="session
end",application=tcp-
1650,netsessid=2d78853c66a24,src_geo=US,srcip=140.31.22.101,srcpor
t=54614,srczone=dmz,protocol=6,dstip=192.168.100.10,dstport=1550,d
stzone=external,bytes_written_to_client=1265,bytes_written_to_serv
er=1670155,rule_name="sky_access",cache_hit=0,start_time="2014-07-
17 12:03:48 +0000"
```

Chapter 6

Firewall change tracking tasks

This chapter describes how to add firewall log data for change tracking to the current model.

In this chapter

IMPORTING SYSLOG CHANGE TRACKING EVENTS

Skybox can use online collection tasks to extract data from syslog events, and add the changes of the access rules and objects to the current model for the following firewalls and firewall management systems:

- Cisco PIX/ASA/FWSM
- Fortinet FortiGate
- Fortinet FortiManager
- Juniper Networks Junos
- Juniper Networks NetScreen
- Palo Alto Networks
- Palo Alto Panorama

Note that:

- Before importing syslog change tracking events task for the 1st time, run a task to add the configuration data of the firewall to the current model.
- Skybox Appliance includes a built-in syslog server, which is activated by default. If you are working with a Skybox Collector on a non-Appliance machine, you must install a 3rd-party syslog server on the Collector machine. Make sure to use a server that can output events to syslog text files so that Skybox can process them.
- You must configure the firewalls to send syslog messages (see page 171) to the Skybox Collector or any other syslog server and create a collection task (see page 171) to read the syslog file, collect the events, and add their data to the model.

The imported data is used by Analysis – Change Tracking (see page 308) tasks.

Configuring devices to forward syslog messages for change tracking

To work with syslog change events, you must forward the change events from the firewall or syslog server to the Skybox Appliance or Collector machine for parsing by the task. Because most syslog events are not related to firewall changes, we recommend that you forward only the change events and not the other syslog events.

Change-related syslog messages

- Juniper NetScreen: Messages of types `00001`, `00018`, and `00012`

  For information about configuring the firewall to send syslog messages, see Configuring NetScreen firewalls for data collection (on page 129)

- Juniper Junos: All `CFG_AUDIT` messages

  For information about configuring the firewall to send syslog messages, see https://kb.juniper.net/InfoCenter/index?page=content&id=KB10132

- Fortinet FortiGate: All messages of subtype `config`

  For information about configuring the firewall to send syslog messages, see Configuring FortiGate firewalls for data collection (on page 112)

- Cisco PIX/ASA/FWSM: All `[PIX | ASA | FWSM]-5-111008` messages
- Palo Alto Networks: All messages of type `CONFIG`

For examples of syslog records that Skybox uses for change tracking analysis, see Examples of syslog records for change tracking (on page 177).

Syslog change events collection tasks

Change Tracking Events – Syslog Import tasks retrieve syslog change events from firewalls and firewall management systems and add relevant data from the events to the current model. The following device types are supported:

- Cisco PIX/ASA/FWSM
- Fortinet FortiGate
- Fortinet FortiManager
- Juniper Networks Junos
- Juniper Networks NetScreen
- Palo Alto Networks
- Palo Alto Panorama

Note: Log data can be added to the model only for firewalls that exist in the model and have the same rules and objects as those used in the log; if the policy has changed, update the firewall in the model before running the **Change Tracking Events – Syslog Import** task.

Task properties

The properties that control **Change Tracking Events – Syslog Import** tasks are described in the following table.

Property	Description
Basic tab	
Files Directory Path	The full path to the directory containing the syslog files to collect. **Note**: The task also collects any syslog files that are contained in archive (ZIP) files in this directory.
Modules	A list of the modules (firewalls) for which to collect change events.
Filter by Type	A list of the firewall types for which to collect logs.
Advanced tab	
Date Format	The format of the date and time in the syslog records. • **Automatic**: Skybox determines the date format from the 1st (non-ambiguous) date in the syslog records. **Note**: If syslog import is done on a folder with different time formats files, only the 1st time format is considered valid; all other formats will fail. If the required format is not listed, add a row with the format to the file `<Skybox_Home>\server\conf\collector_commands\date_patterns.txt` • Junos and PIX/ASA/FWSM: The format of the syslog header timestamp • NetScreen, FortiGate, and Palo Alto: The formats of the date and time fields, *not* the header timestamp For example, if a FortiGate syslog record starts `Mar 13 13:44:47 134.67.26.8 date=2019-03-13 time=12:37:45 devname=...`, select **2001-03-14 00:00:00** (and not **Mar 14 00:00:00**)

How syslog change events are parsed

Change Tracking Events – Syslog Import tasks use `policy_syslog.txt` to create syslog-based change records from syslog entries that contain change events. The file (in the `<Skybox_Home>\collector\conf\collector_commands` directory) includes a list of regular expressions that handle different types of change.

The task uses the file to:

1. Determine whether a syslog event is a change event
2. Pull the following information out of each relevant syslog entry and use it to create a change record:
   - The type of entity that was changed (access rule or object)
   - The device ID

     Note: If the device ID includes a virtual device, separate the device ID and the virtual device ID with a colon. For example, `A-MPC-DB-F01:MPC-DB`

   - The rule ID (for changes to access rules) or object name
   - The administrator who made the change

- The timestamp for the change
- The type of change (new, modified, or deleted)

The file includes regular expressions that handle events from the following firewalls and firewall management systems:

- Cisco PIX/ASA/FWSM
- Fortinet FortiGate
- Fortinet FortiManager
- Juniper Networks Junos
- Juniper Networks NetScreen
- Palo Alto Networks
- Palo Alto Panorama

To work with events from other devices, contact Skybox Support.

policy_syslog.txt

`policy_syslog.txt` is in the `<Skybox_Home>\collector\conf\collector_commands` directory.

What the file contains

- Default values for the following change properties:
  - Device ID
  - GUID (for access rules)
  - Name (for objects)
  - Change initiator (that is, the person who made the change)
  - Change time

  The default values specify the position of the group defining the change property in the regular expressions. For example, `DEVICE_ID__-__1` means that the 1st group in all patterns is the device ID.

- Rules containing regular expressions that are used to check and parse syslog events. Each regular expression for NetScreen contains the number of groups for which there are defaults, and the order of each group determines the default it matches. For example, the 3rd group in the regular expression matches the default whose value is **3** (that is, changed by).
- Additional rules that add properties to the change records defined by the regular expressions.

Each rule in the file is a key/value set—the key is the name of the rule, the name of the change property (device ID, object name, change initiator, or timestamp), or the change status, followed by `__-__`, followed by the value (the rule, the change property, the change status, the change initiator, or the change timestamp).

The regular expression language used is the Java standard, as explained in http://java.sun.com/javase/6/docs/api/java/util/regex/Pattern.html

How it works

When you run a **Change Tracking Events – Syslog Import** task, Skybox reads each syslog event:

1. The task checks the event against each regular expression in the file until it finds a match.

   For example, the following line:

```
Feb 7 12:06:07 lab-ns lab-ns: NetScreen device_id=lab-ns [Root]system-
notification-00018: Policy (300, Untrust->Trust, Any->my,DHCP-Relay, Deny)
was deleted by admin_300 via web from host 192.168.80.87 to
172.20.0.180:80. (2013-02-07 13:24:37)
```

   matches the following regular expression:

```
NETSCREEN_CHANGE_LOG_ACL_DELETE_PAT__-__.*device_id=([^\s]+).*Policy
\(([^\,]+).*was deleted by ([^\s]+).*\(([^\\)]+).*
```

2. If the task does not find a match, it goes on to the next syslog event.
3. If the task finds a match, it creates a syslog-based change record using the groups in the regular expression to find the values for each default. For example, for NetScreen rules, the value found by the 1st group becomes the device ID in the change record and so on. The status of the change is specified by the _STATE__-__<status value> rule (<status value> is `NEW`, `MODIFIED`, or `DELETED`). Whether the change relates to an access rule or an object (and hence the information that is contained in the 2nd grouping) is defined by the name of the rule (which must contain either the string `ACL` or the string `OBJECT`).
4. The syslog-based change record is added to the model.

Modifying policy_syslog.txt

To use `policy_syslog.txt` to work with a firewall type that is not supported, you must customize the file by adding definitions. In some cases—for example, if you customized the message patterns from supported firewall types—the existing definitions might also need updating.

Important: Consult Skybox Support before modifying this file.

If you do work with this file:

- The prefix of a rule represents the device type.
- The 1st part of a rule represents its name; the 2nd part represents the value. The string "__-__" must separate the 2 parts.
- Each pattern requires a separate parsing rule (regular expression).
- The name of each parsing rule for access rule changes must contain the string "_ACL_"; the name of each parsing rule for objects must contain the string "_OBJECT_". Two rules cannot have the same name.
- The regular expression must contain a group for each default specified at the top of the file. These define each change property in the change record. If the order of the defaults is different from that specified at the top of the file, there must be another rule for each default whose order is different.
- For each parsing rule, there must be another rule that defines the status of the change. This rule must have the same name as the parsing rule, with the

string <state> appended at the end. For example, `<DEVICE TYPE>_CHANGE_LOG_ACL_ADD_PAT_STATE__-__NEW`

To customize policy_syslog.txt for an additional firewall type

1 Look at syslog change events from the firewall to determine their format and what the pattern differences are between this output and the default output expected by the file.

2 Modify `<Skybox_Home>\collector\conf\collector_commands\policy_syslog.txt` on the Skybox Collector machine by adding new rules based on the patterns in syslog for the new firewall type:

   a. For each type of syslog event in the new device type, copy the parallel NetScreen rule and change the device prefix and pattern.

   b. If the order of the defaults for the new device differs from that specified at the top of the file, add another rule for each default whose order is different. For example, if in the new type of firewall, the timestamp comes before the change initiator, you need a separate rule for each of them, for example:

      – `<DEVICE TYPE>_CHANGE_LOG_ACL_ADD_PAT_CHANGE_TIME__-__3`

      – `<DEVICE TYPE>_CHANGE_LOG_ACL_ADD_PAT_CHANGED_BY__-__4`

      Note: This step must be done per parsing rule.

   c. Make sure that each parsing rule for the new device has a matching state rule with a value of `NEW`, `MODIFIED`, or `DELETED`.

      For example, `<DEVICE TYPE>_CHANGE_LOG_ACL_ADD_PAT_STATE__-__NEW`

CHECK POINT FIREWALL-1 CHANGE EVENTS (AUDIT LOG DATA)

You can add or update firewall audit log data from Check Point FireWall-1 NG and NGX firewalls to the current model using an online collection task:

- Configure the device holding the firewall activity logs (see page 164) to permit access from a Skybox Collector and create a collection task (see page 175) to collect the logs and add their data to the model.

Note: Add the configuration data of each firewall to the current model (by running a Check Point FireWall-1 CPMI collection task (see page 74) or a Check Point R80 Security Management collection task (see page 96), as relevant) before running a **Change Tracking Events – Check Point Audit Log Collection** task for the 1st time.

Skybox uses the imported data for Analysis – Change Tracking tasks (see page 308).

Check Point FireWall-1 change events collection tasks

Change Tracking Events – Check Point Audit Log Collection tasks retrieve firewall audit logs from Check Point FireWall-1 Management Servers (or from dedicated log servers) and add the log data to the current model.

You can add log data to the model only for firewalls that exist in the model and have the same rules and objects as those used in the log; if the policy changes, update the firewall in the model before running the change events collection task.

Task properties

The properties that control **Change Tracking Events – Check Point Audit Log Collection** tasks are described in the following table.

Property	Description
Basic tab	
Management Server	The IP address of the FireWall-1 Management Server. **Note**: Provide the IP address, not the name of the server. **Note**: Authentication is against the FireWall-1 Management Server, even if it is managed by a Provider-1 Domain Server (CMA).
Initialize	
Certificate Issue Date	• If this field is empty, the connection to the Management Server is not initialized • <Timestamp>: The timestamp of the authentication certificate To retrieve an authentication certificate, click **Initialize Certificate** to open the Initialize Certificate dialog box (see page 77).
Authentication	If a Permissions Profile exists, the task uses the profile; any values entered in this section are ignored.
Username	The user name of the administrator to access the Management Server.
Password	The administrator password.
Collection	
Collect from Log Server	Specifies whether the audit logs are collected from a log server. If cleared, the audit logs are collected from the Management Server.
Log Server	This field is enabled only if you select **Collect from Log Server**. The IP address of the log server. To collect logs from the log server, install the OPSEC application database on the log server (see Configuring devices for FireWall-1 log collection (on page 164)).
SIC Name	The DN of the location of the audit logs (the DN depends on the value of **Collect from Log Server**). Skybox displays the value from the authentication certificate that it retrieves when you initialize the connection. Do not change this value.
Modules	A list of the modules (firewalls and firewall folders) for which to collect logs.

Property	Description
Advanced tab	
OPSEC Application	The name given to the OPSEC application when it was configured for Skybox (see Configuring devices for FireWall-1 log collection (on page 164)).
Clear Mode	Specifies whether the Management Server or log server works in clear mode. Clear this option if the Management Server or log server works in encrypted mode rather than clear mode.
Port	The port to use on the Management Server or log server. **Note**: If the Management Server is working in encrypted mode and uses a non-default port (a port other than 18184), modify fwopsec.conf and cpmad_opsec.conf.
Excluded Log Files	A comma-separated list of log files that the task does not collect.

EXAMPLES OF SYSLOG RECORDS FOR CHANGE TRACKING

Examples of syslog records with change events

- Cisco PIX/ASA/FWSM

  This example is for ASA; PIX and FWSM are similar.

  ```
  Dec  3 14:20:22 172.1.1.1 %ASA-5-111008: User 'admin1' executed
  the 'access-list name1 extended permit tcp any any' command.
  ```

- Juniper Networks Junos

  ```
  Apr 7 18:00:00 srxskybox-1 mgd[71250]: UI_CFG_AUDIT_SET: User
  'admin' set: [juniper-config security zones security-zone trust
  address-book address addr7] <unconfigured> -> "1.1.1.7"
  ```

- Palo Alto Networks

  ```
  May  6 00:03:12 pan-1:vsys1
  23:03:11,002201000500,CONFIG,0,0,2014/05/06
  23:03:11,172.30.128.221,,edit,john.doe,Web,Succeeded, vsys  vsys1
  address  PAN-01,2236,0x0
  ```

- Juniper Networks NetScreen

  ```
  Jan 13 13:56:44 lab-ns lab-ns: NetScreen device_id=lab-ns
  [Root]system-notification-00018: Policy (403, Trust->Untrust,
  1.1.1.1/24->2.2.2.2/24,ANY,  Permit) was added by admin via web
  from host 192.168.1.1 to 172.1.1.1:80. (2013-01-13 15:14:50)
  ```

- Fortinet FortiGate

  ```
  Apr  3 14:10:19 192.168.1.1 date=2013-04-10 time=14:46:00
  devname=FGT600-new-lab device_id=FGT6001111111111
  log_id=0109044547 type=event subtype=config pri=information
  vd="vdom1" user="admin" ui="GUI(192.168.1.2)" action=edit
  cfg_tid=1638404 cfg_path="firewall.policy" cfg_obj="18"
  cfg_attr="service[DHCP->AOL]" msg="Edit firewall.policy 18"
  ```

Chapter 7

Router, switch, and wireless controller tasks

This chapter describes how to add router, switch, and wireless controller configuration data to the current model.

In this chapter

ALCATEL-LUCENT ROUTER

You can add or update configuration data from Alcatel-Lucent routers to the current model using an online collection task:

- Configure a router (see page 179) to permit access from a Skybox Collector and create a collection task (see page 179) to collect the router configurations and add the configuration data to the model.

  The collection task can collect data from multiple routers.

Configuring Alcatel-Lucent routers for data collection

To configure an Alcatel-Lucent router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Alcatel-Lucent Collection tasks use the SSH protocol to connect to Alcatel-Lucent routers.

Commands sent to device

Routers – Alcatel-Lucent Collection tasks send the following commands to Alcatel-Lucent routers:

- `write terminal`
- `show system`
- `show ip routes`
- `show ip route`

Alcatel-Lucent collection tasks

Routers – Alcatel-Lucent Collection tasks retrieve configuration data from Alcatel-Lucent routers and add this data to the current model.

Task properties

The properties that control **Routers – Alcatel-Lucent Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Alcatel-Lucent routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Username	The user name to access the routers.
Password	The user password.
Advanced tab	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different

Property	Description
	locations can have the same IP address.

ARISTA NETWORKS ROUTER

You can add or update configuration data from Arista Networks routers to the current model:

- Using an online collection task:
  - Configure a router (see page 180) to permit access from a Skybox Collector and create a collection task (see page 181) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.
- Using an offline file import task:
  - Generate and retrieve router configuration files and import their data into the model (see page 182).

    The file import task can import the data of multiple routers.

Configuring Arista Networks routers for data collection

To configure an Arista Networks router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Arista Collection tasks use the SSH protocol to connect to Arista Networks routers.

Commands sent to device

Routers – Arista Collection tasks send the following commands to Arista Networks routers:

- `enable`
- `show run`
- `show ip route vrf all`

  Old versions of the Arista operating system (EOS) do not support this command; if the router returns `% IP Routing table for VRF all does not exist`, the task also sends the following commands:
  - `show vrf`
  - `show ip route vrf <VRF name>` (for each VRF returned by `show vrf`)
  - `sh ip route vrf default`
- `no page`
- `terminal length 0`

Arista Networks collection tasks

Routers – Arista Collection tasks retrieve configuration data from Arista Networks routers and add this data to the current model.

Task properties

The properties that control **Routers – Arista Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Arista Networks routers, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 22. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the routers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Enable password	The password for enable command privileges on the routers.
Advanced tab	
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system Temp directory.
Get password timeout	The time to wait for a response to the login command before the task skips the device.
Port (v2 use only)	The port on which the firewalls listen.
Type (v2 use only)	The protocol to use to connect to the device.
Arista Collector Executor	The version of the collector to use. (Do not change the default unless told to do so by

Property	Description
	Skybox Professional Services.)
Arista Parser Executor	The version of the parser to use. (Do not change the default unless told to do so by Skybox Professional Services.)
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Importing Arista Networks configuration data

You can use an **Import – Directory** task to import Arista Networks configuration data.

The following file is required to import an Arista Networks router configuration:

- `run.txt`:

  1. The Arista configuration file

     This file is the output of the Arista show `running-config` command.

  2. (Optional) Append a dump of the Arista routing table (the output of the Arista show `ip route` command) to the configuration file

You can import the configurations of multiple routers.

ARUBA NETWORKS WIRELESS CONTROLLER

You can add or update configuration data from Aruba Networks wireless controllers to the current model using an online collection task:

- Configure a wireless controller (see page 182) to permit access from a Skybox Collector and create a collection task (see page 183) to collect the wireless controller configurations and add the configuration data to the model.

  The collection task can collect data from multiple wireless controllers.

Configuring Aruba Networks wireless controllers for data collection

To configure an Aruba Networks wireless controller for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Wireless Controller – Aruba Collection tasks use the SSH protocol to connect to Aruba Networks wireless controllers.

Commands sent to device

Wireless Controller – Aruba Collection tasks send the following commands to Aruba Networks wireless controllers:

- `enable`

- `show running-config`
- `show ip route`
- `no page`
- `terminal length 0`

Aruba Networks collection tasks

Wireless Controller – Aruba Collection tasks retrieve configuration data from Aruba Networks wireless controllers add this data to the current model.

Task properties

The properties that control **Wireless Controller – Aruba Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Aruba Networks wireless controllers. **Note**: A task can collect the configurations of multiple wireless controllers only if the same authentication is used for all the wireless controllers.
Username	The user name to access the wireless controllers.
Password	The user password.
Enable Password	The password for enable command privileges on the wireless controllers.
Advanced tab	
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.) The location of the debug log file. If this field is empty, the task does not save debug messages.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the wireless controllers. **Note**: Use this property if different locations use the same set of IP addresses, so that wireless controllers at different locations can have the same IP address.

AVAYA ROUTER

You can add or update configuration data from Avaya routers to the current model using an online collection task:

- Configure a router (see page 184) to permit access from a Skybox Collector and create a collection task (see page 184) to collect the router configurations and add the configuration data to the model.

  The collection task can collect data from multiple routers.

Configuring Avaya routers for data collection

To configure an Avaya router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Avaya Collection tasks use the SSH protocol to connect to Avaya routers.

Commands sent to device

Routers – Avaya Collection tasks send the following commands to Avaya routers:

- `enable`
- `terminal more disable`

  If this command fails, the task sends the command `terminal length 0`
- `show running-config`
- `show ip route`
- `sh ip route vrfids 1-512`

Avaya collection tasks

Routers – Avaya Collection tasks retrieve configuration data from Avaya routers and add this data to the current model.

Task properties

The properties that control **Routers – Avaya Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Avaya routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the routers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user

Property	Description
	authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system Temp directory.
Model Loopback	Specifies whether to model loopback interfaces.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

AVAYA ERS ROUTING SWITCH

You can add or update configuration data from Avaya Ethernet Routing Switches to the current model:

- Using an online collection task:
  - Configure a switch (see page 185) to permit access from a Skybox Collector and create a collection task (see page 186) to collect the switch configurations and add the configuration data to the model.

    The collection task can collect data from multiple switches.
- Using an offline file import task:
  - Generate and retrieve switch configuration files and import their data into the model (see page 187).

    The file import task can import the data of multiple switches.

Configuring Avaya ERS routing switches for data collection

To configure an Avaya ERS switch for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Avaya ERS Collection tasks use the Telnet protocol to connect to Avaya ERS switches.

Commands sent to device

Routers – Avaya ERS Collection tasks send the following commands to Avaya ERS switches:

- `no terminal more`
- `config`
- `show config`
- `show sys info`
- `show ip route info`

Avaya ERS collection tasks

Routers – Avaya ERS Collection tasks retrieve configuration data from Avaya ERS switches and add this data to the current model.

Task properties

The properties that control **Routers – Avaya ERS Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Avaya ERS switches. **Note**: A task can collect the configurations of multiple switches only if the same authentication is used for all the switches.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the switches.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Connection Protocol	The connection protocol to use.
Advanced tab	
Override device prompt	The router prompt. If this field is empty, the default prompt is expected: **#$**.
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system Temp

Property	Description
	directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the switches. **Note**: Use this property if different locations use the same set of IP addresses, so that switches at different locations can have the same IP address.

Importing Avaya ERS configuration data

You can use an **Import – Directory** task to import Avaya ERS configuration data.

Note: If you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import an Avaya ERS switch configuration:

- `run.txt`: The Avaya ERS configuration file

  This file is the output of the Avaya ERS show `config` command.

- (Optional) `route.txt`: Dump of the Avaya ERS routing table

  This file is the output of the Avaya ERS show `ip route info` command.

You can import the configurations of multiple switches; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

BROCADE VDX ROUTER

You can add or update configuration data from Brocade VDX routers to the current model:

- Using an online collection task:
  - Configure a router (see page 187) to permit access from a Skybox Collector and create a collection task (see page 188) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.
- Using an offline file import task:
  - Generate and retrieve router configuration files and import their data into the model (see page 189).

    The file import task can import the data of multiple routers.

Configuring Brocade VDX routers for data collection

To configure an Brocade VDX router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Brocade VDX Collection tasks use the SSH protocol to connect to Brocade VDX routers.

Commands sent to device

Routers – Brocade VDX Collection tasks send the following commands to Brocade VDX routers:

- `terminal length 0`
- `show clock | include xxx`
- `sh run | exclude "ip community-list"`
- `sh ver`
- `sh run | include "rbridge-id"`
- `show ip route rbridge-id 100`

Brocade VDX collection tasks

Routers – Brocade VDX Collection tasks retrieve configuration data from Brocade VDX routers and add this data to the current model.

Task properties

The properties that control **Routers – Brocade VDX Collection** tasks are described in the following table.

Property	Description
Basic tab	
Routers' Addresses	A comma-separated list of the IP addresses of the Brocade VDX routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the routers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.

Property	Description
Advanced tab	
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Importing Brocade VDX configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import an Brocade VDX router configuration:

- `run.txt`: The VDX configuration file

  This file is the output of the VDX `sh run` command.

  Important: Add the line `BROCADE VDX` at the begining of the file.

- `route.txt`: Dump of the VDX routing table

  Create this file as the output of the VDX `sh ip route` command.

  For every RBridge with a routing table (if any), append the output of the `sh ip route rb <RBridge ID>` command to `route.txt`.

You can import the configurations of multiple routers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

CISCO IOS ROUTER

You can add or update configuration data from Cisco IOS routers to the current model:

- Using an online collection task:
  - Configure the routers (see page 189) to permit access from a Skybox Collector and create a collection task (see page 192) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.
- Using an offline file import task:
  - Generate and retrieve router configuration files and import their data into the model (see page 195).

    The file import task can import the data of multiple routers.

Configuring Cisco IOS routers for data collection

To configure a Cisco IOS router so that Skybox can retrieve its configuration data:

- In the router, create an admin user with level 5 privileges.

> Note: If the user name that you use to log in to the router has sufficient permissions, you do not need to create an admin user.
>
> The method described here creates an admin user that does not have login permissions; you need another user name to log in to the router.

- To use the show conf command, grant file privileges to the user.

› Enable access to the router from the Skybox Collector:

- If access rules are configured on the router, configure a rule to permit either SSH or Telnet access from the Skybox Collector IP address to the router.

> Note: By default, Cisco IOS routers do not have an SSH server installed; install an IOS encryption support package to support connection using SSH.

To create a user if you are using Cisco's authentication mechanism (basic or AAA)

1 Add a user with level 5 privileges:

```
# username skybox password skybox privilege 5
```

2 Configure a password for this user.

You need the user name and password when you create the router collection task.

3 Execute the following commands to grant this user permissions to the IOS `show conf` and `show ip route vrf *` commands:

```
# conf term
# privilege exec all level 5 show conf
# privilege exec all level 5 show ip route
# privilege exec all level 5 term length 0
# write mem
```

To create a user if you are using TACACS or RADIUS

1 Configure a level 5 user on the TACACS or RADIUS.

2 Configure a password for this user.

You need the user name and password when you create the router collection task.

3 Execute the following commands to grant this user permissions to the IOS router `show conf` and `show ip route vrf *` commands:

```
# conf term
# privilege exec all level 5 command running-config
# privilege exec all level 5 command route
# write mem
```

To set file permissions for the show conf command

› At step **3** of the previous 2 procedures (before the command `# write mem`), execute:

`file privilege 1`

Commands sent to Cisco IOS routers

Connection type

Routers – Cisco IOS Collection tasks use the SSH protocol to connect to IOS routers.

Commands sent to device

Routers – Cisco IOS Collection tasks send the following commands to IOS routers:

- One of:
  - `enable`
  - `login`

  depending on the value of **Enabling Command** in the **Basic** tab of the task
- `terminal length 0`
- `terminal width 200`
- One of:
  - `show conf` *and* `show ver`
  - `show run`
  - `show run view full`
  - `show run all`
  - `show startup-config` (this command is also sent if you select **Collect Startup Configuration** in the **Advanced** tab of the task)

  depending on the value of **Get Configuration Command** in the **Advanced** tab of the task
- One of:
  - `show ip route vrf *`
  - `show ip route`
  - `show route vrf all`
  - `show route`
  - `show ip route vrf all`
  - `show route` *and* `show route vrf all`
  - `sh route`

  depending on the value of **Get Routing Table Command** in the **Advanced** tab of the task
- `sh snmp user`
- `show access-lists`

  This command is sent only if you select **Collect hit counts** in the **Advanced** tab of the task.

- show vrf ipv6
- show ipv6 route
- show ipv6 route vrf <VRF name> (for each VRF returned by show vrf ipv6)
- show ip bgp vpnv4 all labels

  This command is sent only if you select:

  - **show conf** or **show run** in **Get Configuration Command** in the **Advanced** tab of the task

  and

  - **show ip route vrf *** or **show route vrf all** in **Get Routing Table Command** in the **Advanced** tab of the task

Cisco IOS collection tasks

Routers – Cisco IOS Collection tasks retrieve configuration data from Cisco IOS routers and add this data to the current model.

Specifying the routing information to collect

By default, the Skybox Collector executes the IOS `show ip route vrf *` command. To have the Collector execute only specific subcommands of this command, change the value of `ios.routingCommand` in `<Skybox_Home>\collector\conf\sb_collector.properties`, listing the required (comma-separated) subcommands. For example, if you set **ios.routingCommand=connected,static**, the Collector executes the commands `show ip route vrf connected` and `show ip route vrf static` only.

Task properties

The properties that control **Routers – Cisco IOS Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	The connection protocol to use.
SSH Port	If **Connection Protocol** = **ssh**, the port on which the routers listen. If you change the default port (22) on the routers, the Skybox Collector must have permission to connect to the routers on the port that you specify.
Routers' Addresses	A comma-separated list of the IP addresses and IP address ranges of the Cisco IOS routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from

Property	Description
	CyberArk. (To use this option, configure CyberArk (see page 22).) • **Access token**: Take the values for the user name, user password, administrator name, and administrator password from a repository. For information about the repository, see Device access management (on page 20).
Username	This field is displayed if **Method** = **Device**. The user name to access the routers.
Password	This field is displayed if **Method** = **Device**. The user password.
Admin Username	This field is displayed if **Method** = **Device**. The user name of an administrator on the routers. After logging in with **Username**, Skybox runs set user on the routers using **Admin Username**. **Note**: If **Username** has sufficient permissions, you can leave this field empty; otherwise, it is mandatory.
Admin Password	This field is displayed if **Method** = **Device**. The administrator password. **Note**: Only required if you provide **Admin Username** (see previous note).
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Admin Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the administrator authentication credential object. **Note**: If the user specified in **Object** has sufficient permissions, you can leave this field empty; otherwise, it is mandatory.
Admin Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the administrator name and password. **Note**: Only required if you provide **Admin Safe** (see previous note).
Enable Setting	
Enabling Command	The command to use for user authentication if you provide: • (**Method** = **Device**) **Admin Username** and **Admin Password** • (**Method** = **CyberArk**) **Admin Object**

Property	Description
Enable Privilege	This field is enabled only if **Enabling Command** = **enable**. The privilege to append when sending the enable command. (If this field is empty, the enable command is sent with no value appended.)
Collection Setting	
Collect hit counts	Specifies whether to retrieve the hit counts of the access rules. If selected, rule usage analysis is available immediately; you do not need to run a **Change Tracking Events – Syslog Import** task. **Note**: Actual usage (trace) information is not collected.
Advanced tab	
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.
Get Configuration Command	The command to send to the routers to retrieve the configuration. **Note**: If you select **sh conf**, you must configure file permissions on the router (see Configuring Cisco IOS routers for data collection (on page 189)). **Note**: If you select **Collect Startup Configuration**, do not select **sh conf**.
Collect Startup Configuration	This field is disabled if **Get Configuration Command** = **show startup-config**. Specifies whether to collect the startup configuration. If selected, you can compare the startup configuration and the running configuration. For information about making this comparison, see the Cisco configuration diffs topic in the Skybox Firewall Assurance User Guide.
Get Routing Table Command	The command to send to the routers to generate the routing table. **Note**: For IOS-XR routers, select sh route and *not* show route.
Ignore routing rules with following metrics	A comma-separated list of metrics of BGP routing rules to exclude from the collected routes.
Import BGP Routes	Specifies whether to import BGP routing rules. • **System default**: Use the value of `ios_ignore_BGP_routing_rules` in `<Skybox_Home>\server\conf\sb_common.properties` (this property has a default value of `true`)
Skip SSH Banner	Specifies whether to skip the SSH banner. • **System default**: Use the value of `ios.skip_banner` in `<Skybox_Home>\collector\conf\sb_collector.properties` (this property has a default value of `true`)

Importing Cisco IOS configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Cisco IOS router configuration:

- `run.txt`: The IOS configuration file

  This file is the concatenation of the output of the following 2 IOS commands:

  i. `sh conf | include hostname`

  Note: To use the `sh conf` command, you must have file privileges (see Configuring Cisco IOS routers for data collection (on page 189)). You can use `sh run` instead of `sh conf | include hostname`.

  ii. `sh ver` (use this exact format)

  - (Optional) Hit counts are imported if you append the output of the `show access-lists` command to `run.txt`.

- (Optional) `route.txt`: Dump of the IOS routing table

  This file is the output of the IOS `show ip route vrf *` command.

  Note: If you cannot extract routing rules in device native format, you can manually append the rules to the end of the device configuration file. See Appending routing information to device configuration (on page 43).

  To import the output of selected subcommands of the `ip route vrf *` command, execute the subcommands and manually concatenate the output into a single file.

  Note: For Cisco IOS-XR routers concatenate the output of the `sh route` commands to `route.txt`.

If `route.txt` is included, its routing rules overwrite routing rules from `run.txt` because its information is more extensive and includes static and dynamic routing rules.

You can import the configurations of multiple routers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

CISCO NEXUS ROUTER

You can add or update configuration data from Cisco Nexus routers to the current model:

- Using an online collection task:
  - Configure the routers (see page 196) to permit access from a Skybox Collector and create a collection task (see page 197) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.

- Using an offline file import task:

- Generate and retrieve router configuration files and import their data into the model (see page 199).

  The file import task can import the data of multiple routers.

Configuring Cisco Nexus routers for data collection

To configure a Cisco Nexus router so that Skybox can retrieve its configuration data:

- In the router, create an admin user with level 5 privileges.

> Note: If the user name that you use to log in to the router has sufficient permissions, you do not need to create an admin user.
>
> The method described here creates an admin user that does not have login permissions; you need another user name to log in to the router.

- Enable access to the router from the Skybox Collector:
  - If access rules are configured on the router, configure a rule to permit either SSH or Telnet access from the Skybox Collector IP address to the router.

To create a user if you are using Cisco's authentication mechanism (basic or AAA)

1 Add a user with level 5 privileges:

```
# username skybox password skybox privilege 5
```

2 Configure a password for this user.

You need the user name and password when you create the router collection task.

3 Execute the following commands to grant this user permissions to the Nexus `show conf` and `show ip route vrf all` commands:

```
# conf term
# privilege exec all level 5 show conf
# privilege exec all level 5 show ip route
# privilege exec all level 5 term length 0
# write mem
```

To create a user if you are using TACACS or RADIUS

1 Configure a level 5 user on the TACACS or RADIUS.

2 Configure a password for this user.

You need the user name and password when you create the router collection task.

3 Execute the following commands to grant this user permissions to the Nexus router `show conf` and `show ip route vrf all` commands:

```
# conf term
# privilege exec all level 5 command running-config
# privilege exec all level 5 command route
# write mem
```

Commands sent to Cisco Nexus routers

Connection type

Routers – Cisco Nexus Collection tasks use the SSH protocol to connect to Nexus routers.

Commands sent to device

Routers – Cisco Nexus Collection tasks send the following commands to Nexus routers:

- One of:
  - `enable`
  - `login`

  depending on the value of **Enabling Command** in the **Basic** tab of the task
- `show vdc`
- `terminal length 0`
- `terminal width 200`
- `changeto system`
- `sh hostname`
- `switchto vdc <VDC>`
- One of:
  - `show running-config all`
  - `show startup-config` (this command is also sent if you select **Collect Startup Configuration** in the **Advanced** tab of the task)

  depending on the value of **Get Configuration Command** in the **Advanced** tab of the task
- `sh ver`
- `show ip route vrf all`

Cisco Nexus collection tasks

Routers – Cisco Nexus Collection tasks retrieve configuration data from Cisco Nexus routers and add this data to the current model.

Task properties

The properties that control **Routers – Cisco Nexus Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	The connection protocol to use.
SSH Port	If **Connection Protocol** = **ssh**, the port on which the routers listen. If you change the default port (22) on the routers, the

Property	Description
	Skybox Collector must have permission to connect to the routers on the port that you specify.
Addresses	A comma-separated list of the IP addresses and IP address ranges of the Nexus routers. To collect configurations of all VDCs from a router with multiple VDCs, type the IP address of the admin VDC. (To collect the configuration of 1 VDC, type the IP address of the VDC.) **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the routers.
Password	This field is displayed if **Method** = **Device**. The user password.
Admin Username	This field is displayed if **Method** = **Device**. The user name of an administrator on the routers. After logging in with **Username**, Skybox runs set user on the routers using **Admin Username**. **Note**: If **Username** has sufficient permissions, you can leave this field empty; otherwise, it is mandatory.
Admin Password	This field is displayed if **Method** = **Device**. The administrator password. **Note**: Only required if you provide **Admin Username** (see previous note).
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Enabling Command	The command to use for user authentication.
Advanced tab	
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.
Get Configuration Command	The command to send to the routers to retrieve the configuration.
Collect Startup	This field is disabled if **Get Configuration Command** =

Property	Description
Configuration	**show startup-config**. Specifies whether to collect the startup configuration. If selected, you can compare the startup configuration and the running configuration. For information about making this comparison, see the Cisco configuration diffs topic in the Skybox Firewall Assurance User Guide.
Import BGP Routes	Specifies whether to import BGP routing rules. • **System default**: Use the value of `nexus_ignore_BGP_routing_rules` in `<Skybox_Home>\server\conf\sb_common.properties` (this property has a default value of `true`)

Importing Cisco Nexus configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Cisco Nexus router configuration:

- `run.txt`: The Nexus configuration file

  This file is the concatenation of the output of the following 2 Nexus commands:

  i. `show run | include hostname`

  ii. `sh ver` (use this exact format)

- (Optional) `route.txt`: Dump of the Nexus routing table

  This file is the output of the Nexus `show ip route vrf *` command.

  To import the output of selected subcommands of the `ip route vrf *` command, execute the subcommands and manually concatenate the output into a single file.

If `route.txt` is included, its routing rules overwrite routing rules from `run.txt` because its information is more extensive and includes static and dynamic routing rules.

You can import the configurations of multiple routers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

CISCO WIRELESS LAN CONTROLLER

You can add or update configuration data from Cisco Wireless LAN Controllers to the current model:

- Using an online collection task:
  - Configure a wireless controller (see page 200) to permit access from a Skybox Collector and create a collection task (see page 200) to collect the wireless controller configurations and add the configuration data to the model.

    The collection task can collect data from multiple wireless controllers.

- Using an offline file import task:
  - Generate and retrieve wireless controller configuration files and import their data into the model (see page 201).

    The file import task can import the data of multiple wireless controllers.

Configuring Cisco Wireless LAN Controllers for data collection

To configure a Cisco Wireless LAN Controller for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Wireless Controller – Cisco WLC Collection tasks use the SSH protocol to connect to Cisco Wireless LAN Controllers.

Commands sent to device

Wireless Controller – Cisco WLC Collection tasks send the following commands to Cisco Wireless LAN Controllers:

- `config paging disable`
- `show run-config`
- `show run-config commands`

  This command is sent only if you select **Config Commands** in the **Advanced** tab of the task.

Cisco Wireless LAN Controller collection tasks

Wireless Controller – Cisco WLC Collection tasks retrieve configuration data from Cisco Wireless LAN Controllers add this data to the current model.

Task properties

The properties that control **Wireless Controller – Cisco WLC Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Cisco Wireless LAN Controllers. **Note**: A task can collect the configurations of multiple wireless controllers only if the same authentication is used for all the wireless controllers.
Username	The user name to access the wireless controllers.
Password	The user password.
Advanced tab	
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.) The location of the debug log file.

Property	Description
	If this field is empty, the task does not save debug messages.
Config Commands	Specifies whether to run configuration checks by sending the show `run-config` commands command.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the wireless controllers. **Note**: Use this property if different locations use the same set of IP addresses, so that wireless controllers at different locations can have the same IP address.

Importing Cisco Wireless LAN Controller configuration data

You can use an **Import – Directory** task to import Cisco Wireless LAN Controller (WLC) configuration data.

The following file is required to import a WLC configuration:

- `*.*`: The WLC configuration file

  This file is the output of the WLC show `run-config` command.

You can import the configurations of multiple WLCs.

DIONIS NX ROUTER

You can add or update configuration data from Dionis NX routers to the current model using an online collection task:

- Configure a router (see page 201) to permit access from a Skybox Collector and create a collection task (see page 202) to collect the router configurations and add the configuration data to the model.

  The collection task can collect data from multiple routers.

Configuring Dionis NX routers for data collection

To configure a Dionis NX router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Dionis Collection tasks use the SSH protocol to connect to Dionis NX routers.

Commands sent to device

Routers – Dionis Collection tasks send the following commands to Dionis NX routers:

- `show running-config`
- `show version`

Dionis NX collection tasks

Routers – Dionis Collection tasks retrieve configuration data from Dionis NX routers and add this data to the current model.

Task properties

The properties that control **Routers – Dionis Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Router address	A comma-separated list of IP addresses of Dionis NX routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Username	The user name to access the routers.
Password	The user password.
Advanced tab	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

ENTERASYS ROUTER

You can add or update configuration data from Enterasys routers to the current model:

- Using an online collection task:
  - Configure a router (see page 203) to permit access from a Skybox Collector and create a collection task (see page 203) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.
- Using an offline file import task:
  - Generate and retrieve router configuration files and import their data into the model (see page 204).

    The file import task can import the data of multiple routers.

Configuring Enterasys routers for data collection

To configure an Enterasys router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Enterasys Collection tasks use the SSH protocol to connect to Enterasys routers.

Commands sent to device

Routers – Enterasys Collection tasks send the following commands to Enterasys routers:

- `terminal more disable`
- `show config all`
- `show ip route`

Enterasys collection tasks

Routers – Enterasys Collection tasks retrieve configuration data from Enterasys routers and add this data to the current model.

Task properties

The properties that control **Routers – Enterasys Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Enterasys routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the routers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.

Property	Description
Connection Protocol	The connection protocol to use.
Advanced tab	
Override device prompt	The router prompt. If this field is empty, the default prompt is expected: **#$**.
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Importing Enterasys configuration data

You can use an **Import – Directory** task to import Enterasys configuration data.

Note: If you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import an Enterasys router configuration:

- `run.txt`: The Enterasys configuration file

  This file is the output of the Enterasys show `config all` command.

- (Optional) `route.txt`: Dump of the Enterasys routing table

  This file is the output of the Enterasys show `ip route` command.

You can import the configurations of multiple routers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

EXTREME NETWORKS ROUTER

You can add or update configuration data from Extreme Networks routers to the current model:

- Using an online collection task:
  - Configure a router (see page 205) to permit access from a Skybox Collector and create a collection task (see page 205) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.
- Using an offline file import task:
  - Generate, retrieve, and parse router configuration files and import their data into the model (see page 206).

The file import task can import the data of multiple routers.

Configuring Extreme Networks routers for data collection

To configure an Extreme Networks router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Extreme Networks Collection tasks use the SSH protocol to connect to Extreme Networks routers.

Commands sent to device

Routers – Extreme Networks Collection tasks send the following commands to Extreme Networks routers:

- `terminal more disable`
- `disable clipaging`
- `set length 0`
- `show config`
- `show ipr`
- `show policy detail`

Extreme Networks collection tasks

Routers – Extreme Networks Collection tasks retrieve configuration data from Extreme Networks routers and add this data to the current model.

Task properties

The properties that control **Routers – Extreme Networks Collection** tasks are described in the following table.

Property	Description
Basic tab	
Addresses	A comma-separated list of the IP addresses of the Extreme Networks routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Username	The user name to access the routers.
Password	The user password.
Connection Protocol	The connection protocol to use.
Advanced tab	
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system Temp directory.

Property	Description
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Importing Extreme Networks configuration data

You can use an **Import – Directory** task to import Extreme Networks configuration data.

Skybox includes a script that retrieves Extreme Networks router configuration files and a parser that creates an iXML file from these files. This iXML file can then be imported into Skybox.

The script is `<Skybox_Home>\intermediate\bin\collectors\router\extremeNetworks\extremeNetworksCollection.pl`

The parser is `<Skybox_Home>\intermediate\bin\parsers\router\extremeNetworks\extremeNetworksParser.pl`

For help using a script, run the script without any arguments.

For additional help, open a case at the Skybox Support portal.

You can import the configurations of multiple routers.

JUNIPER NETWORKS MX ROUTER

You can add or update configuration data from Juniper Networks MX routers to the current model using an online collection task or an offline file import task.

MX routers use the Junos operating system—follow the instructions in Juniper Networks Junos firewall (on page 123).

HP PROCURVE ROUTER

You can add or update configuration data from HP ProCurve routers to the current model:

- Using an online collection task:
  - Configure a router (see page 207) to permit access from a Skybox Collector and create a collection task (see page 207) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.
- Using an offline file import task:
  - Generate and retrieve router configuration files and import their data into the model (see page 208).

    The file import task can import the data of multiple routers.

Configuring HP ProCurve routers for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure an HP ProCurve router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – HP ProCurve Collection tasks use the SSH protocol to connect to HP ProCurve routers.

Commands sent to device

Routers – HP ProCurve Collection tasks send the following commands to HP ProCurve routers:

- `show run`
- `show ip route`
- `no page`
- `enable`

HP ProCurve collection tasks

Routers – HP ProCurve Collection tasks retrieve configuration data from HP ProCurve routers and add this data to the current model.

Task properties

The properties that control **Routers – HP ProCurve Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the HP ProCurve routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the routers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user

Property	Description
	authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Enable Password	The password for enable command privileges on the routers.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Importing HP ProCurve configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import an HP ProCurve router configuration:

- `*.*`: The ProCurve configuration file

  This file is the output of the ProCurve `show run` command.

- (Optional) `route.txt`: Dump of the ProCurve routing table

  This file is the output of the ProCurve `show ip route` command.

You can import the configurations of multiple routers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

Note: To run an **Import – Collector** task or an **Import – Collector Advanced** task, the Skybox Collector specified for the task must reside on a Linux platform.

HUAWEI ROUTER

You can add or update configuration data from Huawei routers to the current model:

- Using an online collection task:
  - Configure a router (see page 209) to permit access from a Skybox Collector and create a collection task (see page 209) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.
- Using an offline file import task:
  - Generate and retrieve router configuration files and import their data into the model (see page 210).

The file import task can import the data of multiple routers.

Configuring Huawei routers for data collection

To configure a Huawei router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Huawei Collection tasks use the SSH protocol to connect to Huawei routers.

Commands sent to device

Routers – Huawei Collection tasks send the following commands to Huawei routers:

- `screen-length 0 temporary`
- One or both of:
  - `display ip routing-table all-routes`
  - `display ip routing-table`

  depending on the version of the router
- `display current-configuration`
- `display ip vpn-instance`
- `display ip routing-table vpn-instance <VPN instance name>`

Huawei collection tasks

Routers – Huawei Collection tasks retrieve configuration data from Huawei routers and add this data to the current model.

Task properties

The properties that control **Routers – Huawei Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Huawei routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Username	The user name to access the routers.
Password	The user password.
Connection Protocol	The connection protocol to use.

Property	Description
SSH Port	If **Connection Protocol** = **ssh**, the port on which the routers listen. If you change the default port (22) on the routers, the Skybox Collector must have permission to connect to the routers on the port that you specify.
Advanced tab	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system `Temp` directory.
Logging	(Only select this option if Skybox Professional Services has requested a basic debug file.) Specifies whether the task writes a basic debug log. If selected, the log is saved in the operating system `Temp` directory.
SSH Timeout	The number of seconds that the Skybox Collector waits for a response from a router before timing out.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Importing Huawei configuration data

You can use an **Import – Directory** task to import Huawei configuration data.

A single file, which can have any name, is required to import a Huawei router configuration. Create the file from the following files:

1. The Huawei configuration file

   This file is the output of the Huawei `display current-configuration` command.

2. (Optional) Append a dump of the Huawei routing table to the configuration file

   This is the output of the Huawei `display ip routing-table` or `display ip routing-table all-routes` command; the command to use depends on the version of the router

   If the routing table is included, its routing rules overwrite routing rules from the configuration file because its information is more extensive and includes static and dynamic routing rules

3. (Optional) Append a dump of the routing table for each VPN instance

   For each VPN instance, this is the output of the Huawei `display ip routing-table vpn-instance <VPN instance name>` command

You can import the configurations of multiple routers.

H3C ROUTER

You can add or update configuration data from H3C routers to the current model:

- Using an online collection task:
  - Configure a router (see page 211) to permit access from a Skybox Collector and create a collection task (see page 211) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.
- Using an offline file import task:
  - Generate and retrieve router configuration files and import their data into the model (see page 212).

    The file import task can import the data of multiple routers.

Configuring H3C routers for data collection

To configure an H3C router for data collection:

- Skybox data collection requires a user with admin permissions on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – H3C Collection tasks use the SSH protocol to connect to H3C routers.

Commands sent to device

Routers – H3C Collection tasks send the following commands to H3C routers:

- `screen-length disable`
- `disable paging`
- `display`
- `display ip routing-table`

H3C collection tasks

Routers – H3C Collection tasks retrieve configuration data from H3C routers and add this data to the current model.

Task properties

The properties that control **Routers – H3C Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the H3C routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.

Property	Description
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the routers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
User Type	Specifies the privilege level available to the task.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Importing H3C configuration data

You can use an **Import – Directory** task to import H3C configuration data.

Note: If you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a H3C router configuration:

- `run.txt`: The H3C configuration file

  This file is the output of the H3C `display` command.

- (Optional) `route.txt`: Dump of the H3C routing table

  This file is the output of the H3C `display ip routing-table` command.

You can import the configurations of multiple routers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

NORTEL PASSPORT 8600 ROUTER

You can add or update configuration data from Nortel Passport 8600 routers to the current model:

- Using an online collection task:

  - Configure the routers (see page 213) to permit access from a Skybox Collector and create a collection task (see page 213) to collect the router configurations and add the configuration data to the model.

    The collection task can collect data from multiple routers.

- Using an offline file import task:
  - Generate and retrieve router configuration files and import their data into the model (see page 214).

    The file import task can import the data of multiple routers.

Configuring Nortel Passport 8600 routers for data collection

To configure a Nortel router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Nortel Passport Collection tasks use the SSH protocol to connect to Nortel Passport routers.

Commands sent to device

Routers – Nortel Passport Collection tasks send the following commands to Nortel Passport routers:

- `config cli more false`
- `sh conf`
- `sh ip route info`

Nortel Passport collection tasks

Routers – Nortel Passport Collection tasks retrieve configuration data from Nortel Passport routers and add this data to the current model.

Task properties

The properties that control **Routers – Nortel Passport Collection** tasks are described in the following table.

Property	Description
Basic tab	
Connection Protocol	The connection protocol to use.
Routers' Addresses	A comma-separated list of the IP addresses and IP address ranges of the Nortel Passport routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Authentication	
Use Access Tokens	Specifies whether to take the values for **Username** and **Password** from a repository. • For information about the repository, see Device

Property	Description
	access management (on page 20).
Username	The user name to access the routers.
Password	The user password.
Advanced tab	
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Importing Nortel Passport 8600 configuration data

The following files are required to import a Nortel Passport router configuration:

- `run.txt`: The Nortel configuration file

  This file is the output of the Nortel show conf command.

- (Optional) `route.txt`: Dump of the Nortel routing table

  This file is the output of the Nortel show ip route command.

If `route.txt` is included, its routing rules overwrite routing rules from `run.txt` because its information is more extensive and includes static and dynamic routing rules.

You can import the configurations of multiple routers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

VYATTA ROUTER

You can add or update configuration data from Vyatta routers to the current model using an online collection task:

- Configure a router (see page 214) to permit access from a Skybox Collector and create a collection task (see page 215) to collect the router configurations and add the configuration data to the model.

  The collection task can collect data from multiple routers.

Configuring Vyatta routers for data collection

To configure a Vyatta router for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Routers – Vyatta Collection tasks use the SSH protocol to connect to Vyatta routers.

Commands sent to device

Routers – Vyatta Collection tasks send the following commands to Vyatta routers:

- `show version`
- `show configuration`
- `show ip route`

Vyatta collection tasks

Routers – Vyatta Collection tasks retrieve configuration data from Vyatta routers and add this data to the current model.

Task properties

The properties that control **Routers – Vyatta Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Server Name or IP	A comma-separated list of host names or IP addresses of Vyatta routers. **Note**: A task can collect the configurations of multiple routers only if the same authentication is used for all the routers.
Username	The user name to access the routers.
Password	The user password.
Advanced tab	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system `Temp` directory.
Vyatta router type	Specifies the type of router from which this task collects configuration data.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the routers. **Note**: Use this property if different locations use the same set of IP addresses, so that routers at different locations can have the same IP address.

Chapter 8

Scanner tasks

This chapter describes how to add vulnerability scanner output to the current model.

There are 2 types of scanner tasks:

- Scan tasks: These tasks initiate a scan, collect the results, and add vulnerability occurrence data to the model.
- Collection tasks: These tasks collect the results of previously run scans and add vulnerability occurrence data to the model.

In both cases, vulnerability occurrences are added or updated and, if necessary, new assets and services are added to the model.

In this chapter

GUIDELINES FOR SETTING UP SCANNER TASKS

Review the following when setting up scanner tasks:

- Skybox requires unrestricted scanning output—output with a minimum of control devices blocking the route between the scanner and the scanned assets. Otherwise, Skybox's analysis of access and attack scenarios in the model does not reflect the actual access and possibility of attacks.
- If your organization includes DHCP networks, you get a more accurate model if you use separate scans for the DHCP networks and for the static networks

because Skybox uses a different mechanism to merge scans of DHCP networks into the model.

BEYONDTRUST RETINA SCANNER

You can add or update vulnerability occurrence data from BeyondTrust (eEye) Retina scanners to the current model using an online collection task:

- Create a collection task (see page 217) to collect the vulnerability occurrences found by the scanner and add the vulnerability occurrence data to the model.

You can create a blacklist of scanner IDs (see page 236) that Skybox ignores.

Configuring BeyondTrust Retina scanners for data collection

Skybox supports the Retina 4.9, Retina 5, and Retina 6 vulnerability scanners.

Note: For Retina 4.9, the Skybox Collector that collects the results of the Retina vulnerability scanner must run on a Windows platform.

Connection type

If **Scan Output Type** = **DSN** in the task definition, **Scanners – Retina Collection** tasks use SQL to connect to BeyondTrust Retina scanners.

BeyondTrust Retina collection tasks

Scanners – Retina Collection tasks retrieve vulnerability occurrence data collected by BeyondTrust Retina scanners and add this data to the current model.

Note: By default, data is collected only for assets marked in the Retina scanner database as **scan finished**. In some installations, this field is not filled and assets are skipped; to force collection of all assets, set `Retina.ForceImport` to **true** in `<Skybox_Home>\collector\conf\sb_collector.properties`.

Task properties

The properties that control **Scanners – Retina Collection** tasks are described in the following table.

Property	Description
Basic tab	
Recency	Collect scans generated in the specified number of days before today.
Scan Output Type	The output type of the scan.
Files Directory Path	This field is displayed if **Scan Output Type** = **FILE**. • The full path to a directory containing Retina output RTD files • The full path to an RTD file, including the file name **Note**: If you only specify a path, all RTD files in the directory are parsed and merged.
DSN Name	This field is displayed if **Scan Output Type** = **DSN**. The name of the DSN that is configured for the Retina output.
Dictionary location	Specifies how the Retina dictionary location is defined. **Note**: If the Skybox Collector that collects the results of

Property	Description
	the Retina vulnerability scanner is running on a Linux platform, set this field to **PATH**.
Dictionary files path	This field is displayed if **Dictionary location** = **PATH**. The full path to the Retina dictionary files (`audits.xml` and `services.xml`). **Note**: This option is not supported for the Retina 4.9 vulnerability scanner.
Advanced tab	
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.

MCAFEE VULNERABILITY MANAGER (FOUNDSTONE) SCANNER

You can add or update vulnerability occurrence data from McAfee Vulnerability Manager (Foundstone) scanners to the current model using an online collection task:

- Configure a scanner (see page 218) to permit access from a Skybox Collector and create a collection task (see page 218) to collect the vulnerability occurrences found by the scanner and add the vulnerability occurrence data to the model.

You can create a blacklist of scanner IDs (see page 236) that Skybox ignores.

Configuring McAfee Vulnerability Manager (Foundstone) scanners for data collection

To configure a McAfee Vulnerability Manager (Foundstone) scanner for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Scanners – McAfee MVM Collection tasks use SQL to connect to McAfee Vulnerability Manager (Foundstone) scanners.

McAfee Vulnerability Manager (Foundstone) collection tasks

Scanners – McAfee MVM Collection tasks retrieve vulnerability occurrence data collected by a McAfee Vulnerability Manager (Foundstone) scanner and add this data to the current model.

Task properties

The properties that control **Scanners – McAfee MVM Collection** tasks are described in the following table.

Property	Description
Basic tab	
Network Scope	The assets and container entities whose vulnerability occurrence data is added to the model by the task.
Recency	Collect scans generated in the specified number of days before today.
Database connection	
Address/Name	The name or IP address of the database server that hosts the Foundstone database.
User Authentication	
Database Username	The user name of a user of the McAfee Vulnerability Manager scanner.
Database Password	The user password.
Advanced tab	
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.
Policy Name	The McAfee Vulnerability Manager policy for which to retrieve a scan. If this field is empty, the most recent scan is retrieved. Wildcards are supported, as described in the following table.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
DSN Name	(Read-only) The name of the DSN that is configured for the McAfee Vulnerability Manager output. **Note**: This field is displayed for backward compatibility only; it is for tasks created in previous versions of Skybox. To create a task, provide a value in the **Address/Name** field in the **Basic** tab.

Using wildcards in the Policy Name property

The wildcards that **Policy Name** property can use are described in the following table. For example, to get all scans whose policy name does *not* end with D, use **%[^D]** as the policy name.

Wildcard	Descriptions
%	Any string of zero or more characters
_ (underscore)	Any single character
[ ]	Any single character in the specified range ([a-f]) or set ([abcdef])
[^]	Any single character not in the specified range ([^a-f]) or set ([^abcdef])

IBM SECURITY APPSCAN

You can add or update vulnerability occurrence data from IBM AppScan to the current model:

- Using an online collection task:
  - Configure a scanner (see page 220) to permit access from a Skybox Collector and create a collection task (see page 220) to collect the vulnerability occurrences found by the scanner and add the vulnerability occurrence data to the model.

    The scanner collection task can collect data from multiple scanners.
- Using an offline file import task:
  - Generate scanner vulnerability occurrence files and import their data into the model (see page 221).

    The file import task can import the data of multiple scanners.

Configuring IBM AppScan for data collection

To configure an IBM AppScan for data collection:

- Install the Python `lxml` package on the machine that is running the task.
- Configure the AppScan to generate reports (on a continuous basis).
- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

To download and install the Python lxml package on Skybox

- Download and install the `lxml` package from https://pypi.python.org/pypi/lxml/

IBM AppScan collection tasks

Scanners – AppScan Collection tasks retrieve vulnerability occurrence data collected by IBM AppScan and add this data to the current model.

Task properties

The properties that control **Scanners – AppScan Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Input File	The location of the XML files containing the AppScan scan data.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different

Property	Description
	locations can have the same IP address.

Importing IBM AppScan data

You can use an **Import – Directory** task to import the AppScan vulnerability occurrence data.

The following file is required to import AppScan data:

- `*.xml`: AppScan XML file

You can import the results of multiple scans.

IBM SECURITY SITEPROTECTOR SYSTEM

You can add or update vulnerability occurrence data collected by IBM Internet Scanners from an IBM Security SiteProtector System database to the current model using an online collection task:

- Create a collection task (see page 221) to collect the vulnerability occurrences found by the scanners and add the vulnerability occurrence data to the model.

You can create a blacklist of scanner IDs (see page 236) that Skybox ignores.

Configuring IBM SiteProtector for data collection

To configure an IBM SiteProtector database for data collection:

- Skybox data collection requires a read-only user on the database; we recommend that you create a separate user for this purpose.
- Make sure that the user running the task has the following permissions:
  - EXECUTE stored procedures
  - SELECT views

Connection type

Scanners – ISS SiteProtector Collection tasks use SQL to connect to IBM SiteProtector databases.

IBM SiteProtector collection tasks

Scanners – ISS SiteProtector Collection tasks retrieve vulnerability occurrence data, collected by IBM Internet Scanners, from an IBM SiteProtector database and add this data to the current model.

Task properties

The properties that control **Scanners – ISS SiteProtector Collection** tasks are described in the following table.

Property	Description
Basic tab	
Network Scope	The assets and container entities whose vulnerability occurrence data is added to the model by the task.

Property	Description
Recency	- An integer: Collect scans generated in the specified number of days before today. - A date range: Collect scans generated between the specified dates. Use American date format (MM/dd/yyyy-MM/dd/yyyy).
Sensor IP Address	The IP address of the scanner.
Database connection	
Address/Name	The name or IP address of the database server that hosts the SiteProtector database.
User Authentication	
Database Username	The user name to access the SiteProtector database.
Database Password	The user password.
Advanced tab	
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
DSN name	(Read-only) The name of the DSN that is configured for the server that hosts the SiteProtector database. **Note**: This field is displayed for backward compatibility only; it is for tasks created in previous versions of Skybox. To create a task, provide a value in the **Address/Name** field in the **Basic** tab.

QUALYS QUALYSGUARD SCANNER

You can add or update vulnerability occurrence data from Qualys QualysGuard scanners to the current model:

- Using an online collection task:
  - Configure a scanner (see page 223) to permit access from a Skybox Collector and create a collection task (see page 223) to collect the vulnerability occurrences found by the scanner and add the vulnerability occurrence data to the model.
- Using an offline file import task:
  - Generate scanner vulnerability occurrence files and import their data into the model (see page 226).

    The file import task can import the data of multiple scanners.

You can create a blacklist of scanner IDs (see page 236) that Skybox ignores.

Configuring Qualys QualysGuard scanners for data collection

The Qualys vulnerability scanner is unique among the vulnerability scanners used by Skybox, in that the scan results are not stored in Skybox. Rather, Skybox accesses the Qualys website to pull network configurations and vulnerabilities scan results.

Before configuring Qualys to work with Skybox, contact Qualys and open an account. We strongly recommend that you license Qualys API v2 (if you use Qualys API v1 and try to retrieve many scans, you might exceed the permitted number of API calls).

Save the following account information; you need the information when you create the Skybox task.

- Qualys account user name
- Qualys account password

After creating your Qualys account, configure connection between the Skybox Collector and the QualysGuard vulnerability scanner (that is, the Qualys IP address).

To configure connection to the QualysGuard vulnerability scanner

1. Make sure that the connection is not blocked by any firewalls.

   Note: Connecting to the Qualys website via a proxy server is supported.

2. Enable access from the Skybox Collector to the QualysGuard API server at:
   - (Users of Qualys US site) `https://qualysapi.qualys.com/`
   - (Users of Qualys European site) `https://qualysapi.qualys.de/`

   Fallback: Use the Qualys website at:

   (Users of Qualys US site) `https://qualysguard.qualys.com/`

   (Users of Qualys European site) `https://qualysguard.qualys.de/`

   If web access from the Skybox Collector goes through a proxy, configure the proxy IP address and port (see the Proxy Settings (Server) topic in the Skybox Installation and Administration Guide).

Connection type

Scanners – Qualys Collection tasks use HTTPS to connect to Qualys QualysGuard scanners.

Qualys QualysGuard collection tasks

Scanners – Qualys Collection tasks retrieve vulnerability occurrence data collected by Qualys QualysGuard scanners and add this data to the current model.

Task properties

The properties that control **Scanners – Qualys Collection** tasks are described in the following table.

Property	Description
Basic tab	
Qualys site	The Qualys site to which to connect. If the Qualys site is not in the list, select **Custom** and type the site URL in **Custom Qualys site**.
Custom Qualys site	This field is enabled only if **Qualys site** = **Custom**. The URL of the Qualys site to which to connect. **Note**: This field supports IPv4 only.
Username	The user name of a user, as defined on the Qualys Management Site. **Note**: We recommend that the user have read-only permissions only.
Password	The user password.
Network Scope	The assets and container entities whose vulnerability occurrence data is collected by the task.
Exclude Scope	The Assets and container entities that match **Network Scope** but whose vulnerability occurrence data is not to be added to the model by the task.
Filter	
Collection Method	Specifies whether to retrieve vulnerability occurrence data from a Qualys database or from Qualys scans.
Filter by	This field is disabled if **Collection Method** = **Database**. Specifies whether to collect scan and map files by name, by ID, or by user login. **Note**: This is user login and *not* user name.
Filter by Scan	This field is disabled if **Collection Method** = **Database**. Specifies whether to retrieve scan data.
Scan Filter	This field is enabled if **Filter by Scan** is selected. • (**Filter by** = **NAME**) The scan name to use when collecting the scan data. Only scans with names matching this string are imported. **Note**: Information about this filter appears in the table that follows this table. • (**Filter by** = **USER**) The user name to use when collecting the scan data. Only scans launched by users whose user name matches this string are imported. • (**Filter by** = **ID**) The exact ID of the scan to use.
Filter by Map	This field is disabled if **Collection Method** = **Database**. Specifies whether to retrieve map data.
Map Filter	This field is enabled if **Filter by Map** is selected. • (**Filter by** = **NAME**) The map name to use when collecting the scan data. Only maps with names matching this string are imported. **Note**: Information about this filter appears in the table that follows this table. • (**Filter by** = **USER**) The user name to use when collecting the scan data. Only maps launched by users whose user name matches this string are imported.

Property	Description
	- (**Filter by** = **ID**) The exact ID of the map to use.
Filter by Kernel Activity	Specifies whether to add vulnerability occurrence data to the model for some kernels only. By default, vulnerability occurrence data is added for all kernels.
Kernel Activity	This field is enabled if **Filter by Kernel Activity** is selected. The kernels for which to add vulnerability occurrence data to the model.
Recency	This field is ignored if **Collection Method** = **Database**. • An integer: Collect scans generated in the specified number of days before today. • A date range: Collect scans generated between the specified dates. Use American date format (MM/dd/yyyy-MM/dd/yyyy). **Note**: If you are using Qualys API v1, set the number of days as low as possible to avoid exceeding the permitted number of API calls.
Proxy	
Use Proxy	Specifies whether to use HTTP proxy settings. The proxy settings are set in the Options dialog box (see the Proxy Settings (Server) topic in the Skybox Installation and Administration Guide).
Advanced tab	
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Attach services to interfaces	Specifies whether to attach each service to an interface (instead of attaching it to all interfaces) after importing a scan.

About the Scan filter and Map filter fields

The strings to use for the **Scan filter** field and the **Map filter** field (if **Filter by** = **NAME** or **Filter by** = **USER**) are listed in the following table.

This text string	Collects these scans or maps
Empty string	All scans or maps within the date range specified in the

	Recency field.
A partial name (do not use quotation marks)	• (**Filter by** = **NAME**) Only scans or maps whose title contains this string. • (**Filter by** = **USER**) Only scans or maps launched by a user whose user name contains this string.
“N/A” (without quotation marks)	• (**Filter by** = **NAME**) Scans or maps that have no title in the Qualys UI • (**Filter by** = **USER**) Not relevant (do not use)
A regular expression (do not use quotation marks)	• (**Filter by** = **NAME**) All scans or maps that contain the result of the regular expression in their title. For example, the regular expression **Light|Full** matches scan titles including “Light scan” and “All Networks Full Scan”. • (**Filter by** = **USER**) All scans or maps launched by a user whose user name contains the result of the regular expression. **Note**: Text matching using regular expressions is not case-sensitive.

Importing Qualys QualysGuard scanner data

Note: We recommend that you use an **Import – Directory** task to import the scan data; if you include the Qualys Map, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import Qualys scan results:

- `scan.xml`: The Qualys scan file
- (Optional) `map.xml`: The Qualys Map

You can import the results of multiple scans; put each set of files in a separate 1st-level subdirectory of the specified directory.

RAPID7 NEXPOSE SCANNER

You can add or update vulnerability occurrence data from Rapid7 Nexpose scanners to the current model:

- Using an online collection task:
  - Configure a scanner (see page 226) to permit access from a Skybox Collector and create a collection task (see page 227) to collect the vulnerability occurrence data and add it to the model.
- Using an offline file import task:
  - Retrieve scanner audit reports and import their data into the model (see page 228).

    The file import task can import the data of multiple scanners.

Configuring Rapid7 Nexpose scanners for data collection

To configure a Rapid7 Nexpose scanner for data collection:

- Configure the Rapid7 scanner to generate reports on a continuous basis.

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Note: Reports for Skybox data collection must be generated and owned by this user. Skybox cannot access reports owned by other users.

To configure a Rapid7 scanner to generate reports

1. In the Nexpose web interface, select **Create a report**.
2. Type a name for the report in the **Name** field.
3. In the Template area:
   a. Select **Export**.
   b. Select **XML Export 2**.
4. In the Scope area, select **Selected Sites**.
5. In the **Frequency** field, select **Run a recurring report after every scan**.
6. Click **Save & run the report**.
7. (Optional) Type all or part of the report name in the **Filter By Name** field in the **Advanced** tab of the **Scanners – Rapid7 Collection** task.

Connection type

Scanners – Rapid7 Collection tasks use a web service to connect to Rapid7 Nexpose scanners.

Rapid7 Nexpose collection tasks

Scanners – Rapid7 Collection tasks retrieve vulnerability occurrence data (audit reports) collected by a Rapid7 Nexpose scanner and add this data to the current model.

Task properties

The properties that control **Scanners – Rapid7 Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Scanner IP	The IP address and port of the Rapid7 Nexpose scanner, with the format `nnn.nnn.nnn.nnn:<port>`. **Note**: The default port *of the scanner* is 3780.
Username	The user name to access the scanner.
Password	The user password.
Advanced tab	
Recency	Collect reports generated in the specified number of days before today.
Filter By Name	If you provide a full or partial report name, only reports with names matching this string are imported. Wildcards are supported.

Property	Description
Filter By Format	If you provide a format, only reports in this format are imported. Possible formats are: • ns-xml • (Recommended) raw-xml • qualys-xml
Filter By Template	If you provide a template type, only reports using this template are imported. Possible templates are: • audit-report • full-audit
Filter By API Version	If you provide an API version, only reports using this API version are imported.
Merge Host From The Same Scan	
Strict certificate validation	Specifies whether to force SSL certificate authentication
Use Proxy	Specifies whether to use HTTP proxy settings.
Proxy Address	Only required if you select **Use Proxy**. Configuration of the proxy that the task must use to connect to the scanner.
Proxy Username	
Proxy Password	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.

Importing Rapid7 Nexpose audit reports

Note: We recommend that you use an **Import – Directory** task to import the audit reports.

You can import Rapid7 Nexpose audit reports in:

- ns-xml
- raw-xml
- qualys-xml

You can import multiple audit reports; put each set of files in a separate 1st-level subdirectory of the specified directory.

TENABLE NETWORK SECURITY NESSUS SCANNER

You can add or update vulnerability occurrence data from Tenable Network Security Nessus scanners to the current model.

- Using an online collection task:
  - Configure a scanner (see page 229) to permit access from a Skybox Collector and create a task (see page 229) to execute a scan, collect the

vulnerability occurrences found by the scanner, and add the vulnerability occurrence data to the model.

- Using an offline file import task:
  - Generate scanner vulnerability occurrence files and import their data into the model (see page 230).

    The file import task can import the data of multiple scanners.

You can create a blacklist of scanner IDs (see page 236) that Skybox ignores.

Configuring Nessus scanners for data collection

To configure a Nessus scanner for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Scanners – Nessus Collection tasks use a web service to connect to Nessus scanners.

Tenable Network Security Nessus collection tasks

Scanners – Nessus Collection tasks retrieve vulnerability occurrence data collected by a Tenable Network Security Nessus scanner and add this data to the current model.

Task properties

The properties that control **Scanners – Nessus Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Scanner URL	The URL of the Tenable Network Security Nessus scanner, with the format `https://<Nessus host name>[:<port>]`. The default port is 8834
Username	The user name to access the scanner.
Password	The user password.
Nessus Version	The Nessus version running on the scanner: • **5**: Version 5 • **6**: Version 6 or higher
Advanced tab	
Recency	Collect reports generated in the specified number of days before today.
Filter By Name	If you provide a full or partial report name, only reports with names matching this string are imported. Wildcards are supported.

Property	Description
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.) The location of the debug log file. If this field is empty, the task does not save debug messages.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.

Importing Tenable Network Security Nessus scanner data

Note: We recommend that you use an **Import – Directory** task to import the scan data.

The following file is required to import Nessus scanner data:

- `*.nessus`: Nessus XML file

  Note: For an **Import – Basic** task change the extension from `.nessus` to `.xml`.

You can import the results of multiple scans.

TENABLE NETWORK SECURITY TENABLE.IO

You can add or update vulnerability occurrence data from Tenable Network Security Tenable.io to the current model using an online collection task:

- Configure Tenable.io (see page 230) to permit access from a Skybox Collector and create a collection task (see page 230) to collect the Nessus scans found by Tenable.io and add the vulnerability occurrence data to the model.

You can create a blacklist of scanner IDs (see page 236) that Skybox ignores.

Configuring Tenable.io for data collection

To configure Tenable.io for data collection:

- Skybox data collection requires a read-only user on the Tenable.io; we recommend that you create a separate user for this purpose.

Connection type

Scanners – Tenable.io Collection tasks use a web service to connect to Tenable.io.

Tenable Network Security Tenable.io collection tasks

Scanners – Tenable.io Collection tasks retrieve Nessus scans collected from Tenable Network Security Nessus scanners managed by Tenable Network Security Tenable.io and add the vulnerability occurrence data to the current model.

The following scan result types are supported:

- Basic scan
- Host discovery
- Advanced scan

Task properties

The properties that control **Scanners – Tenable.io Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	The name or IP address of Tenable.io.
Access key	The Tenable.io access key ID.
Secret key	The Tenable.io secret access key.
Filter	
Filter by	Specifies the filter to use when collecting scan files.
Filter value	This field is displayed if **Filter by** = **NAME** or **Filter by** = **ID**. • (**Filter by** = **NAME**) A comma-separated list of the names of the scans to collect. Use the character ***** for standard pattern matching. • (**Filter by** = **ID**) A comma-separated list of the exact IDs of the scans to collect.
Recency	This field is displayed if **Filter by** = **NO FILTER** or **Filter by** = **NAME**. • An integer: Collect scans generated in the specified number of days before today. • A date range: Collect scans generated between the specified dates. Use American date format (MM/dd/yyyy-MM/dd/yyyy).
Proxy	
Use Proxy	Specifies whether to use HTTP proxy settings. The proxy settings are set in the Options dialog box (see the Proxy Settings (Server) topic in the Skybox Installation and Administration Guide).
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the scanners. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.

TENABLE NETWORK SECURITY TENABLE.SC

You can add or update vulnerability occurrence data from Tenable Network Security Tenable.sc to the current model using an online collection task:

- Configure Tenable.sc (see page 232) to permit access from a Skybox Collector and create a collection task (see page 232) to collect the Nessus scans found by Tenable.sc and add the vulnerability occurrence data to the model.

You can create a blacklist of scanner IDs (see page 236) that Skybox ignores.

Configuring Tenable.sc for data collection

To configure Tenable.sc for data collection:

- Skybox data collection requires a read-only user on the Tenable.sc; we recommend that you create a separate user for this purpose.

Connection type

Scanners – Tenable SecurityCenter Collection tasks use a web service to connect to Tenable.sc.

Tenable Network Security Tenable.sc collection tasks

Scanners – Tenable SecurityCenter Collection tasks retrieve Nessus scans collected from Tenable Network Security Nessus scanners managed by Tenable Network Security Tenable.sc and add the vulnerability occurrence data to the current model.

Task properties

The properties that control **Scanners – Tenable SecurityCenter Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or IP	The name or IP address of Tenable.sc.
Username	The user name to access Tenable.sc.
Password	The user password.
Filter	
Filter by	Specifies the filter to use when collecting scan files.
Filter value	This field is displayed if **Filter by** = **NAME** or **Filter by** = **ID**. • (**Filter by** = **NAME**) A comma-separated list of the names of the scans to collect. Use the character ***** for standard pattern matching. • (**Filter by** = **ID**) A comma-separated list of the exact IDs of the scans to collect.
Recency	This field is displayed if **Filter by** = **NO FILTER** or **Filter by** = **NAME**. • An integer: Collect scans generated in the specified number of days before today. • A date range: Collect scans generated between the specified dates. Use American date format (MM/dd/yyyy-MM/dd/yyyy).
Proxy	

Property	Description
Use Proxy	Specifies whether to use HTTP proxy settings. The proxy settings are set in the Options dialog box (see the Proxy Settings (Server) topic in the Skybox Installation and Administration Guide).
Scan results	This field is displayed if **Filter by** = **NO FILTER** or **Filter by** = **NAME**. Specifies whether to use only successfully completed scans or all usable scans regardless of their status.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the scanners. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.

TRIPWIRE IP360 SCANNER

You can add or update vulnerability occurrence data from Tripwire IP360 (nCircle) scanners to the current model:

- Using an online collection task:
  - Configure a Tripwire IP360 VnE Manager (see page 233) to permit access from a Skybox Collector and create a collection task (see page 233) to collect the vulnerability occurrences from the Manager and add the vulnerability occurrence data to the model.
- Using an offline file import task:
  - Generate scanner vulnerability occurrence files and import their data into the model (see page 226).

    The file import task can import the data of multiple scanners.

You can create a blacklist of scanner IDs (see page 236) that Skybox ignores.

Configuring Tripwire IP360 scanners for data collection

To configure a Tripwire IP360 scanner for data collection:

- Skybox data collection requires a read-only user on the Tripwire IP360 VnE Manager server; we recommend that you create a separate user for this purpose.

Tripwire IP360 collection tasks

Scanners – Tripwire IP360 Collection tasks retrieve vulnerability occurrence data collected by Tripwire IP360 scanners and add this data to the current model.

Task properties

The properties that control **Scanners – Tripwire IP360 Collection** tasks are described in the following table.

Property	Description
Basic tab	
Management Name or IP	The name or IP address of the Tripwire IP360 VnE Manager.
Username	A user name to access the Tripwire server.
Password	The user password.
Filter	
Filter by scan ID	A comma-separated list of scan IDs.
Recency	• An integer: Collect scans generated in the specified number of days before today. • A date range: Collect scans generated between the specified dates. Use in American date format (MM/dd/yyyy-MM/dd/yyyy).
Advanced tab	
File format	The format of the files to be generated by the task.
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.

Importing Tripwire IP360 scanner data

Note: We recommend that you use an **Import – Directory** task to import the scan data; the files for each XML3 device (or XML2 device if you are including the ASPL file) must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import Tripwire IP360 (nCircle) scan results (the ASPL file contains vulnerability definitions):

- For nCircle XML3:
  - `scan.xml`: nCircle XML3 scan report
  - `aspl.xml`: nCircle ASPL file

  You can import the results of multiple scans; put each set of files in a separate 1st-level subdirectory of the specified directory.

- For nCircle XML2:
  - `*.xml`: nCircle XML2 scan report
  - (Optional) `aspl.xml`: nCircle ASPL file

  You can import the results of multiple scans; if you are including the ASPL file, put each set of files in a separate 1st-level subdirectory of the specified directory.

Note: If you are using an **Import – Directory** task and importing multiple scans, we recommend that you specify a single location for the ASPL XML file (in the **Tripwire ASPL File** field of the task) so that the file is only parsed once by Skybox. For additional information, see Import directory tasks (on page 39).

Creating IP360 files for import

To create and download a scan report file

1 Log in to Tripwire IP360

2 Navigate to **Discover** > **Scan History**.

3 Next to the relevant scan type, click **export**.

4 Select the relevant export format and click **export**.

5 Click **view** to download the file.

To download an ASPL file

1 Log in to Tripwire IP360

2 Navigate to **Administer** > **Support** > **Resources**.

3 Select the relevant ASPL file and download it.

4 If the file has a **.**gz extension, unzip the file.

WHITEHAT SENTINEL SCANNER

You can add or update vulnerability occurrence data from WhiteHat Sentinel scanners to the current model using an online collection task:

- Configure a scanner (see page 235) to permit access from a Skybox Collector and create a collection task (see page 235) to collect the vulnerability occurrences found by the scanner and add the vulnerability occurrence data to the model.

Configuring WhiteHat Sentinel scanners for data collection

To configure a WhiteHat Sentinel scanner for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Scanners – WhiteHat Sentinel Collection tasks use a REST API to connect to WhiteHat Sentinel scanners.

WhiteHat Sentinel collection tasks

Scanners – WhiteHat Sentinel Collection tasks retrieve vulnerability occurrence data collected by WhiteHat Sentinel scanners and add this data to the current model.

Task properties

The properties that control **Scanners – WhiteHat Sentinel Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
WhiteHat Site	The URL of the WhiteHat server.
User API Key	Your WhiteHat API key.
Advanced tab	
Verify Certification	Specifies whether to check that the CA signed the scanner CA certificate.
Use Proxy	Specifies whether to use HTTP proxy settings.
Proxy Address	Only required if you select **Use Proxy**. Configuration of the proxy that the task must use to connect to the scanner.
Proxy Username	
Proxy Password	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the scanner. **Note**: Use this property if different locations use the same set of IP addresses, so that scanners at different locations can have the same IP address.

BLACKLISTS

Not all information found by vulnerability scanners is about vulnerability occurrences, some is about the asset or its services (for example, the number of users and the number of shares) and some is information that the scanner needs but has no additional value. Skybox does not use this information for attack simulation.

This section describes how to exclude unnecessary scanner information from the model.

The Skybox Vulnerability Dictionary includes a predefined *blacklist*—a list of scanner IDs that contain irrelevant information and so should not be translated into vulnerability occurrences in the model. You can create a blacklist file for a scanner that lists additional scanner IDs to ignore.

Store blacklist files on the Skybox Server machine, in `<Skybox_Home>\data\specials`

Creating blacklists

The scanners for which Skybox supports blacklists are listed in the following table. A separate text file is required for each scanner type.

Scanner	File name
Nessus	nessus
IBM Internet Scanner	iss
Retina	retina
Qualys	qualys
McAfee Vulnerability	foundscan

Scanner	File name
Manager (Foundstone)	
Tripwire IP360 (nCircle)	ncircle

Note: Skybox ignores files with other names.

To create a blacklist for a scanner

1. Create a text file named according to the scanner type. The file name must not have an extension.

   If a file with the name of your scanner exists, you can modify it or add extra lines.

2. In the text file, add a separate line for each scanner ID with the format `<scanner ID><space><action>[<space><regular expression>]`

   Note: For blacklists, the regular expression is not case-sensitive.

   <action> can be:

   - DELETE: Delete all appearances of this scanner ID from the network model.
   - IGNORE: Create vulnerability occurrences for a scanner with this ID with the system life-cycle status **Suspected False Positive**.

   You can use a *regular expression* to select between scanner results produced by the same scanner check. For example, if scanner check 1234 can produce 2 different results: “Vulnerability occurrence is found” and “Maybe vulnerability occurrence is found”, add

```
1234 IGNORE Maybe
```

   Skybox ignores scanner ID 1234 if its result matches the regular expression “Maybe”.

   Do *not* set off the regular expression with quotation marks.

3. Use “;” at the start of a line to add a comment.

4. Save the file.

Using blacklists

Skybox applies blacklists to filter new scanner data that is imported into Skybox; data that is already in the model is not affected.

To delete or ignore scanner IDs that exist in the current model

› Run the **Dictionary Update – Daily** task.

  This task:

  - Retrieves the latest Vulnerability Dictionary from the internet
  - Checks all vulnerability occurrences in the model against blacklists and updates the model accordingly

Note: Loading a model (using **File** > **Models** > **Load**) does not check vulnerability occurrences against the blacklists. If you load a saved model that contains vulnerability occurrences specified in the blacklists, these vulnerability occurrences are part of that model until you run the **Dictionary Update – Daily** task on the loaded model.

Chapter 9

Cloud and virtualization tasks

This chapter describes how to add data from the cloud and virtualized devices to the current model.

In this chapter

AMAZON WEB SERVICES

You can add or update device and asset configuration data from Amazon Web Service accounts to the current model using an online collection task:

- Configure the service (see page 239) to permit access from Skybox and create a collection task (see page 240) to collect the configuration data and add it to the model.

Configuring Amazon Web Services for data collection

To configure Amazon Web Services for data collection:

- (Recommended) Create a separate access key (access key ID and secret access key pair) for Skybox data collection.

  Note: Amazon recommends that you use IAM access keys and not AWS root account access keys. For information about Amazon access keys, see http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSGettingStartedGuide/AWSCredentials.html

- Skybox data collection requires a user with read-only access permissions; we recommend that you create a separate user for this purpose.
  - In the AWS Console, apply the IAM Managed Policy named **ReadOnlyAccess**. This policy grants read-only access to active resources on most AWS services.

    Note: The minimum user permissions for Skybox data collection are **AWSDirectConnectReadOnlyAccess** and **AmazonEC2ReadOnlyAccess**.

- The system clock in the machine running the Skybox Collector must be synchronized:

- The clock time must match the time zone specified in the OS.
- The clock time must be correct.

Connection type

Cloud & Virtualization – Amazon Web Services Collection tasks use Amazon Web Services over HTTPS to connect to Amazon Web Services data centers.

API methods used by task

Cloud & Virtualization – Amazon Web Services Collection tasks use the following API methods:

- `directconnect:OvertureService.DescribeVirtualGateways`
- `directconnect:OvertureService.DescribeVirtualInterfaces`
- `ec2:DescribeAddresses`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeTags`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpnConnections`
- `ec2:DescribeVpnGateways`
- `elb:DescribeLoadBalancers`

Amazon Web Services collection tasks

Cloud & Virtualization – Amazon Web Services Collection tasks retrieve device and asset configuration data from an Amazon Web Services (AWS) data center and add this data to the current model.

Note: The task collects ec2 tags; these are added to the model as custom business attributes (see the Business attributes section in the Skybox Firewall Assurance User Guide).

These tasks support:

- Virtual Private Clouds (see the Virtualization and clouds topic in the Skybox Vulnerability Control User Guide or in the Skybox Network Assurance User Guide)

- Elastic Load Balancing

Task properties

The properties that control **Cloud & Virtualization – Amazon Web Services Collection** tasks are described in the following table.

Note: This task must run on a Skybox Collector, not on the Server.

Property	Description
Basic tab	
Access Key	The Amazon access key ID.
Secret Key	The Amazon secret access key.
VPC IDs	A semicolon-separated list of Virtual Private Cloud IDs.
Region	The name of the Amazon data center. Take the value from the following table; use the value in the **Region** column and *not* the value in the **Region name** column.
Use Proxy	Specifies whether to use HTTP proxy settings. The proxy settings are set in the Options dialog box (see the Proxy Settings (Server) topic in the Skybox Installation and Administration Guide).
Session Token	The Amazon session token (for use when the task is only granted temporary security credentials).
Assume Role	Specifies from which accounts to retrieve data. • **Disabled**: Retrieve data from your account only. • **Role List**: Retrieve data from accounts specified in **Assume Role Data**. • **From File**: Retrieve data accounts listed in a JSON file whose location is specified in **Assume Role Data**.
Assume Role Data	(**Assume Role** = **Role List**) A semicolon-separated list of the credentials of the accounts from which to retrieve data. Each set of credentials has the format `<account ID>,<role name>[,<region>]`. (**Assume Role** = **From File**) The path to the JSON file that contains the credentials of the accounts from which to retrieve data.
Advanced tab	
Collect data from files	Specifies whether to import configuration data from files that you downloaded and not directly from an AWS data center. If selected, all fields in the **Basic** tab are ignored.
Raw data path	If you select **Collect data from files**: The full path to the directory containing the configuration data files. The default value is `<Skybox_Home>\data\collector\temp`
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.

Property	Description
Location Hint	The location of the Amazon Web Services data center. **Note**: Use this property if different locations use the same set of IP addresses, so that devices at different locations can have the same IP address.

Supported Amazon EC2 regions and endpoints

Region name	Region	Endpoint
US East (N. Virginia)	us-east-1	ec2.us-east-1.amazonaws.com
US East (Ohio)	us-east-2	ec2.us-east-2.amazonaws.com
US West (Oregon)	us-west-2	ec2.us-west-2.amazonaws.com
US West (N. California)	us-west-1	ec2.us-west-1.amazonaws.com
Asia Pacific (Mumbai)	ap-south-1	ec2.ap-south-1.amazonaws.com
Asia Pacific (Seoul)	ap-northeast-2	ec2.ap-northeast-2.amazonaws.com
Asia Pacific (Singapore)	ap-southeast-1	ec2.ap-southeast-1.amazonaws.com
Asia Pacific (Sydney)	ap-southeast-2	ec2.ap-southeast-2.amazonaws.com
Asia Pacific (Tokyo)	ap-northeast-1	ec2.ap-northeast-1.amazonaws.com
Canada (Central)	ca-central-1	ec2.ca-central-1.amazonaws.com
EU (Ireland)	eu-west-1	ec2.eu-west-1.amazonaws.com
EU (London)	eu-west-2	ec2.eu-west-2.amazonaws.com
EU (Frankfurt)	eu-central-1	ec2.eu-central-1.amazonaws.com
South America (Sao Paulo)	sa-east-1	ec2.sa-east-1.amazonaws.com
GovCloud (US)	us-gov-west-1	ec2.us-gov-west-1.amazonaws.com

CISCO ACI

You can add or update data from a Cisco ACI server to the current model using an online collection task:

- Configure the server (see page 242) to permit access from Skybox and create a collection task (see page 243) to collect the data and add it to the model.

Configuring Cisco ACI for data collection

To retrieve data from Cisco ACI servers:

- We recommend that you create a separate read-all user on each server for Skybox data collection.

Connection type

Cloud & Virtualization – Cisco ACI Collection tasks use a REST API to connect to Cisco ACI servers.

Cisco ACI collection tasks

Cloud & Virtualization – Cisco ACI Collection tasks retrieve data from Cisco ACI servers and add this data to the current model.

Task properties

The properties that control **Cloud & Virtualization – Cisco ACI Collection** tasks are described in the following table.

Property	Description
Server Name or IP	The name or IP address of the server.
Authentication	
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the server.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.

MICROSOFT AZURE CLOUD SERVICES

You can add or update virtual domain configuration data from Microsoft Azure Cloud Service platforms to the current model using an online collection task:

- Configure the platforms (see page 243) to permit access from Skybox and create a collection task (see page 245) to collect the configuration data and add it to the model.

Configuring Azure Cloud Services for data collection

To retrieve data from Azure Cloud Service platforms:

1 You must have an Azure subscription.

2 **Cloud & Virtualization – Azure Collection** tasks requires credentials based on Azure Active Directory service principal functionality.

Get these credentials from the Azure UI.

3 You need **Log Analytics Reader** (or higher) permissions for your app.

To get Azure credentials from the Azure UI

1. Log in to the Azure UI.
2. Get the **Application ID** by creating an app registration:
   a. Select **App registrations** > **New application registration**.
   b. Fill in the fields in the Create pop-up:
      - **Name**: The name of your app (for example, **Skybox–Collection**)
      - **Application Type**: Always set to **Web App/API**
      - **Sign-on URL**: The URL where you sign in to use the app (you can change this later)
   c. Click **Create**.

      Information about the **Skybox–Collection Registered app** is displayed.
   d. Copy the value of the **Application ID** and paste it into the **Client** field of the **Cloud & Virtualization – Azure Collection** task that you are creating.
3. Get the app **Key**:
   a. From **Skybox–Collection Registered app**, select **Settings** > **Keys**.
   b. Fill in the fields in the Passwords pop-up:
      - **Description**: Your description of the key
      - **Expires**: The duration of the key
   c. Click **Save**.

      The key is displayed in the **Value** field.
   d. Copy the key and paste it into the **Key** field of the **Cloud & Virtualization – Azure Collection** task that you are creating.

      Important: Copy this key; after you leave the pop-up, the value is hidden.
4. Get the **Directory ID**:
   a. From **Skybox–Collection Registered app**, select **Azure Active Directory** > **Properties**.
   b. Copy the value of the **Directory ID** and paste it into the **Tenant** field of the **Cloud & Virtualization – Azure Collection** task that you are creating.
5. (Optional) If you are collecting data from 1 subscription, get the **Subscription ID**:
   a. From the main menu, select **Subscription**.

      A list of all subscriptions is displayed.
   b. Copy the value of the relevant **Subscription ID** and paste it into the **Subscription** field of the **Cloud & Virtualization – Azure Collection** task that you are creating.

To assign permissions to your app

1. Log in to the Azure UI.
2. Select **Subscription** > **<Subscription Name>** > **Access control (IAM)**.
3. Fill in the fields in the Add permissions pop-up:
   a. **Role**: The permissions to assign to your app (select **Log Analytics Reader** (or higher))
   b. **Select**: The name of your app (select from the drop-down list)

      The app is added to the **Selected members** list.
4. Click **Save**.

Connection type

Cloud & Virtualization – Azure Collection tasks use a web service to connect to Azure Cloud Service platforms.

API methods used by task

Cloud & Virtualization – Azure Collection tasks use the following API methods:

- `azure.loadBalancers`
- `azure.networkSecurityGroups`
- `azure.networkInterfaces`
- `azure.publicIPAddresses`
- `azure.virtualMachines`
- `azure.networks`
- `azure.subscriptions`

Microsoft Azure Cloud Services collection tasks

Cloud & Virtualization – Azure Collection tasks retrieve virtual domain configuration data from an Azure Cloud Service platform and add this data to the current model.

For information about modeling of virtual domains, see the Virtualization and clouds topic in the Skybox Vulnerability Control User Guide or in the Skybox Network Assurance User Guide.

Task properties

The properties that control **Cloud & Virtualization – Azure Collection** tasks are described in the following table.

Note: This task must run on a Skybox Collector, not on the Server.

Property	Description
Basic tab	
Tenant	Take values for these properties (*Directory ID*, *Application ID*, and *Key* respectively) from the Azure service principal-based authentication file that you created for the task (see Configuring Azure Cloud Services for data
Client	

Property	Description
Key	collection (on page 243)).
Collect all subscriptions	Specifies whether to collect data for all subscriptions.
Subscription	If **Collect all subscriptions** is cleared, collect data from this *Subscription ID* (see Configuring Azure Cloud Services for data collection (on page 243)).
Use Proxy	Specifies whether to use HTTP proxy settings. The proxy settings are set in the Options dialog box (see the Proxy Settings (Server) topic in the Skybox Installation and Administration Guide).
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the Azure Cloud Service platform. **Note**: Use this property if different locations use the same set of IP addresses, so that Azure platforms at different locations can have the same IP address.

VMWARE NSX AND VSPHERE

You can add or update network and device configuration data from VMware NSX Manager and vSphere vCenter servers to the current model using an online collection task:

- Configure the servers (see page 246) to permit access from Skybox and create a collection task (see page 247) to collect the configuration data and add it to the model.

Configuring VMware NSX and vSphere for data collection

To retrieve data from VMware NSX Manager and vSphere vCenter servers:

- Skybox data collection requires a read-only (Auditor) user on each server; we recommend that you create separate users for this purpose.

Creating a user in NSX

To create a user in NSX

1 Create the new user in the NSX Manager:

a. Connect to the NSX Manager via SSH.

b. Create the new user by running the following command:

```
user <new user> password plaintext <new password>
```

c. Grant the new user the `web-interface` privilege by running the following command:

```
user <new user> privilege web-interface
```

d. Log out of the NSX Manager.

2 On a Linux machine, grant the new user CLI privileges via the API:

Important: Do *not* add the user as an Auditor in the Web Client.

a. Create a file, `<new file>.xml`, to serve as the body of the POST command in the following step.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<accessControlEntry>
   <role>auditor</role>
   <resource>
      <resourceId>globalroot-0</resourceId>
   </resource>
</accessControlEntry>
```

b. Enable CLI privileges by running the following command:

```
curl -i -k -u '<admin name>:<admin password>' -H "Content-
Type:application/xml" -X POST --data "@<new file>.xml"
https://<NSX manager IP>/api/2.0/services/usermgmt/role/skybox-
readonly?isCli=true
```

The response is an HTTP 204 No Content status.

c. To confirm CLI privileges, run the following command:

```
curl -i -k -u 'admin:password' -X GET https://<NSX manager
IP>/api/2.0/services/usermgmt/user/skybox-readonly
```

The (XML) response includes the line: `[isCli]true[/isCli]`

Creating a user in vSphere

For information about creating a user in vSphere, see: https://kb.vmware.com/s/article/2082641.

Connection type

Cloud & Virtualization – NSX and vSphere Collection tasks use web services to connect to VMware NSX Manager and vSphere vCenter servers.

VMware NSX and vSphere collection tasks

Cloud & Virtualization – NSX and vSphere Collection tasks retrieve networking configuration data and firewall configuration data, including micro-segmentation and asset data, from VMware NSX Manager and vSphere vCenter servers, and add this data to the current model.

For information about modeling of tenants, see the Virtualization and clouds topic in the Skybox Vulnerability Control User Guide or in the Skybox Network Assurance User Guide.

Task properties

The properties that control **Cloud & Virtualization – NSX and vSphere Collection** tasks are described in the following table.

Note: This task must run on a Skybox Collector, not on the Server.

Property	Description
Basic tab	
NSX IP Address	The name or IP address of the VMware NSX Manager

Property	Description
	server.
NSX Username	The user name to access the NSX Manager server.
NSX Password	The NSX Manager user password.
vSphere IP Address	The name or IP address of the VMware vSphere vCenter server.
vSphere Username	The user name to access the vSphere vCenter server.
vSphere Password	The vSphere vCenter user password.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the VMware server. **Note**: Use this property if different locations use the same set of IP addresses, so that VMware servers at different locations can have the same IP address.

VMWARE NSX-T DATA CENTER

You can add or update NSX-T edge gateway configuration data from a VMware NSX-T Data Center to the current model using an online collection task:

- Configure the Data Center (see page 248) to permit access from Skybox and create a collection task (see page 248) to collect the configuration data and add it to the model.

Configuring VMware NSX-T Data Centers for data collection

To retrieve data from VMware NSX-T Data Centers:

To configure a VMware NSX-T Data Center for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Cloud & Virtualization – NSX-T Data Center tasks use the NSX-T REST API to connect to VMware NSX-T Data Centers.

VMware NSX-T Data Center collection tasks

Cloud & Virtualization – NSX-T Data Center tasks retrieve retrieve firewall and NAT configuration data from NSX-T edge gateways and add this data to the current model.

Task properties

The properties that control **Cloud & Virtualization –NSX-T Data Center** tasks are described in the following table.

Property	Description
Basic tab	
Run In	Where to run the data collection.
Authentication Method	The authentication to use when connecting to the NSX-T Data Center.
NSX Manager URL	The URL of the NSX Manager node.
Username	The user name to access the NSX-T Data Center.
Password	The user password.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the VMware Data Center. **Note**: Use this property if different locations use the same set of IP addresses, so that VMware Data Centers at different locations can have the same IP address.

Chapter 10

Management systems tasks

This chapter describes how to add data from management systems to the current model.

In this chapter

BMC BLADELOGIC NETWORK AUTOMATION

You can add or update network device configuration data from a BMC BladeLogic Network Automation (BNA) database to the current model using an online collection task:

- Configure the database (see page 250) to permit access from Skybox and create a collection task (see page 251) to collect the configuration data and add it to the model.

Configuring BMC BladeLogic Network Automation for data collection

To retrieve data from a BMC BladeLogic Network Automation (BNA) database:

- Skybox requires read-only access to the BNA database

Connection type

Asset Management – BNA Collection tasks use a web service to connect to BNAs.

BMC BladeLogic Network Automation collection tasks

Asset Management – BNA Collection tasks retrieve network device configuration data from a BMC BladeLogic Network Automation (BNA) database and add this data to the current model.

Task properties

The properties that control **Asset Management – BNA Collection** tasks are described in the following table.

Property	Description
Basic tab	
Web App URL	
Username	The user name to access the BNA database.
Password	The user password.
Name Filter	
Device Type Filter	The vendor of the devices whose configuration data is to be imported into the model.
Group Filter	The group whose device configuration data is to be imported into the model.
Realm Filter	The realm whose device configuration data is to be imported into the model.
Filter List	
Filter Operator	• **Exclude**: Exclude the device type specified by **Exclude Category**. • **Include**: Only import the configuration data of the device type specified by **Exclude Category**.
Exclude Category	The device type whose data is to be imported or excluded (according to the value of **Filter Operator**).
Advanced tab	
Supported Trail UID	
Collection Artifact in Single File	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the BNA database. **Note**: Use this property if different locations use the same set of IP addresses, so that BNA databases at different locations can have the same IP address.

FORESCOUT

You can add or update data from a Forescout database to the current model using an online collection task:

- Configure the Forescout database (see page 252) to permit access from Skybox and create a collection task (see page 252) to collect the data and add it to the model.

Configuring Forescout for data collection

To retrieve data from a Forescout database:

- Skybox requires access to the Forescout database. You can use the predefined Administrator, but we recommend that you create a separate user for data collection by cloning the Administrator user.

Connection type

Asset Management – Forescout Collection tasks use a proprietary Forescout API to connect to Forescout databases.

API calls used by task

Asset Management – Forescout Collection tasks use the following Forescout API calls:

- `generateTokenRestRequest`
- `retrieveActiveEndpointsRestRequest`
- `retrieveSpecifiedHostPropertyValuesByIPForEndpointRestRequest`
- `retrieveSpecifiedHostPropertyValuesByIDForEndpointRestRequest`
- `retrieveSpecifiedHostPropertyValuesByMACForEndpointRestRequest`

Forescout collection tasks

Asset Management – Forescout Collection tasks retrieve device data from a Forescout database and add this data to the current model.

Task properties

The properties that control **Asset Management – Forescout Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server IP	The IP address of the server holding the Forescout database, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 443.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the database.

Property	Description
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Location Hint	The location of the database server. **Note**: Use this property if different locations use the same set of IP addresses, so that servers at different locations can have the same IP address.

HPE NETWORK AUTOMATION

You can add or update network device configuration data from an HPE Network Automation (HPNA) database to the current model using an online collection task:

- Configure the database (see page 253) to permit access from Skybox and create a collection task (see page 254) to collect the configuration data and add it to the model.

Configuring HPE Network Automation for data collection

To retrieve data from an HPE Network Automation (HPNA):

- Skybox requires read-only access to the HPNA

Cisco IOS and Cisco Nexus

By default, HPNA executes `sh run` on these devices. This command returns the major version of installed software, which is insufficient input for the Vulnerability Detector algorithm.

HPNA permits additional commands to be added as *Diagnostics*.

To configure HPNA to collect Cisco IOS and Cisco Nexus data

1. Open the HPNA UI, and, from the main menu, select **Devices** > **Inventory** > **Device Tools**.
2. Provide a name for the Diagnostics.

   When you configure the Skybox HPNA collection task, enter this name in **Route Diagnostic Name** in the **Advanced** tab.
3. Select the **Mode**: **Cisco IOS enable**.
4. In the **Command Box**, add the following commands in the order given here:

   a. `sh conf | include hostname`

   b. `sh ver` (use this exact format)

c. `show ip route vrf *`

Connection type

Asset Management – HPNA Collection tasks use a web service to connect to HPNAs.

HPE Network Automation collection tasks

Asset Management – HPNA Collection tasks retrieve network device configuration data from an HPE Network Automation (HPNA) and add this data to the current model.

Task properties

The properties that control **Asset Management – HPNA Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Server	The name or IP address of the HPNA.
Username	The user name to access the HPNA.
Password	The user password.
WSDL	The location of the WSDL definition file, `hpna.wsdl`. If this field is empty, Skybox uses the basic WSDL file located in `<Skybox_Home>\intermediate\bin\collectors\System_Management\hpna`.
Filter	Specifies the filter to use for **Filter List**.
Filter List	To retrieve all devices, set this field to **All**. • (**Mode** = **Groups**) A comma-separated list of groups whose configuration data is to be retrieved. • (**Mode** = **Hosts**) A comma-separated list of assets whose configuration data is to be retrieved. • (**Mode** = **Regex**) Retrieve configuration data of devices that match the regex.
Advanced tab	
Device Vendor	The vendor of the devices whose configuration data is to be imported into the model.
Route Diagnostic Name	The (HPE) diagnostic name, required if routing rules are to be imported into the model.
Filter Operator	Specifies whether to include or exclude the device types listed in **Device Type Filter**.
Device Type Filter	A semicolon-separated list of device types to collect or exclude from collection (depending on the value of **Filter Operator**).
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the HPNA. **Note**: Use this property if different locations use the

Property	Description
	same set of IP addresses, so that HPNAs at different locations can have the same IP address.

IBM BIGFIX

You can add or update data from an IBM BigFix database to the current model using an online collection task:

- Configure the BigFix database (see page 255) to permit access from Skybox and create a collection task (see page 255) to collect the data and add it to the model.

Configuring IBM BigFix for data collection

To retrieve data from an IBM BigFix database:

- Skybox requires read-only access to the BigFix database

Connection type

Asset Management – BigFix Collection tasks use a REST API to connect to BigFix databases.

IBM BigFix collection tasks

Asset Management – BigFix Collection tasks retrieve data (asset information, vulnerability occurrences and installed patches, and installed software) from an IBM BigFix database and add this data to the current model.

Task properties

The properties that control **Asset Management – BigFix Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server IP	The name or IP address of the BigFix database server, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 52311.
Username	A BigFix console user name.
Password	The BigFix console password for **Username**.
Advanced tab	
Include only assets in specified file	The full path to a text file that contains a list of device names of assets (1 per line). The task collects data for assets with the listed device names only.
Maximum number of assets to collect	The maximum number of assets that the task collects. If this field is empty or set to **0**, all assets are collected.
Collect patches per host	Specifies whether to collect patches per asset
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.

Property	Description
Location Hint	The location of the database server. **Note**: Use this property if different locations use the same set of IP addresses, so that database servers at different locations can have the same IP address.

IBM Z/OS

You can add or update configuration data from IBM z/OS mainframes to the current model using an online collection task:

- Export the data from z/OS, save the files for each asset in a separate subdirectory of a selected directory, and create a collection task (see page 256) to import the data and add it to the model.

IBM z/OS collection tasks

Asset Management – z/OS Collection tasks retrieve configuration data from an IBM z/OS mainframe and add this data to the current model.

Task properties

The properties that control **Asset Management – z/OS Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Input Hosts Directory	The location of the configuration files from z/OS. The files must be in 1st-level subdirectories of the specified directory (1 subdirectory per asset).
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the IBM z/OS mainframe. **Note**: Use this property if different locations use the same set of IP addresses, so that mainframes at different locations can have the same IP address.

INFOBLOX NETMRI

You can add or update network metadata (NetMRI Extensible Attributes) from an Infoblox NetMRI to the current model using an online collection task:

- Configure the NetMRI (see page 256) to permit access from Skybox and create a collection task (see page 258) to collect the data and add it to the model.

Configuring Infoblox NetMRI for data collection

To retrieve data from an Infoblox NetMRI:

- Skybox data collection requires a read-only user on the NetMRI; we recommend that you create a separate user for this purpose.

To create a Skybox read-only user in Infoblox

1 Log in to the Infoblox UI.

2 Create an Admin Group for use with Skybox:

a. Navigate to **Administration** > **Administrators** > **Groups**.

b. Select **Create New Admin Group**.

c. In the 1st page of the Add Admin Group Wizard, type a **Name** for the group.

For example, `Skybox read-only`.

d. There is no need to make any changes in the other pages of the Wizard; click **Save & Close**.

3 Assign read-only permissions to the group:

a. Navigate to **Administration** > **Administrators** > **Permissions**.

b. Select **Create New Permission**.

c. In the Manage Global Permissions dialog box:

i. Select **Group Permission** and, from the drop-down list, select the Admin Group that you created in the previous step (in our example, `Skybox read-only`).

ii. Select **IPAM Permissions** from the **Permissions Type** drop-down list.

iii. Select **Read-Only** for all **Resources/Functions** *except* **Port Control**.

iv. Click **Save & Close**.

4 Add a user for the Skybox collection task:

a. Navigate to **Administration** > **Administrators** > **Admins**.

b. Select **Create New Administrator**.

c. In the 1st page of the Add Administrator Wizard:

i. Provide a user name (in the **Login** field) and password.

These are the user name and password that you will use when you create the Skybox **Network Management – Infoblox NetMRI** task.

ii. Select the Admin Group that you created for use with Skybox (in our example, `Skybox read-only`).

iii. Click **Save & Close**.

Connection type

Network anagement – Infoblox NetMRI tasks use a REST API to connect to NetMRIs.

Infoblox NetMRI collection tasks

Network Management – Infoblox NetMRI tasks retrieve network metadata (NetMRI *Extensible Attributes*—NetMRI network tags) from an Infoblox NetMRI and add this data to the current model (the task uses NetMRI network tags to create or update Skybox zones; one NetMRI Extensible Attribute can be mapped to a Skybox zone with the same name).

Task properties

The properties that control **Network Management – Infoblox NetMRI** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Infoblox Address	The URL of the Infoblox server.
Infoblox Username	The user name to access Infoblox.
Infoblox Password	The Infoblox user password.
Server End Point	The Skybox server IP address and port, with the format `nnn.nnn.nnn.nnn:<port>`. **Note**: There is no default port.
Skybox Username	The user name to access Skybox.
Skybox Password	The Skybox user password.
Zone Field	The (case-sensitive) name of the NetMRI Extensible Attribute to map to a Skybox zone of the same name.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the NetMRI. **Note**: Use this property if different locations use the same set of IP addresses, so that NetMRIs at different locations can have the same IP address.

MCAFEE EPOLICY ORCHESTRATOR

You can add or update data from a McAfee ePolicy Orchestrator (ePO) database to the current model using an online collection task:

- Configure the database (see page 258) to permit access from Skybox and create a collection task (see page 259) to collect the data and add it to the model.

Configuring McAfee ePolicy Orchestrator for data collection

To retrieve data from a McAfee ePolicy Orchestrator (ePO) database:

- Skybox requires read-only access to the ePO database

Connection type

Asset Management – ePO Collection tasks use ODBC to connect to ePO databases.

McAfee ePolicy Orchestrator collection tasks

Asset Management – ePO Collection tasks retrieve configuration data (asset information, vulnerability occurrences and installed patches, and installed software) from a McAfee ePolicy Orchestrator (ePO) database and add this data to the current model.

Task properties

The properties that control **Asset Management – ePO Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Database IP	The IP address of the database server used by the ePO, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 1433.
Database Name	The name of the ePO database to access.
Username	The user name to access the ePO database.
Password	The user password.
Advanced tab	
Include only assets in specified file	The full path to a text file that contains a list of device names of assets (1 per line). The task collects data for assets with the listed device names only.
Collect hosts of type	Specifies the types of assets to collect (as defined in in the ePO database).
Use NTLM v2	Specifies whether to permit authentication using NTLM v2 only. To configure NTLM v2, see the Proxy Settings (Server) topic in the Installation and Administration Guide.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the ePO database. **Note**: Use this property if different locations use the same set of IP addresses, so that ePO databases at different locations can have the same IP address.

MICROSOFT SCCM

You can add or update data from a Microsoft System Center Configuration Manager (SCCM) database to the current model using an online collection task:

- Configure the SCCM database (see page 260) to permit access from Skybox and create a collection task (see page 260) to collect the data and add it to the model.

Configuring Microsoft SCCM for data collection

To retrieve data from a Microsoft SCCM database:

- Skybox requires read-only access to the SCCM database
- For Windows, if you are using Windows authentication (rather than SQL authentication), the user running the task must be the user who is running the Skybox service.
- For Linux, retrieval is only possible if you are using Skybox Appliance, ISO version 6.5.101.87-2.80-6.5.1.47 or higher.
- To retrieve information about software installed on assets, populate the v_GS_INSTALLED_SOFTWARE_CATEGORIZED table in the SCCM database.

To populate the v_GS_INSTALLED_SOFTWARE_CATEGORIZED table

1. Log in to the SCCM database.
2. Navigate to **Asset Intelligence** > **Hardware Inventory**.
3. Enable **SMS_InstalledSoftware**.
4. Run the hardware inventory cycle.

Connection type

Asset Management – SCCM Collection tasks use ODBC to connect to SCCMs.

Microsoft SCCM collection tasks

Asset Management – SCCM Collection tasks retrieve data (asset information, vulnerability occurrences and installed patches, and installed software) from a Microsoft System Center Configuration Manager (SCCM) database and add this data to the current model.

Note: To retrieve information about installed software, populate the v_GS_INSTALLED_SOFTWARE_CATEGORIZED table in the SCCM database (see Configuring Microsoft SCCM for data collection (on page 260)).

The task uses a script that is written in Perl and requires the following Perl modules:

- DBI
- DBD::ODBC
- Parallel::ForkManager

Task properties

The properties that control **Asset Management – SCCM Collection** tasks are described in the following table.

Note: If **Collector Version** = **v2**, the task must run on a Skybox Collector, not on the Server.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Server IP	The name or IP address of the SCCM database server,

Property	Description
	with the format `<server name>[:<port>]` or `nnn.nnn.nnn.nnn[:<port>]`. The default port is 1433.
DSN Name	The Microsoft SQL server name in the DSN. This field is retained for backward compatibility only; use the **Server IP** field. (If you provide values in both fields, the task uses **Server IP**.)
Username	An SCCM database user name. The format depends on the authentication type: • Windows: `domain\user` • SQL: `user`
Password	The SCCM database password for **Username**.
Advanced tab	
Include only assets in specified file	The full path to a text file that contains a list of device names of assets (1 per line). The task collects data for assets with the listed device names only.
Maximum number of assets to collect	The maximum number of assets that the task collects. If this field is empty or set to **0**, all assets are collected.
Number of Threads	The number of threads to use for calculations when running the task.
Use raw version for selected products	Specifies whether to retrieve raw version data for products whose version information is known to be insufficiently granular after SCCM product normalization.
Collect vulnerability	The format in which to collect vulnerabilities.
Support special characters	Specifies whether to support folder names that include non-ASCII characters (for example, French or Japanese).
SCCM DB name	The name of the SCCM database from which to retrieve data.
Collector Version	The version of the collector to use. (Do not change the default unless told to do so by Skybox Professional Services.)
Active Directory Protocol	The protocol to use to connect to Active Directory.
Support NTLMv2	Specifies whether to include support for NTLMv2. To configure NTLM v2, see the Proxy Settings (Server) topic in the Installation and Administration Guide.
Debug (Collector v2 only)	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system `Temp` directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.

Property	Description
Location Hint	The location of the database server. **Note**: Use this property if different locations use the same set of IP addresses, so that database servers at different locations can have the same IP address.

MICROSOFT WSUS

You can add or update data from a Microsoft WSUS (Windows Server Update Services) database to the current model using an online collection task:

- Configure the WSUS database (see page 262) to permit access from Skybox and create a collection task (see page 262) to collect the data and add it to the model.

Configuring Microsoft WSUS for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Windows platform.

To retrieve data from a Microsoft WSUS database:

- The user running the Skybox WSUS collection utility must be part of the WSUS Reporters group.
- To run the Skybox WSUS collection task remotely, the WSUS Administration Console must be installed.
- .NET Framework must be installed on the Skybox Collector.

To download and install the Windows Server Update Services Administration Console (Windows Server 2008)

1. Download Windows Server Update Services 3.0 from http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5216
2. During the installation, select to install the Administration Console only (you do not need the full installation).

To install the Windows Server Update Services Administration Console (Windows Server 2012 and higher)

Note: In Windows Server 2012 and higher, WSUS is integrated with the operating system as a server role.

1. Start the PowerShell Console (as Administrator).
2. Run: `Install-WindowsFeature -Name UpdateServices -Ui`

For a step-by-step (unofficial) guide, go to https://wiseindy.com/it/how-to-set-up-wsus-on-windows-server-2012-r2-a-step-by-step-guide/

Microsoft WSUS collection tasks

Asset Management – WSUS Collection tasks retrieve information from a Microsoft Windows Server Update Services (WSUS) database about the Microsoft updates that are installed on devices and add this information to the current model.

Note: This task supports WSUS on Windows Server 2008, 2008 R2, 2012, 2012 R2, and 2016.

Task properties

The properties that control **Asset Management – WSUS Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Server IP	(Mandatory if you select **Run Locally** in the **Advanced** tab) The name or IP address of the WSUS database server.
Remote Port	(Mandatory if you select **Run Locally** in the **Advanced** tab) The port to which to connect.
Advanced tab	
Filter asset list based on filter file	
Filter asset list based on host name	
Client OS Version	The version of the WSUS client that is installed on the Skybox Collector.
Maximum number of assets to collect	The maximum number of assets that the task collects. If this field is empty or set to **0**, all assets are collected.
Run Locally	Specifies whether to run the collection locally or from the remote client. If you select **Run Locally**, you must specify **Server IP** and **Remote Port** in the **Basic** tab.
Host Only	
FQDN for Hostname	Specifies whether to show the fully qualified domain name (FQDN).
Use SSL	(Relevant only if you select **Run Locally**) Specifies whether to use SSL to connect to the WSUS server.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the database server. **Note**: Use this property if different locations use the same set of IP addresses, so that database servers at different locations can have the same IP address.

RED HAT SATELLITE

You can add or update data from a Red Hat Satellite (version 6 and higher) to the current model using an online collection task:

- Configure the device (see page 264) to permit access from Skybox and create a collection task (see page 264) to collect the data and add it to the model.

Configuring Red Hat Satellite for data collection

Note: Red Hat Satellite collection is supported for version 6 and higher.

To configure a Red Hat Satellite for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Asset Management – Red Hat Satellite Collection tasks use a web service to connect to Red Hat Satellites.

Red Hat Satellite collection tasks

Asset Management – Red Hat Satellite Collection tasks retrieve device configuration data from a Red Hat Satellite and add this data to the current model.

Task properties

The properties that control **Asset Management – Red Hat Satellite Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server IP	The IP address of the Red Hat Satellite.
Username	The user name to access the device.
Password	The user password.
Advanced tab	
Collect unmanaged hosts	Specifies whether to collect the available, limited device configuration data for assets that are not running the Red Hat Update Agent.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the Red Hat Satellite. **Note**: Use this property if different locations use the same set of IP addresses, so that configuration manager servers at different locations can have the same IP address.

SOLARWINDS NCM

You can add or update data from a SolarWinds NCM to the current model using an online collection task:

- Configure the configuration manager server (see page 265) to permit access from Skybox and create a collection task (see page 265) to collect the data and add it to the model.

Configuring SolarWinds NCM for data collection

To retrieve data from a SolarWinds NCM:

- Skybox requires read-only access to the configuration manager server.
- Configure the configuration manager server to permit collection. (The Skybox Collector must have permission to connect to the configuration manager server using HTTPS on port 17778.)

Connection type

Asset Management – SolarWinds NCM Collection tasks use a web service to connect to SolarWinds NCMs (SolarWinds API v2 uses SOAP, API v3 uses a REST API).

SolarWinds NCM collection tasks

Asset Management – SolarWinds NCM Collection tasks retrieve device configuration data from a SolarWinds NCM and add this data to the current model.

Task properties

The properties that control **Asset Management – SolarWinds NCM Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Management Address	The IP address of the SolarWinds configuration manager server.
Username	The user name to access the SolarWinds configuration manager server.
Password	The user password.
Port	The port on which the configuration manager server listens. If you change the default port (17778) on the configuration manager server, the Skybox Collector must have permission to connect to the configuration manager server using HTTPS on the port that you specify.
API Version	The version of the SolarWinds API that the task uses.
Advanced tab	
Recency	Collect configurations saved on the configuration manager server in the specified number of days before today.
Filter by Name	If you provide a full or partial configuration name, only configurations with names matching this string are imported.
Node type Filter Key	Specifies whether to read the device types listed in **Filter Node Type** from the **DeviceTemplate** field or the **Device_Type** field in SolarWinds.

Property	Description
Filter Node Type	A comma-separated list of device types whose configuration data is imported. The device types are read from the field specified by **Node type Filter Key**.
Collect Routing Information	Specifies whether to retrieve device routing information as well as device configuration data.
Collect VRF Routing Information	Specifies whether to retrieve device VRF routing information as well as device configuration data.
Collect VRF Routing From Orion	Specifies whether the SolarWinds NCM is using the SolarWinds Orion platform.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the configuration manager server. **Note**: Use this property if different locations use the same set of IP addresses, so that configuration manager servers at different locations can have the same IP address.

SYMANTEC ALTIRIS

You can add or update data from a Symantec Altiris database to the current model using an online collection task:

- Configure the database (see page 266) to permit access from Skybox and create a collection task (see page 266) to collect the data and add it to the model.

Configuring Symantec Altiris for data collection

To retrieve data from a Symantec Altiris database:

- Skybox requires read-only access to the Altiris database

Connection type

Asset Management – Symantec Altiris Collection tasks use ODBC to connect to Altiris.

Symantec Altiris collection tasks

Asset Management – Symantec Altiris Collection tasks retrieve configuration data (general asset information and installed software) from a Symantec Altiris database and add this data to the current model.

Task properties

The properties that control **Asset Management – Symantec Altiris Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Server IP	The IP address of the Altiris server, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 1433.
DB Name	The name of the Altiris database to access.
Username	The user name to access the Altiris database.
Password	The user password.
Advanced tab	
Include only assets in specified file	The full path to a text file that contains a list of device names of assets (1 per line). The task collects data for assets with the listed device names only.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.

TREND MICRO DEEP SECURITY

You can add or update network device configuration data from a Trend Micro Deep Security management server to the current model using an online collection task:

- Configure the server (see page 267) to permit access from Skybox and create a collection task (see page 267) to collect the configuration data and add it to the model.

Configuring Trend Micro Deep Security for data collection

To retrieve data from a Trend Micro Deep Security management server:

- Skybox requires read-only access to the Deep Security server

Connection type

Asset Management – Trend Micro Deep Security Collection tasks use a web service over HTTPS to connect to Trend Micro Deep Security management servers.

Trend Micro Deep Security collection tasks

Asset Management – Trend Micro Deep Security Collection tasks retrieve network device configuration data from a Trend Micro Deep Security management server and add this data to the current model.

Task properties

The properties that control **Asset Management – Trend Micro Deep Security Collection** tasks are described in the following table.

Property	Description
Basic tab	
Server Name or	The name and port, or IP address and port of the Deep Security server, with the format `<server name>:<port>`

Property	Description
IP	or nnn.nnn.nnn.nnn:<port>. **Note**: There is no default port.
Username	The user name to access the Deep Security server.
Password	The user password.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the BNA database. **Note**: Use this property if different locations use the same set of IP addresses, so that Deep Security servers at different locations can have the same IP address.

TWISTLOCK

You can add or update container information (running container instances and images in the repository) from a Twistlock container security solution to the current model using an online collection task:

- Configure the solution (see page 268) to permit access from a Skybox Collector and create a collection task (see page 268) to collect the data found by the solution and add the data to the model.

Configuring Twistlock for data collection

To configure a Twistlock solution for data collection:

- Skybox data collection requires a read-only user on the solution; we recommend that you create a separate user for this purpose.

Twistlock collection tasks

Containers – Twistlock Collection tasks retrieve container information (running container instances and images in the repository) collected by Twistlock container security solutions and add this data to the current model.

Task properties

The properties that control **Containers – Twistlock Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Twistlock Server	The name or IP address of the Twistlock solution.
Username	The user name to access the solution.
Password	The user password.
Advanced tab	
Endpoint Mapping File	

Property	Description
Certificate File Path	The absolute path to a file containing the Twistlock certificate and key.
Use Token Auth	
Label filters	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the solution. **Note**: Use this property if different locations use the same set of IP addresses, so that solutions at different locations can have the same IP address.

MICROSOFT ACTIVE DIRECTORY

You can add or update device data from a Microsoft Active Directory database to the current model using an online collection task:

- Configure the database (see page 269) to permit access from Skybox and create a collection task (see page 269) to collect the data and add it to the model.

Configuring Microsoft Active Directory for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Windows platform.

To retrieve data from a Microsoft Active Directory (AD) database:

- Skybox requires read-only access to the AD database

Active Directory Automation collection tasks

Asset Management – Active Directory Collection tasks retrieve device data from a Microsoft Active Directory (AD) database and add this data to the current model.

Task properties

The properties that control **Asset Management – Active Directory Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Global Catalog Path	The global catalog path. Make sure that the protocol is *not* part of the path.
Protocol	The protocol used by this AD database.

Property	Description
Username	The user name to access the AD database.
Password	The user password.
Advanced tab	
LDAP Filter	
Search Base Filter File Path	A path to a file that contains search base filters in rows. An example of this file is at `<Skybox_Home>\intermediate\bin\collectors\System_Management\activeDirectory\example\searchBaseFilters.txt`
Discovery Method	
Ignore Unresolved Hosts	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.

CISCOWORKS

CiscoWorks network management system provides:

- Advanced monitoring of network devices
- Configuration capabilities for the network devices
- Management capabilities that simplify network administration

CiscoWorks keeps a repository of configurations for these network devices.

You can export these configurations to files named `<device IP address>.cfg`. The device configuration contained in these files is the equivalent of the information generated by a `show conf` command.

To import these configuration files from CiscoWorks, use:

- An Import – Collector task (see page 51)
- An Import – Advanced task (see page 49) (and set **File Type** to **Cisco Work Configuration**)
- An Import – Collector Advanced task (see page 52) (and set **File Type** to **Cisco Work Configuration**)

Note: **Import – Basic** tasks do not support CiscoWorks.

HP SOFTWARE & SOLUTIONS (OPENVIEW)

HP Software & Solutions Network Node Manager (NNM) is a comprehensive network management system that uses network discovery methods to build a network topology map. The resulting map topology information is stored in a database.

Skybox supports the import of the topology information as formatted by the ovtopodump utility. This utility, part of every standard HP Software & Solutions NNM installation, dumps the HP Software & Solutions topology database into a formatted text file. Skybox reads information about networks, gateways, and assets from this file.

› To extract the HP Software & Solutions topology information to a formatted file that Skybox can import, run:

```
# ovtopodump -CLlsr > output.txt
```

You can import the file generated by the ovtopodump utility using a file import task (any variant: **Basic**, **Advanced**, **Collector**, or **Collector Advanced**, see File import tasks (on page 39)). Set **Format** or **File Type** (depending on the import task) to **HPOV Topology Dump**.

PORTNOX PLATFORM

Skybox includes a script that retrieves Portnox Platform data files and a parser that creates an iXML file from these files. This iXML file can then be imported into Skybox.

The script is `<Skybox_Home>\intermediate\bin\collectors\System_Management\portnox\portnoxCollection.pl`

The parser is `<Skybox_Home>\intermediate\bin\parsers\System_Management\portnox\portnoxParser.pl`

For help using a script, run the script without any arguments.

For additional help, open a case at the Skybox Support portal.

SYMANTEC ENDPOINT MANAGEMENT

Skybox includes a script that retrieves Symantec Endpoint Management data files and parses these files to create an iXML file that you can import into the model.

The script is `<Skybox_Home>\intermediate\bin\collectors\System_Management\symantec\sepManagementCollection.pl`

For help using the script, run the script without any arguments.

For additional help, open a case at the Skybox Support portal.

Chapter 11

Operational technology tasks

This chapter describes how to add operational technology output to the current model.

In this chapter

CLAROTY OPERATIONAL TECHNOLOGY

You can add or update vulnerability occurrence data from Claroty Platforms to the current model using an online collection task:

- Configure the Platforms (see page 272) to permit access from a Skybox Collector and create a collection task (see page 272) to collect the vulnerability occurrences found by the Platforms and add the vulnerability occurrence data to the model.

  The collection task can collect data from multiple Platforms.

Configuring Claroty Platforms for data collection

To configure a Claroty Platform for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Operational Technology – Claroty Collection tasks use a REST API to connect to Claroty Platforms.

Claroty collection tasks

Operational Technology – Claroty Collection tasks retrieve vulnerability occurrence data collected by Claroty Platforms and add this data to the current model.

Task properties

The properties that control **Operational Technology – Claroty Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Server Name or IP	A semicolon-separated list of the names or IP addresses of Claroty Platforms, with the format `<server name>[:<port>]` or `nnn.nnn.nnn.nnn[:<port>]`. The default port is 5000. **Note**: A task can collect the configurations of multiple Platforms only if the same authentication is used for all the Platforms.
Username	The user name to access the Platforms.
Password	The user password.
Advanced tab	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the Platforms. **Note**: Use this property if different locations use the same set of IP addresses, so that Platforms at different locations can have the same IP address.

CYBERX OPERATIONAL TECHNOLOGY

You can add or update vulnerability occurrence data from CyberX platforms to the current model using an online collection task:

- Configure a platform (see page 273) to permit access from a Skybox Collector and create a collection task (see page 273) to collect the vulnerability occurrences found by the platform and add the vulnerability occurrence data to the model.

Configuring CyberX platforms for data collection

To configure a CyberX platform for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Operational Technology – CyberX Collection tasks use HTTPS to connect to CyberX platforms.

CyberX collection tasks

Operational Technology – CyberX Collection tasks retrieve vulnerability occurrence data collected by a CyberX platform and add this data to the current model.

Task properties

The properties that control **Operational Technology – CyberX Collection** tasks are described in the following table.

Property	Description
Basic tab	
Address	The IP address of the CyberX platform.
User Token	The user token to access the CyberX platform.
Advanced tab	
Location Hint	The location of the platform. **Note**: Use this property if different locations use the same set of IP addresses, so that platforms at different locations can have the same IP address.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.

INDEGY OPERATIONAL TECHNOLOGY

You can add or update vulnerability occurrence data from Indegy platforms to the current model using an online collection task:

- Configure the platforms (see page 274) to permit access from a Skybox Collector and create a collection task (see page 274) to collect the vulnerability occurrences found by the platform and add the vulnerability occurrence data to the model.

  The collection task can collect data from multiple platforms.

Configuring Indegy platforms for data collection

To configure an Indegy platform for data collection:

- Create and save a file containing the Indegy certificate and key.
- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Operational Technology – Indegy Collection tasks use a REST API to connect to Indegy platforms.

Indegy collection tasks

Operational Technology – Indegy Collection tasks retrieve vulnerability occurrence data collected by Indegy platforms and add this data to the current model.

Task properties

The properties that control **Operational Technology – Indegy Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A semicolon-separated list of the names or IP addresses of Indegy platforms, with the format `<server name>[:<port>]` or `nnn.nnn.nnn.nnn[:<port>]`. The default port is 23443. **Note**: A task can collect the configurations of multiple platforms only if the same authentication is used for all the platforms.
Certificate full file path	The absolute path, including the file name, to a file containing a concatenation of the Indegy certificate and key.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the platforms. **Note**: Use this property if different locations use the same set of IP addresses, so that platforms at different locations can have the same IP address.

SECURITYMATTERS OPERATIONAL TECHNOLOGY

You can add or update vulnerability occurrence data from SecurityMatters platforms to the current model using an online collection task:

- Configure a platform (see page 275) to permit access from a Skybox Collector and create a collection task (see page 275) to collect the vulnerability occurrences found by the platform and add the vulnerability occurrence data to the model.

Configuring SecurityMatters platforms for data collection

To configure a SecurityMatters platform for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Operational Technology – SecurityMatters Collection tasks use a REST API to connect to SecurityMatters platforms.

SecurityMatters collection tasks

Operational Technology – SecurityMatters Collection tasks retrieve vulnerability occurrence data collected by SecurityMatters platforms and add this data to the current model.

Task properties

The properties that control **Operational Technology – SecurityMatters Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of IP addresses of SecurityMatters platforms. **Note**: A task can collect the configurations of multiple platforms only if the same authentication is used for all the platforms.
Username	The user name to access the platforms.
Password	The user password.
Advanced tab	
Verify Certification	Specifies whether to check that the CA signed the platforms' CA certificates.
Use Proxy	Specifies whether to use HTTP proxy settings.
Proxy Address	Only required if you select **Use Proxy**. Configuration of the proxy that the task must use to connect to the platforms.
Proxy Username	
Proxy Password	
Debug	(Only select this option if Skybox Professional Services has requested a complete debug file.) Specifies whether the task writes a complete debug log. If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the platforms. **Note**: Use this property if different locations use the same set of IP addresses, so that platforms at different locations can have the same IP address.

Chapter 12

Load balancer tasks

This chapter describes how to add load balancer configuration data to the current model.

Load balancers are modeled in Skybox using access and address translation rules.

In this chapter

A10 NETWORKS LOAD BALANCER

You can add or update configuration data from A10 Networks load balancers to the current model:

- Using an online collection task:
  - Configure the load balancers (see page 277) to permit access from a Skybox Collector and create a collection task (see page 278) to collect the load balancer configurations and add the configuration data to the model.

    The collection task can collect data from multiple load balancers.
- Using an offline file import task:
  - Generate and retrieve load balancer configuration files and import their data into the model (see page 279).

    The file import task can import the data of multiple load balancers.

Configuring A10 Networks load balancers for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure an A10 Networks load balancer for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Load Balancers – A10 Collection tasks use the SSH protocol to connect to A10 Networks load balancers.

Commands sent to device

Load Balancers – A10 Collection tasks send the following commands to A10 Networks load balancers:

- `show version | in ACOS`
- One of:
  - (Lower than version 4) `show run all-partitions`
  - (Version 4.0.x) `show partition-config all`
  - (Version 4.1 and higher) `show running-config partition-config all`

  depending on the output of `show version | in ACOS`
- `enable`

  This command is sent only if you provide a value for **Enable password** in the **Advanced** tab of the task.
- `show ip route all`
- `active-partition <partition name>`

A10 Networks collection tasks

Load Balancers – A10 Collection tasks retrieve configuration data from A10 Networks load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – A10 Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the A10 Networks load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the load balancers.

Property	Description
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Use enable mode	Specifies whether to use enable mode for the data collection. • If this field is cleared but there is a value for **Enable Password**, enable mode *is* used. • If this field is selected and **Enable Password** is empty, enable mode is used with an empty password.
Enable Password	The password for enable command privileges on the load balancers.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

Importing A10 Networks configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import an A10 Networks load balancer configuration:

- `*.txt` or `*.log`: The A10 configuration file

  This file is the output of the A10 `show run all-partitions` command.

- (Optional) `route.txt`: Dump of the A10 routing table

  This file is the output of the A10 `show ip route all` command.

  If the A10 Networks load balancer has multiple administrative domains (partitions), run the command once per administrative domain and concatenate the output into a single file.

You can import the configurations of multiple load balancers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

Note: To run an **Import – Collector** task or an **Import – Collector Advanced** task, the Skybox Collector specified for the task must reside on a Linux platform.

BROCADE ADX LOAD BALANCER

You can add or update configuration data from Brocade ADX load balancers to the current model using an online collection task:

- Configure the load balancers (see page 280) to permit access from a Skybox Collector and create a collection task (see page 280) to collect the load balancer configurations and add the configuration data to the model.

  The collection task can collect data from multiple load balancers.

Configuring Brocade ADX load balancers for data collection

To configure a Brocade ADX load balancer for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Load Balancers – Brocade ADX Collection tasks use the SSH protocol to connect to Brocade ADX load balancers.

Commands sent to device

Load Balancers – Brocade ADX Collection tasks send the following commands to Brocade ADX load balancers:

- `skip-page-display`
- `show run`
- `show ip route`
- `show ip mgmt-route`

Brocade ADX collection tasks

Load Balancers – Brocade ADX Collection tasks retrieve configuration data from Brocade ADX load balancers add this data to the current model.

Task properties

The properties that control **Load Balancers – Brocade ADX Collection** tasks are described in the following table.

Property	Description
Basic tab	
Addresses	A comma-separated list of the IP addresses of the Brocade ADX load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Username	The user name to access the load balancers.
Password	The user password.
Advanced tab	
Debug Logger	(Only use this option if Skybox Professional Services has requested a debug file.)

Property	Description
	The location of the debug log file. If this field is empty, the task does not save debug messages.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

CISCO ACE LOAD BALANCER

You can add or update configuration data from Cisco ACE load balancers to the current model:

- Using an online collection task:
  - Configure the load balancers (see page 281) to permit access from a Skybox Collector and create a collection task (see page 281) to collect the load balancer configurations and add the configuration data to the model.

    The collection task can collect data from multiple load balancers.
- Using an offline file import task:
  - Generate and retrieve load balancer configuration files and import their data into the model (see page 282).

    The file import task can import the data of multiple load balancers.

Configuring Cisco ACE load balancers for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure a Cisco ACE load balancer for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Load Balancers – Cisco ACE Collection tasks use the SSH protocol to connect to Cisco ACE load balancers.

Commands sent to device

Load Balancers – Cisco ACE Collection tasks send the following commands to Cisco ACE load balancers:

- `terminal length 0`
- `sh run`

Cisco ACE collection tasks

Load Balancers – Cisco ACE Collection tasks retrieve configuration data from Cisco ACE load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – Cisco ACE Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Cisco ACE load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the load balancers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Connection Protocol	The connection protocol to use.
Advanced tab	
Resolve LB IP to Host Name Using Configuration File	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

Importing Cisco ACE configuration data

You can use an **Import – Directory** task to import Cisco ACE configuration data.

Note: If you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Cisco ACE load balancer configuration:

- `run.txt`: The ACE configuration file

  This file is the output of the ACE `show run` command.

- (Optional) `route.txt`: Dump of the ACE routing table

  This file is the output of the ACE `show ip route` command.

If `route.txt` is included, its routing rules overwrite routing rules from `run.txt` because its information is more extensive and includes static and dynamic routing rules.

You can import the configurations of multiple load balancers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

CISCO CSS LOAD BALANCER

You can add or update configuration data from Cisco CSS load balancers to the current model:

- Using an online collection task:
  - Configure the load balancers (see page 283) to permit access from a Skybox Collector and create a collection task (see page 284) to collect the load balancer configurations and add the configuration data to the model.

    The collection task can collect data from multiple load balancers.

- Using an offline file import task:
  - Generate and retrieve load balancer configuration files and import their data into the model (see page 284).

    The file import task can import the data of multiple load balancers.

Configuring Cisco CSS load balancers for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure a Cisco CSS load balancer for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Load Balancers – Cisco CSS Collection tasks use the SSH protocol to connect to Cisco CSS load balancers.

Commands sent to device

Load Balancers – Cisco CSS Collection tasks send the following commands to Cisco CSS load balancers:

- `no terminal more`
- `sh run`

Cisco CSS collection tasks

Load Balancers – Cisco CSS Collection tasks retrieve configuration data from Cisco CSS load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – Cisco CSS Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the Cisco CSS load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the load balancers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Connection Protocol	The connection protocol to use.
Advanced tab	
Resolve LB IP to Host Name Using Configuration File	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

Importing Cisco CSS configuration data

You can use an **Import – Directory** task to import Cisco CSS configuration data.

Note: If you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Cisco CSS load balancer configuration:

- `run.txt`: The CSS configuration file

  This file is the output of the CSS `sh run` command.

- (Optional) `route.txt`: Dump of the CSS routing table

  This file is the output of the CSS `sh route` command.

If `route.txt` is included, its routing rules overwrite routing rules from `run.txt` because its information is more extensive and includes static and dynamic routing rules.

You can import the configurations of multiple load balancers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

CITRIX NETSCALER LOAD BALANCER

You can add or update configuration data from Citrix NetScaler load balancers to the current model:

- Using an online collection task:
  - Configure the load balancers (see page 285) to permit access from a Skybox Collector and create a collection task (see page 286) to collect the load balancer configurations and add the configuration data to the model.

    The collection task can collect data from multiple load balancers.
- Using an offline file import task:
  - Generate and retrieve load balancer configuration files and import their data into the model (see page 287).

    The file import task can import the data of multiple load balancers.

Configuring Citrix NetScaler load balancers for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure a Citrix NetScaler load balancer for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Load Balancers – NetScaler Collection tasks use the SSH protocol to connect to NetScaler load balancers.

Commands sent to device

Load Balancers – NetScaler Collection tasks send the following command to NetScaler load balancers:

- `show ns.conf`

Citrix NetScaler collection tasks

Load Balancers – NetScaler Collection tasks retrieve configuration data from NetScaler load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – NetScaler Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the NetScaler load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the load balancers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Override device prompt	The load balancer prompt. If this field is empty, the default prompt is expected: **#$**.
Override password prompt	The password prompt. If this field is empty, the default prompt is expected: **[p|P]assword:\s$**.
Model VIP Addresses	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

Importing Citrix NetScaler configuration data

You can use an **Import – Directory** task to import Citrix NetScaler configuration data.

The following file is required to import a Citrix NetScaler load balancer configuration:

- `*.*`: The NetScaler configuration file

  This file is the output of the NetScaler show `ns.conf` command.

You can import the configurations of multiple load balancers.

F5 BIG-IP LOAD BALANCER

You can add or update configuration data from F5 BIG-IP load balancers to the current model:

- Using an online collection task:
  - Configure the load balancers (see page 287) to permit access from a Skybox Collector and create a collection task (see page 290) to collect the load balancer configurations and add the configuration data to the model.

    The collection task can collect data from multiple load balancers.
- Using an offline file import task:
  - Generate and retrieve load balancer configuration files and import their data into the model (see page 291).

    The file import task can import the data of multiple load balancers.

    Note: The file import task can only import the data of v11 and higher.

Configuring F5 BIG-IP load balancers for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure an F5 BIG-IP load balancer for data collection:

- Create a separate user on the device with `admin` or `root` permissions for Skybox data collection.
- (Optional) Change the timeouts for the different stages of data collection.

To set timeouts for BIG-IP data collection

1. Use a text editor to create a file named `timeouts.txt` in `<Skybox_Home>\intermediate\bin\collectors\loadBalancers\bigIp`

   An example of this file is at `<Skybox_Home>\intermediate\bin\parsers\collectors\loadBalancers\bigIp\timeouts.example`
2. Add or edit a line for each timeout (listed and described in the following table) whose value is to differ from the default value.

   The format of each line is `<timeout>=<time in seconds>`

   A value of `0` means that the script checks once for matching patterns.

3 Save the file.

Timeout	Default	Description
password_prompt_timeout	10	The time (in seconds) to wait for the password prompt on connection.
device_prompt_timeout	10	The time (in seconds) to wait for the device prompt or device config prompt after providing the password.
tmsh_shell_Prompt_timeout	0	The time (in seconds) to wait for the `tmos` prompt after issuing the `run util bash` command.
advanced_shell_command_prompt_timeout	10	The time (in seconds) to wait for the device prompt or device config prompt after issuing the `run util bash` command.
net_route_command_timeout	120	The time (in seconds) to wait for the device prompt or device config prompt after issuing the `tmsh show /net route` command.
netstat_command_timeout	120	The time (in seconds) to wait for the device prompt or device config prompt after issuing the `netstat -nr` command.
show_running_config_command_timeout	120	The time (in seconds) to wait for the device prompt or device config prompt after issuing the `tmsh modify /cli preference pager disabled,tmsh show running-config` command.
save_config_timeout	120	The time (in seconds) to wait for the device prompt or device config prompt after issuing the `tmsh save /sys config file bigip.conf no-passphrase` command.
grep_list_of_policies_prompt_timeout	15	The time (in seconds) to wait for the device prompt or device config prompt after issuing the `grep -A 4 $regex /var/local/scf/bigip.conf | grep -B 4 asm\r` command.
tmsh_save_asm_policy_prompt_timeout	60	The time (in seconds) to wait for the device prompt or device config prompt after issuing the `tmsh save asm policy overwrite $profile xml-file $profileFileName\r` command.
scp_pass_prompt_timeout	4	The time (in seconds) to wait for the password prompt after issuing the SCP command for copying files
scp_connection_prompt_timeout	1	The time (in seconds) to wait for the device prompt or device config prompt after issuing the SCP command for copying files.

Timeout	Default	Description
scp_device_prompt_timeout	60	The time (in seconds) to wait for the `connecting\s\(yes\/no\)\?\s$` prompt after issuing the SCP command for copying files.

Commands sent to F5 BIG-IP load balancers

Connection type

Load Balancers – BIG-IP Collection tasks use the SSH protocol to connect to BIG-IP load balancers. Files are transferred over SSH using SCP.

Commands sent to device (v12-v15)

Load Balancers – BIG-IP Collection tasks send the following commands to v12-v15 BIG-IP load balancers:

- `tmsh show /sys version | grep ' Version'\r`
- `tmsh save /sys config file bigip.conf no-passphrase\r`
- `netstat -nr`
- `tmsh modify /cli preference pager disabled`
- `tmsh show running-config`
- `tmsh show /net route`

Commands sent to device (v11)

Load Balancers – BIG-IP Collection tasks send the following commands to v11 BIG-IP load balancers:

- `tmsh show /sys version | grep ' Version'\r`
- `tmsh save /sys config file bigip.conf no-passphrase`
- `netstat -nr`
- `tmsh modify /cli preference pager disabled`
- `tmsh show running-config`
- `tmsh show /net route`

Commands sent to device (v7-v10)

Load Balancers – BIG-IP Collection tasks send the following commands to v7-v10 BIG-IP load balancers:

- `SCP: files`
- `/config/bigip_base.conf`
- `/config/bigip.conf`
- `tmsh show /net route`
- `netstat -nr`

F5 BIG-IP collection tasks

Load Balancers – BIG-IP Collection tasks retrieve configuration data from BIG-IP load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – BIG-IP Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.
Addresses	A comma-separated list of the IP addresses of the BIG-IP load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers. **Note:** For BIG-IP V10 and lower, the task supports single IP addresses only.
Version	The version of the BIG-IP load balancer.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the load balancers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Collect AFM Firewall	Specifies whether to collect BIG-IP Advance Firewall Management (AFM) configuration data.
Collect Additional Configuration Files	Specifies whether to collect the output of the `tmsh show running-config` command.
Collect ASM Configuration	Specifies whether to collect the configuration of the BIG-IP Application Security Manager (ASM).
Use iControl for ASM Configuration	Specifies whether to collect ASM configuration via HTTP instead of via SSH.

Property	Description
Write Debug Log	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system Temp directory.
Save Config Timeout	Time (in seconds) to wait for a load balancer prompt or config prompt after issuing the `tmsh save /sys config file bigip.conf no-passphrase` command. If the field contains a value, it overrides the setting for `save_config_timeout` in `timeouts.txt` (see Configuring BIG-IP load balancers for data collection (on page 287)).
Use IP Forwarding	Specifies whether to use IP forwarding (rather than load balancing the traffic to a pool).
Use Strict Host Key Checking	Specifies whether collection fails if an RSA key conflict occurs.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

Importing F5 BIG-IP configuration data

You can use an **Import – Directory** task to import F5 BIG-IP (v11 and higher) configuration data.

Note: If you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a F5 BIG-IP load balancer configuration:

- `bigip.conf`: The BIG-IP configuration file

  This file is generated by the BIG-IP `tmsh save /sys config file bigip.conf no-passphrase` command.

- (Optional) `netroute.txt`: Dump of the BIG-IP routing table

  This file is the output of the BIG-IP `netstat -nr` command.

You can import the configurations of multiple load balancers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

PULSE SECURE VTM LOAD BALANCER

You can add or update configuration data from Pulse Secure vTM load balancers to the current model using an online collection task:

- Configure the load balancers (see page 292) to permit access from a Skybox Collector and create a collection task (see page 292) to collect the load balancer configurations and add the configuration data to the model.

The collection task can collect data from multiple load balancers.

Configuring Pulse Secure vTM load balancers for data collection

To configure a Pulse Secure vTM load balancer for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Load Balancers – Pulse Secure vTM Collection tasks use a REST API to connect to Pulse Secure load balancers.

Pulse Secure vTM collection tasks

Load Balancers – Pulse Secure vTM Collection tasks retrieve configuration data from Pulse Secure load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – Pulse Secure vTM Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the program.
Addresses	A comma-separated list of the IP addresses of the Pulse Secure load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Username	The user name to access the load balancers.
Password	The user password.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

RADWARE ALTEON LOAD BALANCER

You can add or update configuration data from Radware Alteon load balancers to the current model using an online collection task:

- Configure the load balancers (see page 293) to permit access from a Skybox Collector and create a collection task (see page 293) to collect the load balancer configurations and add the configuration data to the model.

  The collection task can collect data from multiple load balancers.

Configuring Radware Alteon load balancers for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure a Radware Alteon load balancer for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Load Balancers – Alteon Collection tasks use the SSH protocol to connect to Alteon load balancers.

Commands sent to device

Load Balancers – Alteon Collection tasks send the following commands to Alteon load balancers:

- `terminal length 0`
- `/cfg/dumo`

Radware Alteon collection tasks

Load Balancers – Alteon Collection tasks retrieve configuration data from Alteon load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – Alteon Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the program.
Addresses	A comma-separated list of the IP addresses of the Alteon load balancers, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 22. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the load balancers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.

Property	Description
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Logging	(Only select this option if Skybox Professional Services has requested a debug file.) Specifies whether the task writes a debug log. If selected, the log is saved in the operating system Temp directory.
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

RADWARE APPDIRECTOR LOAD BALANCER

You can add or update configuration data from Radware AppDirector load balancers to the current model:

- Using an online collection task:
  - Configure the load balancers (see page 294) to permit access from a Skybox Collector and create a collection task (see page 295) to collect the load balancer configurations and add the configuration data to the model.

    The collection task can collect data from multiple load balancers.
- Using an offline file import task:
  - Generate and retrieve load balancer configuration files and import their data into the model (see page 296).

    The file import task can import the data of multiple load balancers.

Configuring Radware AppDirector load balancers for data collection

Note: To run this collection task, the Skybox Collector specified for the task must reside on a Linux platform.

To configure a Radware AppDirector load balancer for data collection:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.

Connection type

Load Balancers – AppDirector Collection tasks use the SSH protocol to connect to AppDirector load balancers.

Commands sent to device

Load Balancers – AppDirector Collection tasks send the following commands to AppDirector load balancers:

- `system config immediate`
- `show ip route`
- `manage terminal more-prompt set 2`

Radware AppDirector collection tasks

Load Balancers – AppDirector Collection tasks retrieve configuration data from AppDirector load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – AppDirector Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the program.
Addresses	A comma-separated list of the IP addresses of the AppDirector load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Method	• **Device**: Use the authentication credentials provided here. • **CyberArk**: Retrieve authentication credentials from CyberArk. (To use this option, configure CyberArk (see page 22).)
Username	This field is displayed if **Method** = **Device**. The user name to access the load balancers.
Password	This field is displayed if **Method** = **Device**. The user password.
Safe	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk safe that contains the user authentication credential object.
Object	This field is displayed if **Method** = **CyberArk**. The name of the CyberArk object that contains the user name and password.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

Importing Radware AppDirector configuration data

Note: We recommend that you use an **Import – Directory** task to import the configuration data; if you include the routing table, the files for each device must be in a separate subdirectory of the specified directory (even if you are importing a single device).

The following files are required to import a Radware AppDirector load balancer configuration:

- `*.*`: The AppDirector configuration file

  This file is the output of the AppDirector `system config immediate` command.

- (Optional) `route.txt`: Dump of the AppDirector routing table

  This file is the output of the AppDirector `show ip route` command.

You can import the configurations of multiple load balancers; put each set of configuration files in a separate 1st-level subdirectory of the specified directory.

Note: To run an **Import – Collector** task or an **Import – Collector Advanced** task, the Skybox Collector specified for the task must reside on a Linux platform.

RADWARE WSD LOAD BALANCER

You can add or update configuration data from Radware WSD load balancers to the current model:

- Using an online collection task:
  - Configure the load balancers (see page 296) to permit access from a Skybox Collector and create a collection task (see page 297) to collect the load balancer configurations and add the configuration data to the model.

    The collection task can collect data from multiple load balancers.
- Using an offline file import task:
  - Generate and retrieve load balancer configuration files and import their data into the model (see page 297).

    The file import task can import the data of multiple load balancers.

Configuring Radware WSD load balancers for data collection

To configure a Radware WSD load balancer so that Skybox can retrieve its configuration data:

- Configure the load balancer to permit SNMP access from a Skybox Collector.

Connection type

Load Balancers – Radware WSD Collection tasks use SNMP to connect to Radware WSD load balancers.

Commands sent to device

Load Balancers – Radware WSD Collection tasks send the following commands to Radware WSD load balancers:

- `.1.3.6.1.2.1.1.5.0`
- `.1.3.6.1.4.1.89`
- `.1.3.6.1.4.1.89.35.1.62`
- `.1.3.6.1.4.1.89.35.1.68`
- `.1.3.6.1.4.1.89.35.1.80`
- `.1.3.6.1.4.1.89.35.1.102`

Radware WSD collection tasks

Load Balancers – Radware WSD Collection tasks retrieve configuration data from Radware WSD load balancers and add this data to the current model.

Task properties

The properties that control **Load Balancers – Radware WSD Collection** tasks are described in the following table.

Property	Description
Basic tab	
WSD Addresses	A comma-separated list of the IP addresses and IP address ranges of the Radware WSD load balancers. **Note**: A task can collect the configurations of multiple load balancers only if the same authentication is used for all the load balancers.
Properties	
SNMP Community string	The SNMP Community string to access the Radware WSD load balancers.
Advanced tab	
Location Hint	The location of the load balancers. **Note**: Use this property if different locations use the same set of IP addresses, so that load balancers at different locations can have the same IP address.

Importing Radware WSD configuration data

To import a Radware WSD load balancer configuration, generate a WSD SNMP dump file.

To generate a WSD SNMP dump file

- Generate a WSD SNMP dump file by running the following commands:

```
## snmpwalk.exe -c public -t 3 -v1 -On <IP address> .1.3.6.1.2.1.1.5.0 >
<output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address> .1.3.6.1.4.1.89.26.1.1
>> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.13.1 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.11.1 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.62.1 >> <output name>.txt
```

```
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.62.2 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.80.1 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.80.2 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.81.1 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.81.2 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.68.1 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.68.2 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.102.3 >> <output name>.txt
## snmpwalk.exe -c public -t 3 -v1 -On <IP address>
.1.3.6.1.4.1.89.35.1.102.4 >> <output name>.txt
```

The output file can have any name but must have the extension `txt`.

You can import the configurations of multiple load balancers; give each WSD SNMP dump file a different name.

Chapter 13

IPS tasks

This chapter describes how to add IPS device configuration data to the current model.

In this chapter

TREND MICRO TIPPINGPOINT IPS DEVICES

You can add or update configuration data from Trend Micro TippingPoint IPS devices to the current model:

- Using an online collection task:
  - Configure the IPS devices (see page 299) to permit access from a Skybox Collector and create a collection task (see page 300) to collect the Trend Micro TippingPoint device configuration and add the configuration data to the model.
- Using an offline file import task:
  - Generate and retrieve a Trend Micro TippingPoint device configuration file and import its data into the model (see page 301).

After the data is collected, you must configure Skybox to work with IPS devices. Refer to the IPS support in Skybox section in the Skybox Vulnerability Control User Guide.

Configuring Trend Micro TippingPoint IPS devices for data collection

To configure a Trend Micro TippingPoint IPS device so that Skybox can retrieve its configuration data:

- Create a Super User in the SMS appliance.
- Configure the device to permit collection. (The Skybox Collector must have permission to connect to the SMS appliance using HTTPS on port 433.)

Connection type

IPS – Trend Micro TippingPoint Collection tasks use a REST API to connect to Trend Micro TippingPoint IPS devices.

Trend Micro TippingPoint collection tasks

IPS – Trend Micro TippingPoint Collection tasks retrieve TippingPoint IPS configuration data from a Security Management System (SMS) appliance and add this data to the current model.

Task properties

The properties that control **IPS – Trend Micro TippingPoint Collection** tasks are described in the following table.

Property	Description
Basic tab	
SMS Authentication	
Server Name or IP	The name or IP address of the SMS appliance, with the format `<server name>[:<port>]` or `nnn.nnn.nnn.nnn[:<port>]`. The default port is 443.
Username	The Super User name for logging in to the SMS appliance.
Password	The Super User password.
Collection	
Device Names	A comma-separated list of the devices whose data is collected by this task. Wildcards are permitted.
Device Authentication for Profile Retrieval	**Note**: Some information cannot be collected from the SMS appliance (even though it is the same for all the devices). If device credentials are specified, this information is collected from the specified device. Otherwise, it is collected from any device.
Device	The IP address of the TippingPoint device.
Username	The user name of a user of the TippingPoint device.
Password	The user password.
Advanced tab	
Location Hint	The location of the devices whose configuration data is to be imported. **Note**: Use this property if different locations use the same set of IP addresses, so that devices at different locations can have the same IP address.
Segments to clone	A comma-separated list of segments to clone in the model, with the format: `<segment name>, <# of clones>[, <segment2 name>, <# of clones>][, ...]` Use this option if multiple VLANs pass through an interface of the IPS appliance.
Filter status scan mode	Specifies how to collect filter information. The collection task uses the output of the show `configuration filter <filter number>` command multiple times at different stages of processing. If there are many filters, the task might run slowly if the command is sent every time. (Skybox caches the output

Property	Description
	of the command.) • **Full filter scan**: Send the `show configuration filter <filter number>` command every time that the output is required. • **Recently changed**: All filters that are connected to a profile that was changed in the current version are collected from a device. Other filters are taken from the cache. (If the filter is not in the cache, the command is sent and the result is added to the cache.) • **Use cache only**: Take all filters from the cache. (If the filter is not in the cache, the command is sent and the result is added to the cache.)

Importing Trend Micro TippingPoint configuration data

You can use an **Import – Directory** task to import Trend Micro TippingPoint configuration data.

Note: If you use an **Import – Directory** task, some policy-related ACLs are not imported into the model.

The following file is required to import a Trend Micro TippingPoint configuration:

- `*.xml`: TippingPoint XML file

This file can contain:

- All the TippingPoint tables: Use 1 request to fetch all the tables.
- Selected tables: Use 1 request per table, and append the output of each request into a single file.

  You can import any combination of the following tables: ACTIONSET, DEVICE, PROFILE_INSTALL_INVENTORY, POLICY, PROFILE, SEGMENT, SEVERITY, SIGNATURE, VIRTUAL_SEGMENT.

To create an XML file containing all the TippingPoint tables

1 Run the following API request: `https://<url>/dbAccess/tptDBServlet?method=DataDictionary&format=xml`

2 Save the response as an XML file.

3 Add `<skybox vendor="TippingPoint" />` after the `<resultset>` tag, so that the first lines of the XML file are:

```
<?xml version="1.0" ?>
<resultset>
<skybox vendor="TippingPoint" />
<table name=...
```

To create an XML file containing selected TippingPoint tables

1 Create an empty XML file.

2 Add the following lines to the file:

```
<?xml version="1.0" ?>
<resultset>
<skybox vendor="TippingPoint" />
```

3 For each required table:

a. Run the following API request: `https://<url>/dbAccess/tptDBServlet?method=DataDictionary&table=<tableName>&format=xml`

`<tableName>` can be any of `ACTIONSET`, `DEVICE`, `PROFILE_INSTALL_INVENTORY`, `POLICY`, `PROFILE`, `SEGMENT`, `SEVERITY`, `SIGNATURE`, `VIRTUAL_SEGMENT`

b. Append the response to the XML file.

4 Append `</resultset>` to the end of the file.

MCAFEE IPS DEVICES

You can add or update configuration data from McAfee IPS devices to the current model using an online collection task:

- Configure the IPS devices (see page 299) to permit access from a Skybox Collector and create a collection task (see page 300) to collect the McAfee IPS device configuration and add the configuration data to the model.

Configuring McAfee IPS devices for data collection

To configure a McAfee IPS device so that Skybox can retrieve its configuration data:

- Skybox data collection requires a read-only user on the device; we recommend that you create a separate user for this purpose.
- Configure the device to permit collection. (The Skybox Collector must have permission to connect to the device using HTTPS on port 3306.)

Connection type

IPS – McAfee IPS Collection tasks use SQL to connect to McAfee IPS devices.

McAfee IPS collection tasks

IPS – McAfee IPS Collection tasks retrieve configuration data from McAfee IPS devices and add this data to the current model.

Task properties

The properties that control **IPS – McAfee IPS Collection** tasks are described in the following table.

Property	Description
Basic tab	
Run in	Where to run the data collection.

Property	Description
Server IP	The IP address of the McAfee IPS device, with the format `nnn.nnn.nnn.nnn[:<port>]`. The default port is 3306.
Username	The user name of a user of the McAfee IPS device.
Password	The user password.
DB Name	The name of the McAfee IPS database.
Advanced tab	
Merge assets by WINS name	Specifies whether to merge assets from the same network by name and not by IP address.

IBM PROVENTIA G APPLIANCES

You can add or update configuration data of IBM Proventia G appliances from an IBM SiteProtector database to the current model using an online collection task:

- Create a collection task (see page 303) to collect the Proventia G appliance configuration and add the configuration data to the model.

After the data is collected, you must configure Skybox to work with IPS devices. Refer to the IPS support in Skybox section in the Skybox Vulnerability Control User Guide.

Configuring IBM Proventia G appliances for data collection

To configure an IBM SiteProtector database for data collection (IBM Proventia G appliance configuration data is collected from an IBM SiteProtector database):

- Skybox data collection requires a read-only user on the database; we recommend that you create a separate user for this purpose.

Connection type

IPS – ISS SiteProtector IPS Collection tasks use SQL to connect to IBM SiteProtector databases.

IBM SiteProtector IPS collection tasks

IPS – ISS SiteProtector IPS Collection tasks retrieve configuration data of IBM Proventia G appliances from IBM SiteProtector databases and add this data to the current model.

Task properties

The properties that control **IPS – ISS SiteProtector IPS Collection** tasks are described in the following table.

Property	Description
Basic tab	
Sensor IP Address	The IP address of the Proventia G appliance.
Database connection	
Connection Method	The method to use to connect to the SiteProtector database.

Property	Description
	DSN is retained for backward compatibility only. Do *not* select it when creating tasks.
Address/Name	This field is enabled only if **Connection Method** = **Direct**. The name or IP address of the database server that hosts the SiteProtector database.
User Authentication	
Database Username	The user name to access the SiteProtector sensor.
Database Password	The user password.
Advanced tab	
Location Hint	The location of the device. **Note**: Use this property if different locations use the same set of IP addresses, so that devices at different locations can have the same IP address.

Interface pairs to clone	A comma-separated list of interface pairs to clone in the model, with the format:
	`<interface pair name>, <# of clones>[, <interface pair2 name>, <# of clones>][, ...]`
	`<interface pair name>` can be any of `Interfaces_AB`, `Interfaces_CD`, `Interfaces_EF`, `Interfaces_GH`
	Use this option if multiple VLANs pass through an interface of the IPS appliance.

Chapter 14

Alerts services tasks

This chapter describes how to add the output of alert services to the current model.

In this chapter

SYMANTEC DEEPSIGHT ALERT SERVICES

You can add or update threat alerts from the Symantec DeepSight alert services to the current model using an online collection task:

- Create a collection task (see page 305) to collect the threat alerts made available by the service and add the threat alert data to the model.

Configuring Symantec DeepSight alert services for data collection

To retrieve data from the DeepSight alert services:

- You need a subscription to the DeepSight DataFeed service

Connection type

Alert Service – DeepSight Collection tasks use a web service to connect to the DeepSight alert services.

Symantec DeepSight collection tasks

Alert Service – DeepSight Collection tasks collect DeepSight threat alerts and add or update the relevant threat alerts in the current model. These tasks also update the DeepSight product catalog.

Note: Schedule these tasks to run on a higher frequency than other tasks to ensure that all alerts are downloaded as soon as they become available.

Task properties

The properties that control **Alert Service – DeepSight Collection** tasks are described in the following table.

Property	Description
Download Recent Alerts Only	Specifies whether to download only alerts added or updated since the most recent download. If cleared, downloads all content available from the service (including old alerts). **Note**: The 1st time that you run the task all alerts are downloaded, even if you select **Download Recent Alerts**

Property	Description
	Only.
Download Product Catalog	Specifies whether to download the DeepSight product catalog while downloading the alerts. If you select **Download Recent Alerts Only**, only recent products are downloaded. **Note**: The 1st time that you run the task the product catalog is downloaded, even if you do *not* select **Download Product Catalog**.
User Authentication	
Username	User name for DeepSight alert services.
Password	Password for DeepSight alert services.
DataFeed service version	Select the version of the DeepSight DataFeed service to which you are subscribed.

Note: By default, DeepSight threat alerts are not displayed. To view these alerts, navigate to **Tools** > **Options** > **Server Options** > **Threat Manager** and then select **DeepSight**.

See also the Setting up threat alert collection section in the Skybox Threat Manager User Guide.

VERISIGN IDEFENSE ALERT SERVICES

You can add or update threat alerts from the VeriSign iDefense alert services to the current model using an online collection task:

- Create a collection task (see page 306) to collect the threat alerts made available by the service and add the threat alert data to the model.

Configuring VeriSign iDefense alert services for data collection

To retrieve data from the iDefense alert services:

- You need a subscription to the iDefense alert services

Connection type

Alert Service – iDefense Collection tasks use a web service to connect to the iDefense alert services.

VeriSign iDefense collection tasks

Alert Service – iDefense Collection tasks collect iDefense threat alerts and add or update the relevant threat alerts in the current model. These tasks also update the iDefense product catalog.

Note: Schedule these tasks to run on a higher frequency than other tasks to ensure that all alerts are downloaded as soon as they become available.

Task properties

The properties that control **Alert Service – iDefense Collection** tasks are described in the following table.

Property	Description
Download only recent alerts	Specifies whether to download only alerts added or updated since the most recent download. If cleared, downloads all content available from the service (including old alerts). **Note**: Before running this task for the 1st time, read the subsection that follows this table.
Authentication	
Username	User name for iDefense alert services.
Password	Password for iDefense alert services.
iDefense alert types	
Include MalCode IRs	Specifies whether to collect MalCode Intelligence Reports.
Include Threat IRs	Specifies whether to collect Threat Intelligence Reports.

Note: By default, iDefense threat alerts are not displayed. To display these alerts, navigate to **Tools** > **Options** > **Server Options** > **Threat Manager** and then select **iDefense**.

Running an iDefense collection task for the 1st time

The 1st time that you run the task, *all* alerts from 2000-01-01 are downloaded, even if you select **Download only recent alerts**.

Note: The task can take up to 20 hours to download all the alerts the 1st time it runs. If you do not need data from so far back, change the starting date by changing the value of `idefense_epoch_date` in `<Skybox_Home>\server\conf\sb_server.properties`

A progress message is displayed for each 10% of the data that is downloaded.

Chapter 15

Analysis tasks

This chapter describes how to set the properties of the analysis tasks.

In this chapter

CHANGE TRACKING TASKS

Analysis – Change Tracking tasks create change records by comparing the current firewall configuration file with the previous file. Change records describe differences in access rules and firewall objects. These changes can then be viewed in Skybox. These tasks also reanalyze the results of all change requests in all Access Change tickets.

Task properties

The properties that control **Analysis – Change Tracking** tasks are described in the following table.

Property	Description
Firewall Scope	The firewalls and firewall folders for which the task creates change tracking records.
Exclude Firewall Scope	The firewalls and firewall folders that match **Firewall Scope** but are not included in the analysis.
Firewall Filter	Specifies whether to analyze all firewalls (in **Firewall Scope**) or only firewalls with an ACL that has changed since the most recent analysis.
Maximum Access Rules in Device	Devices that have more than this number of access rules are not analyzed.

For information about change tracking, see the Change tracking chapter in the Skybox Firewall Assurance User Guide.

Change tracking and change reconciliation

If change reconciliation is enabled, the task matches the change records with change requests in Access Change tickets. Matching uses the following methods:

- Match the **Extracted Ticket ID** field of the change record with the **External Ticket ID** field in the Skybox ticket

  The extracted ticket ID is the ID of the ticket issued by your organization about the requested change; the ID is extracted from the **Comment** field of the access rule or firewall object using a regular expression.

- Match the IP addresses and ports of the source and destination of the actual change with those in the change requests in the Access Ticket

  If matching is by IP addresses and ports, the results include the percentage of coverage of the change-by request

For information about change tracking and change reconciliation settings, see the Change Tracking Settings topic in the Skybox Installation and Administration Guide.

For information about the Change Reconciliation feature, see the Reviewing and reconciling changes section in the Skybox Firewall Assurance User Guide.

EXPOSURE (ATTACK SIMULATION) TASKS

Analysis – Exposure tasks run *attack simulations* (see the Simulating attacks section in the Skybox Vulnerability Control User Guide).

Attack simulation involves heavy computations. An **Analysis – Exposure** task can run for minutes or even hours, depending on the size and complexity of the network. The following options in `/server/conf/sb_server.properties` can be used to cut down the run time if necessary:

- Reduce the maximum data analysis that attack simulation processes to prepare the next step analysis by lowering the value of `ATS_limit_of_target_access_boxes`.
- Decrease the calculation steps performed by changing the value of `ATS_max_steps_for_attack` to **1**.

Task properties

The properties that control **Analysis – Exposure** tasks are described in the following table.

Property	Description
Basic tab	
Calculate Risks	Specifies whether the task calculates exposure status and risks. If this property is cleared, attacks are generated; you can view attack maps, but exposure status and risks are not calculated. **Note**: Only clear this property (as a work-around) if severe problems are encountered in the exposure and risk analysis stages of attack simulation.
Backdoor Exploits	Specifies whether an attack that exploits a backdoor can

Property	Description
Require Vulnerability Occurrences	be developed only if a backdoor vulnerability occurrence is defined on the service. **Note**: If selected, the existence of a service without a backdoor vulnerability occurrence is not sufficient to develop an attack. Similarly, if the backdoor vulnerability occurrence is marked as fixed (the backdoor was removed), attacks that use the backdoor are blocked in the model, even if the service exists on the asset.
Simulate Full IP Spoofing	Specifies whether simulated attackers try spoofing their source IP address to all IP addresses. If this property is cleared, spoofing is limited to IP addresses in the actual network of the attacker. **Note**: Full IP address spoofing slows the task.
Advanced tab	
Asset Aggregation	
Enabled	Specifies whether asset aggregation is enabled. If asset aggregation is enabled, assets that behave in the same way from an attacker's point of view (for example, the same vulnerability occurrences or the same access) are modeled internally by the task as a single node (aggregated). Using this mode improves the performance of the task. Usually, there is no effect on the accuracy of the results.
Workstation Ignore Ports	A comma-separated list of ports to ignore when checking similarities between workstations to aggregate them into groups.
Ignore List	Assets that appear in this list of scopes are not aggregated into groups of similar assets.

FALSE POSITIVE REDUCTION TASKS

Analysis – False Positive Reduction tasks check whether any vulnerability occurrences in the model that were reported by a scanner are intrinsically false (for example, a Linux vulnerability occurrence reported for a Windows machine).

Task properties

The properties that control **Analysis – False Positive Reduction** tasks are described in the following table.

Property	Description
Network Scope	The assets and container entities to analyze.
Exclude Network Scope	The assets and container entities that match **Network Scope** but are not included in the analysis.

For additional information, see the False positive reduction topic in the Skybox Vulnerability Control User Guide.

POLICY COMPLIANCE TASKS

Analysis – Policy Compliance tasks check whether the network is compliant with your policies.

Task properties

The properties that control **Analysis – Policy Compliance** tasks are described in the following table.

Property	Description
Basic tab	
Scope	The type of compliance to analyze.
Firewall Scope	This field is displayed if **Scope** = **Firewall Assurance**. The firewalls and firewall folders for which compliance is analyzed.
Exclude Firewall Scope	This field is displayed if **Scope** = **Firewall Assurance**. The firewalls and firewall folders that match **Firewall Scope** but are not included in the analysis.
Network Scope	This field is displayed if **Scope** = **Network Assurance**. The assets and container entities for which compliance is analyzed.
Exclude Network Scope	This field is displayed if **Scope** = **Network Assurance**. The assets and container entities that match **Network Scope** but are not included in the analysis.
Firewall Filter	This field is enabled only if **Scope** = **Firewall Assurance**. Specifies whether to analyze all firewalls (in **Firewall Scope**) or only firewalls with at least 1 ACL that has changed since the most recent analysis.
Analyze Access Policy	Specifies whether to analyze Access Compliance.
Access Policy Scope	This field is enabled only if you select **Analyze Access Policy**. The parts of the Access Policy (policy folders, policy sections, or Access Checks) to analyze.
Analyze Rule Policy	(Firewall Assurance only) Specifies whether to analyze Rule Compliance.
Rule Policy Scope	This field is enabled only if you select **Analyze Rule Policy**. The parts of the Rule Policy (policy folders or Rule Checks) to analyze.
Analyze Configuration Policy	Specifies whether to analyze Configuration Compliance.
Configuration Policy Scope	This field is enabled only if you select **Analyze Configuration Policy**. The parts of the Configuration Policies (policy folders, policies, or Configuration Checks) to analyze.

Property	Description
Advanced tab	
Severity Threshold	The severity threshold to use when analyzing policies for compliance. Only Access Checks / Rule Checks / Configuration Checks with at least this severity are checked for compliance.
Analyze Access Queries	Specifies whether to analyze access queries when analyzing the Access Policy. *Access queries* are access-related queries that do not affect policy compliance.
Number of Threads	The number of threads to use for calculations when running the task.
Included Source Asset Groups	A comma-separated list of IDs of source asset groups to include in the analysis.
Excluded Source Asset Groups	A comma-separated list of IDs of source asset groups to exclude from the analysis.
Timeout in Minutes for Access Queries	Maximum time for calculating each access query.
Generate Access Query CSVs	Specifies whether to generate CSV reports for access queries.
Maximum Access Rules in Device	Devices that have more than this number of access rules are not analyzed.

RULE RECERTIFICATION TASKS

Rule Recertification tasks check all access rules against rule review policies and update the next review date of those that meet the criteria of a policy. They can also generate new recertification tickets and initialize the next review date of new access rules.

For information about rule review, see the Rule review and recertification section in the Skybox Firewall Assurance User Guide.

Task properties

The properties that control **Analysis – Rule Recertification** tasks are described in the following table.

Property	Description
Initialize Next Review Date of rules without Next Review Date	Specifies whether to set an initial review date for access rules that do not have one already, such as after they are first imported to Skybox.
Firewall Scope	Only set an initial review date for access rules in this firewall scope.

Property	Description
Baseline	Specifies the initial review date.
Compute Next Review Date according to the defined Rule Review Policies	Specifies whether the task should compute next review dates for access rules according to the Rule Review policies. **Note**: This is the basic action necessary for the Rule Recertification process; it is selected by default.
Generate Recertification tickets according to the defined Rule Recertification Ticket Policies	Specifies whether the task should generate new recertification tickets according the Rule Recertification Ticket policies. **Note**: This is the same action performed by **Ticket – Auto Generation** tasks with **Rule Recertification Ticket Policies** selected.

SECURITY METRICS CALCULATION TASKS

Analysis – Security Metrics tasks calculate the security metrics scores for Skybox Manager and the risk scores for Skybox Web Client.

These scores are sensitive to changes in the model. Actions that might affect the scores include:

- Data import or collection
- Skybox Vulnerability Dictionary update
- Aging (running a **Model – Outdated** task)
- Running an **Analysis – Vulnerability Detector** task
- User changes to the model (for example, deleting, adding, or modifying vulnerability occurrences or assets)

Run the task on a regular basis, especially after any of these actions. This can be done using a task sequence.

Task properties

The properties that control **Analysis – Security Metrics** tasks are described in the following table.

Property	Description
Calculate Risk Scores for Skybox Web Client	Calculates the risk scores for Vulnerability Control in Skybox Web Client.
Calculate Security Metrics for Skybox Manager (Java Client)	Calculates the security metrics for Vulnerability Control in Skybox Manager.

RULE OPTIMIZATION STATUS TASKS

Analysis – Rule Optimization Status tasks analyze the access rules of selected firewalls for:

- Shadowed rules: Access rules shadowed by other rules above them in the rule chain
- Redundant rules: Access rules covered by rules of the same type below them in the rule chain

For additional information, see the Shadowing and redundancy analysis section in the Skybox Firewall Assurance User Guide.

Task properties

The properties that control **Analysis – Rule Optimization Status** tasks are described in the following table.

Property	Description
Firewall Scope	The firewalls and firewall folders to analyze.
Exclude Firewall Scope	The firewalls and firewall folders that match **Firewall Scope** but are not included in the analysis.
Firewall Filter	Specifies whether to analyze all firewalls (in **Firewall Scope**) or only firewalls with at least 1 ACL that has changed since the most recent analysis.
Maximum Access Rules in Device	Devices that have more than this number of access rules are not analyzed.
Calculate Redundant Rules	Specifies whether to calculate redundant rules. • If cleared, only shadowed rules are calculated.
Redundant Rules Timeout in Minutes	Specifies the timeout for calculation of redundant rules.

VULNERABILITY DETECTION TASKS: PATCH DATA

Analysis – Vulnerability Detector tasks detect vulnerability occurrences based on version and patch information (imported from patch management and asset management systems) and add them to the model.

Note: Because this task does not involve active scanning, you can run it frequently without disrupting the network.

Task properties

The properties that control **Analysis – Vulnerability Detector** tasks are described in the following table.

Property	Description
Basic tab	
Network Scope	The assets and container entities to analyze.
Service Source	Specifies whether to add vulnerability occurrences to the model for the specified services only.
Vulnerability Publication Period	Specifies whether to add vulnerability occurrences to the model for Vulnerability Definitions published within the specified time frame only. • **Custom**: Select **Specific** or **Relative** start and end times.

Property	Description
Do Not Generate Microsoft Vulnerabilities	If cleared and **Service Source** is, for example, **SCCM**, the task adds vulnerability occurrences to the model for Microsoft vulnerabilities using missing patch information.
Advanced tab	
Platform dependency	
Ignore Platform Dependency	Some Vulnerability Definitions are platform-dependent. However, Skybox does not always know the device platform. • If selected, Skybox ignores the platform dependency and the vulnerability occurrences are added to the model even though they might not exist. • If cleared, vulnerability occurrences corresponding to platform-dependent Vulnerability Definitions are not added to the model even though they might exist.
Scope & Threshold	
Include Vulnerability Definitions	Specifies the Vulnerability Definitions for which vulnerability occurrences are added to the model.
Exclude Vulnerability Definitions	Specifies the Vulnerability Definitions for which vulnerability occurrences are not added to the model.
Vulnerability Severity Threshold	Specifies whether only vulnerability occurrences with the specified threshold and higher are added to the model. You can select a severity level or type a severity score.
Product Scope	Specifies whether to add vulnerability occurrences to the model for the specified vendors and products only.
Only Assets with Patch Data	Specifies whether the task only adds vulnerability occurrences to the model for assets that have patch data.

VULNERABILITY DETECTION TASKS: DEVICE CONFIGURATION

Note: Because this task does not involve active scanning, you can run it frequently without disrupting the network.

Analysis – Vulnerability Detector for Network Devices tasks extract vulnerability occurrences from:

- Ingested configuration data of firewalls and other devices, and add the vulnerability occurrences to the model; you can view the vulnerability occurrences in the **Vulnerability Occurrences** tab of the Configuration Compliance section for each device (this can be useful if there is no scanner data available for the devices)
- Ingested scan data and add the vulnerability occurrences to the model (this can be useful if updates were made to a vulnerability source after you

ingested scan data—scanning is intrusive and resource-intensive; running an **Analysis – Vulnerability Detector for Network Devices** task is neither)

Note: Only Qualys QualysGuard and McAfee Vulnerability Manager (Foundstone) scanners are supported for these tasks.

Task properties

The properties that control **Analysis – Vulnerability Detector for Network Devices** tasks are described in the following table.

Property	Description
Basic tab	
Network Scope	The assets and container entities to analyze.
Vulnerability Publication Period	Specifies whether to add vulnerability occurrences to the model for Vulnerability Definitions published within the specified time frame only. • **Custom**: Select **Specific** or **Relative** start and end times.
Advanced tab	
Platform dependency	
Ignore Platform Dependency	Some Vulnerability Definitions are platform-dependent. However, Skybox does not always know the device platform. • If selected, Skybox ignores the platform dependency—the vulnerability occurrences are added to the model even though they might not exist. • If cleared, vulnerability occurrences corresponding to platform-dependent Vulnerability Definitions are not added to the model even though they might exist. **Note**: For Cisco IOS and Cisco Nexus, you must select **Ignore Platform Dependency**; and refer to the subsection following this table.
Scope & Threshold	
Include Vulnerability Definitions	Specifies the Vulnerability Definitions for which vulnerability occurrences are added to the model.
Exclude Vulnerability Definitions	Specifies the Vulnerability Definitions for which vulnerability occurrences are not added to the model.
Vulnerability Severity Threshold	Specifies whether only vulnerability occurrences with the specified threshold and higher are added to the model. You can select a severity level or type a severity score.
Product Scope	Specifies whether to add vulnerability occurrences to the model for the specified vendors and products only.

Vulnerability occurrences on Cisco IOS and Cisco Nexus devices

The Vulnerability Detector results are based on the Cisco IOS Software Checker API. This API supports only Critical- and High-severity vulnerabilities.

Although Skybox can return additional vulnerability occurrences (based on other sources), it might not create all Medium-severity vulnerability occurrences.

Chapter 16

Model maintenance tasks

This chapter describes how to set the properties of model tasks.

In this chapter

MODEL COMPLETION AND VALIDATION TASKS

Model – Completion and Validation tasks verify that the model is correct and that it has no missing components or objects. For a list of the validation rules for which these tasks always check, see Validation rules (on page 320). For additional information, see:

- The Validating the model section in the Skybox Vulnerability Control User Guide.
- The Validating the model section in the Skybox Network Assurance User Guide.

After running the task, look in the **Model Analyses** > **Model Validation** analyses for devices with missing routing tables, disconnected interfaces, and missing next hops. If any data is missing, add it manually.

Task output

You can specify the validation message types (error, warning, or information) to display in the **Messages** tab of the Operational Console while the task is running. Note that the **Messages** tab is limited to 2000 lines of output. All validation messages are written to the validation log file on the Skybox Server at `<Skybox_Home>\server\log\validation.log`.

A log file is created for each run of a validation task; older log files are renamed with a sequential numeric extension.

Task properties

The properties that control **Model – Completion and Validation** tasks are described in the following table.

Property	Description
Completion and Cleanup	
Convert Perimeter Networks to Clouds	A perimeter network is a network in the model in which all the next hops of its network interfaces are missing (that is, they lead to gateways that are not in the model). This property specifies whether the task converts these perimeter networks to (Perimeter) Clouds. When a perimeter network is converted to a Perimeter Cloud, its IP address ranges (its *Cloud Addresses*) include all the addresses behind interfaces (ABIs) of its network interfaces. • For information about ABIs, see Addresses behind network interfaces (on page 478).
Update Cloud Addresses	Specifies whether the task recalculates the IP addresses of Perimeter Clouds and Connecting Clouds whose included addresses are marked as **Automatic (routing based)**. The IP addresses are computed based on the ABIs of the network interfaces connected to the cloud.
Update Asset Assignment to Networks and Clouds	Specifies whether the task: • Attempts assignment of previously unassigned assets to networks and clouds (new clouds might have been created and the IP address ranges of existing clouds might have been updated) by checking whether an IP address of the unassigned asset matches a network or cloud. • Checks if assets that are part of clouds belong there (that is, whether an IP address of the asset matches the updated address ranges of the clouds). If an asset no longer matches a cloud it becomes unassigned and Skybox tries to assign it to a network or another cloud, as explained in the previous bullet. **Note**: This option checks only clouds with **Associate Assets Dynamically** selected.
Connect Incomplete Tunnels	Specifies whether the task attempts to connect incomplete tunnels (if the IP addresses of either or both ends of the tunnel do not match other entities in the model).
Fix Next Hop in Separate Network model issue	In some cases, 2 neighboring devices are not connected in the Skybox model even though they are connected in the real network. This is due to a subnet mask misconfiguration. This property specifies whether the task identifies these devices and connects them by locking their network interfaces to a common network, so that the problem cannot recur on future imports.
Delete Empty Networks	Specifies whether to delete empty networks (that is, networks that contain no assets) from the model.

Property	Description
Create Connecting Clouds for MPLS Networks	Specifies whether to create a Connecting Cloud for PE (provider edge) routers on the same MPLS network. **Note**: Do not modify MPLS configuration. Deletion, addition, or any modification to the MPLS structure including the PEs can cause inconsistency and unexpected behavior.
Addresses to Excluded from Clouds	A list of addresses to exclude from Perimeter and Connecting Cloud addresses. This ensures that source and destination addresses reside within real networks, improving accuracy and performance of access queries.
Access Analyzer Cache Precalculation	The fields in this section specify on which devices (with many access rules) to precalculate access analysis (and add the results to the cache of Access Analyzer). Precalculation speeds up subsequent queries in Access Analyzer.
Limitation Type	Specifies the types of assets that have access analysis precalculated for the Access Analyzer cache.
Precalculate Devices with More Than N Access Rules	This field is displayed if **Limitation Type** = **Devices with too many access rules**. Access analysis is precalculated for devices with at least this many access rules.
Precalculate Specific Devices	This field is displayed if **Limitation Type** = **Specific devices**. A list of devices for which access analysis is precalculated.
Exclude Devices from Recalculation	This field is displayed if **Limitation Type** = **Exclude devices**. Access analysis is precalculated for all devices *except* those listed here.
Calculate Cache for Blocked Destinations	Specifies whether access analysis is precalculated for blocked destinations (instead of precalculating for accessible destinations only).

Validation rules

The validation rules that are always checked by Model completion and validation tasks (see page 318) are listed in the following table.

Validation rule	Severity
Asset	
Asset must have a concrete interface	Error
Asset must not have 2 services on the same port	Error
Asset must not have more than 1 operating system	Error
Asset must not have more than 1 platform	Error
Forwarding asset (router) must have a routing table	Warning
Asset or server must have associated services	Error
Netstatus must be set	Warning
Asset must have a default gateway	Information

Validation rule	**Severity**
Network	
Network must have a valid IP address	Error
Network must have a valid label (or an empty string)	Warning
Network must include interfaces	Warning
Network cannot contain an interface that is outside its range	Error
Network that is not empty (that is, does not contain only routers) should have vulnerability occurrences	Warning
Network cannot have 2 non-virtual or non-load balancer interfaces with the same IP address	Error
Vulnerability occurrence	
Vulnerability occurrence must be associated with a service	Error
Vulnerability Definition of vulnerability occurrence must have a valid catalog ID	Error
Service	
Netstatus must be set	Warning
Service must not have duplicate vulnerability occurrence with the same ID	Warning
Service must have a valid catalog ID	Error
Routing rule	
Routing rule must have a destination	Warning
Routing rule must have non-null gateways	Warning
Routing rule that is attached to an interface must not have more than 1 gateway	Warning
Routing rule must have `asset != null`	Warning
Gateway does not exist in model	Error
Gateway asset exists in model, but is not marked as `is_forwarding`	Error
Access rule	
Access rules must not contain null in `originalRuleText`	Error
If the rule's `Unsupported` flag is **false**, *none* of the following can be null: • `actionType` • `directionType` • `firewallServiceSpace` • `sourceIPSpace` • `targetIPSpace`	Error
If asset is `filtering`, it must have access rules defined	Error
Asset Group	
Asset group must not be an empty group	Error

Validation rule	Severity
Dependency	
Dependency must have an src/dst	Error
Threat Origin	
Threat Origin must have an src	Error
Threat Origin must affect applications	Error

COPY MODEL TASKS

Model – Copy tasks copy a model (Live, What If, or Forensics) to a different model in the Skybox database.

Task properties

The properties that control **Model – Copy** tasks are described in the following table.

Property	Description
Source Model	The model from which to copy.
Target Model	The model to which to copy. **Note**: The model in the Skybox database is overwritten (you cannot copy *to* the Live model).

MODEL INTEGRITY TASKS

Model – Integrity tasks:

- Update mappings in the Skybox database between Business Asset Groups and their members
- Update mappings in the Skybox database between Threat alert tickets and networks (when the tickets have a network scope)
- Update the vulnerability counters

Both the mappings and the counters are subject to change; check them (using a **Model – Integrity** task) every time that the model is updated (see the Model integrity topic in the Skybox Vulnerability Control User Guide).

Task properties

There are no properties specific to **Model – Integrity** tasks.

DELETE OUTDATED ENTITIES TASKS

Model – Outdated Removal tasks delete outdated entities from the model. *Outdated entities* are entities that were not changed recently. When a **Model – Outdated Removal** task runs, it compares the scan time of each entity with the current date and time to establish the entity age. Entities of a specified age are marked as **Down** and older entities are deleted from the model.

Assets, networks, and Perimeter Clouds are ignored by this task if you select **Do Not Outdate** in their Properties dialog box.

Task output

All task messages are written to the *aging* log file on the Skybox Server at `<Skybox_Home>\server\log\aging\aging.log`. A new log file is created for each run of a **Model – Outdated Removal** task; older log files are renamed with a sequential numeric extension. Although the **Messages** tab of the Operational Console is limited to 2000 lines of output, the aging log file contains all output of the task.

Task properties

The properties that control **Model – Outdated Removal** tasks are described in the following table.

Property	Description
Basic tab	
Network Scope	The assets and container entities on which to run the task.
Asset	
Down (days)	The number of days that an asset is missing from a scan before it is marked as **Down**.
Removed (days)	The number of days that an asset is missing from a scan before it is deleted from the model.
Relative Date	The date on which to base outdating of assets.
Service	
Down (days)	The number of days that a service is missing from a scan before it is marked as **Down**.
Removed (days)	The number of days that a service is missing from a scan before it is deleted from the model.
Vulnerability Occurrence	
Not Found (days)	The number of days that a vulnerability occurrence is missing from a scan before it is marked as **Not Found**.
Removed (days)	The number of days that a vulnerability occurrence is missing from a scan before it is deleted from the model.
Advanced tab	
Age unassigned Assets	The age in days for unassigned assets (assets that are not associated with any network) to be deleted from the model.
Exclude Gateways	Specifies whether to exclude gateways (and their associated services, vulnerability occurrences, and network interfaces) from the aging process.
Dry Run	Show the entities that would be deleted from the model using this task, but do not delete them. In a dry run, a list of entities that would be aged by the task is written to the **Messages** tab of the Operational Console and to `aging.log` but the entities are not aged.

BACK UP MODEL AND SETTINGS TASKS

Back Up Model and Settings tasks back up the model and selected settings files. Save the files generated by these tasks to an external location in case they are required for disaster recovery (see the Backing up to an external location topic in the Skybox Installation and Administration Guide). For information about restoring the model, see the Restoring the model topic in the Skybox Installation and Administration Guide.

When you run a **Back Up Model and Settings** task, 2 files are generated:

- `<Skybox_Home>\data\xml_models\xml_backup_task_<date>--<time>.xmlx`
- `<Skybox_Home>\data\settings_backup\settings_backup_<date>--<time>.zip`

To back up the model only (for example, to save historical data to load to the Forensics model), select **Files** > **Models** > **Save** (see the Backing up the model topic in the Skybox Installation and Administration Guide).

Note: You can add a custom list of files and directories to be backed up by these tasks. Specify these files and directories in `<Skybox_Home>\server\conf\user_backup_list.txt`. Instructions and format examples are included in this file.

Task properties

The properties that control **Back Up Model and Settings** tasks are described in the following table.

Property	Description
Model	Specifies whether to back up the model.
Tasks and Report Definitions	Specifies whether to back up tasks and report definitions.
Users	Specifies whether to back up the users.
Dictionary	Specifies whether to back up the Skybox Vulnerability Dictionary.
System	
System Settings	Specifies whether to back up system settings.
Ticket Attachments	Specifies whether to back up ticket attachments.
Reports	Specifies whether to back up recently generated reports.
Reports from the last (days)	Only reports generated within the specified number of days are backed up by the task.

SKYBOX SERVER SOFTWARE UPDATE TASKS

Tools – Server Software Update tasks query the Skybox update management server to see whether an update to Skybox is available.

If an update is available, the task:

1. Downloads the update in the background
2. Adds a notification in the status bar of the Skybox Manager window that an update is available
3. Notifies the user at every login until the update is applied

For information about applying the update, see the Updating the Server and local components topic in the Installation and Administration Guide.

Task properties

There are no properties specific to **Tools – Server Software Update** tasks.

COLLECTOR SOFTWARE UPDATE TASKS

Tools – Collector Software Update tasks send a Skybox Collector software update to a selected Skybox Collector.

The Skybox Server checks the version of all running Collectors on an hourly basis to see whether they need updating; you can run a **Tools – Collector Software Update** task if you do not want to wait until the next update check or if a Collector was down during the scheduled update.

Task properties

There are no properties specific to **Tools – Collector Software Update** tasks.

DICTIONARY UPDATE TASKS

Dictionary – Auto Update tasks update the Vulnerability Dictionary via the internet.

The Skybox Server or a Skybox Collector must be able to connect to the internet to run these tasks. If the Skybox Server or the Skybox Collector machine is configured to connect to the internet via a proxy, configure the proxy settings before downloading a dictionary update file (navigate to **Tools** > **Options** > **Server Options** > **Proxy Settings (Server)**; see the Proxy Settings (Server) topic in the Skybox Installation and Administration Guide).

Task properties

The properties that control **Dictionary – Auto Update** tasks are described in the following table.

Property	Description
Update Dictionary Type	How to collect the Dictionary update file.

For additional information, see the Dictionary updates section in the Skybox Installation and Administration Guide.

Chapter 17

Export tasks

This chapter describes how to set the properties of export tasks (including report and ticket creation tasks).

In this chapter

REPORT GENERATION TASKS

Report – Auto Generation tasks generate a report from a report definition (for reports defined in Skybox Manager, see Automating reports (on page 367)).

After reports are generated, they are available from the Reports workspace.

Task properties

The properties that control **Report – Auto Generation** tasks are described in the following table.

Property	Description
Type	The type of the report that this task generates.
Java Client Reports	This field is enabled only if **Type** = **Java Client Reports**. The report definition from which to generate the report, selected from a list of report definitions defined in Skybox Manager.

Property	Description
Web Client Reports	This field is enabled only if **Type** = **Web Client Reports**. The report definition from which to generate the report, selected from a list of report definitions defined in Skybox Web Client.

TICKET CREATION TASKS

A **Tickets – Auto Generation** task checks all policies. The task:

1. Checks whether conditions of any of the policies are met to create tickets.
2. Creates any necessary tickets.
3. Handles the ticket details.

After tickets are created, view them in the Tickets workspace. Use an analysis (for example, **Public Ticket Analyses** > **All Tickets** > **Open Tickets** > **New**).

For information about working with tickets, see the Tickets and workflow section in the Skybox Vulnerability Control User Guide.

These tasks can also be used to automate the creation of rule recertification tickets for firewall access rules. For information about rule recertification, see the Rule review and recertification chapter in the Skybox Firewall Assurance User Guide.

Task properties

The properties that control **Tickets – Auto Generation** tasks are described in the following table.

Property	Description
Policy Types	The policy types for which to create tickets.

CSV ACCESS RULE REVIEW EXPORT TASKS

CSV – Access Rules Review Export tasks save access rule review results to a CSV file:

- (Skybox Firewall Assurance) You can save results for firewalls and firewall folders
- (Skybox Network Assurance) You can save results for all or part of your organization’s network

When you run a **CSV – Access Rules Review Export** task, a file is created in the specified directory. The file is named:

- (All firewalls) `access_rules_review_All_Firewalls_<date>--<time>.csv`
- (Multiple firewalls) `access_rules_review_<date>--<time>.csv`
- (Single firewall) `access_rules_review_<firewall name>_<IP address>_<date>--<time>.csv`

Task properties

The properties that control **CSV – Access Rules Audit Export** tasks are described in the following table.

Property	Description
Basic tab	
Type	The type of results to export.
Firewall Scope	This field is enabled only if **Type** = **Firewall Assurance**. The firewalls and firewall folders for which to export Configuration Compliance results.
Network Scope	This field is enabled only if **Type** = **Network Assurance**. The assets and container entities for which to export Configuration Compliance results.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Export File Properties	
Directory	The directory under <Skybox_Home> where the output file is saved.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Row Count Limit	The maximum number of rows to output to the CSV file.
Header Row	Specifies whether to add a header row to the output file.
Encoding	The character set to use for encoding the output file.
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is enabled. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

Property	Description
Advanced tab	
Action	Specifies whether to output to the CSV file only access rules that perform a specific action.
Recertification Status	Specifies whether to output to the CSV file only access rules with the selected recertification statuses.
Disabled	Specifies whether to output enabled, disabled, or all access rules to the CSV file.
Created Date	Only access rules created in the specified time frame are output to the CSV file. Select **Custom** to define a date range by: • Specifying the earliest and latest creation dates • Specifying the earliest and latest creation times relative to the current time
Modified Date	Only access rules modified in the specified time frame are output to the CSV file. Select **Custom** to define a date range by: • Specifying the earliest and latest modification dates • Specifying the earliest and latest modification times relative to the current time
Next Review Date	Only access rules with a next review date in the specified time frame are output to the CSV file. Select **Custom** to define a date range by: • Specifying the earliest and latest next review dates • Specifying the earliest and latest next review times relative to the current time

CSV ANALYSIS EXPORT TASKS

CSV – Analysis Export tasks save information from an analysis to a CSV file.

When you run a **CSV – Analysis Export** task, a file named `<analysis name>_<date>--<time>.csv` is created in the specified directory.

Task properties

The properties that control **CSV – Analysis Export** tasks are described in the following table.

Property	Description
Analysis Definition	The analysis to export.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Directory	The directory under <Skybox_Home> where the output file is saved.
Encoding	The character set to use for encoding the output file.
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.

Property	Description
Row Count Limit	The maximum number of rows to output to the CSV file.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Header Row	Specifies whether to add a header row to the output file.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

CSV CHANGE TRACKING EXPORT TASKS

CSV – Analysis Export tasks save information from an analysis to a CSV file.

When you run a **CSV – Analysis Export** task, a file named `<analysis name>_<date>--<time>.csv` is created in the specified directory.

Task properties

The properties that control **CSV – Analysis Export** tasks are described in the following table.

Property	Description
Analysis Definition	The analysis to export.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Directory	The directory under <Skybox_Home> where the output file is saved.
Encoding	The character set to use for encoding the output file.

Property	**Description**
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Row Count Limit	The maximum number of rows to output to the CSV file.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Header Row	Specifies whether to add a header row to the output file.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

CSV COMPLIANCE RESULTS EXPORT TASKS

CSV – Analysis Export tasks save information from an analysis to a CSV file.

When you run a **CSV – Analysis Export** task, a file named `<analysis name>_<date>--<time>.csv` is created in the specified directory.

Task properties

The properties that control **CSV – Analysis Export** tasks are described in the following table.

Property	**Description**
Analysis Definition	The analysis to export.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Directory	The directory under <Skybox_Home> where the output file is saved.

Property	Description
Encoding	The character set to use for encoding the output file.
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Row Count Limit	The maximum number of rows to output to the CSV file.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Header Row	Specifies whether to add a header row to the output file.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

CSV CONFIGURATION COMPLIANCE EXPORT TASKS

CSV – Configuration Compliance Export tasks save Configuration Compliance results to a CSV file:

- (Skybox Firewall Assurance) You can save results for firewalls and firewall folders, for some of or all the available Configuration Policies
- (Skybox Network Assurance) You can save results for some of or all the available Configuration Policies and all or part of your organization's network

When you run a **CSV – Configuration Compliance Export** task, a file is created in the specified directory. The file name depends on the value of **Type**:

- **Network Assurance**
  - (All Configuration Policies) `fw_config_compliance_All_PolicyConfigChecks_<date>--<time>.csv`
  - (Multiple Configuration Policies or Configuration Checks) `fw_config_compliance_<date>--<time>.csv`

- (Single Configuration Policy or Configuration Check) `fw_config_compliance_<entity name>_<date>--<time>.csv`

› **Firewall Assurance**

- (All firewalls) `fw_config_compliance_All_Firewalls_<date>--<time>.csv`
- (Multiple firewalls) `fw_config_compliance_<date>--<time>.csv`
- (Single firewall) `fw_config_compliance_<firewall name>_<IP address>_<date>--<time>.csv`

Task properties

The properties that control **CSV – Configuration Compliance Export** tasks are described in the following table.

Property	Description
Type	The type of results to export.
Firewall Scope	This field is enabled only if **Type** = **Firewall Assurance**. The firewalls and firewall folders for which to export Configuration Compliance results.
Policy Scope	The parts of the Configuration Policies (policy folders, policies, or Configuration Checks) for which to export compliance results.
Network Scope	This field is enabled only if **Type** = **Network Assurance**. The assets and container entities for which to export Configuration Compliance results.
Asset Type	The asset types to export.
Violations Scope	The compliance results to export. Specifies whether to include only violations or all tests in the output file. The exported content depends on the value selected: • **All Tests**: All access tests (compliant tests and violations) for each firewall are exported. • **Violations Only**: Only violations are exported. • **New Violations**: Only new violations (according to the definition in **Tools** > **Options** > **Server Options** > **Entity Settings**) are exported.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Export File Properties	
Directory	The directory under <Skybox_Home> where the output file is saved.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Row Count Limit	The maximum number of rows to output to the CSV file.
Header Row	Specifies whether to add a header row to the output file.
Encoding	The character set to use for encoding the output file.

Property	**Description**
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

CSV EXCEPTION EXPORT TASKS

CSV – Exception Export tasks save policy exceptions to a CSV file.

When you run a **CSV – Exception Export** task, a file named `<product type>_<exception type>_Exceptions_<date>--<time>.csv` is created in the specified directory.

Task properties

The properties that control **CSV – Exception Export** tasks are described in the following table.

Property	**Description**
Product Type	The type of results to export.
Firewall Scope	This field is enabled only if **Product Type** = **Firewall Assurance**. The firewalls and firewall folders for which to export exceptions.
Exception Type	This field is enabled only if **Product Type** = **Firewall Assurance**. The type of exceptions to export.
Access Policy Scope	The parts of the Access Policy (policy folders, policy sections, or Access Checks) for which to export exceptions.

Property	Description
Rule Policy Scope	This field is enabled only if **Exception Type** = **Rule Policy**. The parts of the Rule Policy (policy folders or Rule Checks) for which to export exceptions.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Export File Properties	
Directory	The directory under <Skybox_Home> where the output file is saved.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Row Count Limit	The maximum number of rows to output to the CSV file.
Header Row	Specifies whether to add a header row to the output file.
Encoding	The character set to use for encoding the output file.
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

CSV FIREWALL ASSURANCE EXPORT TASKS

CSV – Firewall Assurance Export tasks save firewall summary information from selected firewalls to a CSV file.

When you run a **CSV – Firewall Assurance Export** task, a file is created in the specified directory. The file is named:

- (All firewalls) `fw_summary_All_Firewalls_<date>--<time>.csv`
- (Multiple firewalls) `fw_summary_<date>--<time>.csv`
- (Single firewall) `fw_summary_<firewall name>_<IP address>_<date>--<time>.csv`

Task properties

The properties that control **CSV – Firewall Assurance Export** tasks are described in the following table.

Property	Description
Firewall Scope	The firewalls and firewall folders whose data is exported.
Exported Information	The type of information to export.
Change Tracking Period	The time frame of the data to export. • **Custom**: Select **Specific** or **Relative** start and end times.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Export File Properties	
Directory	The directory under <Skybox_Home> where the output file is saved.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Row Count Limit	The maximum number of rows to output to the CSV file.
Header Row	Specifies whether to add a header row to the output file.
Encoding	The character set to use for encoding the output file.
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.

Property	Description
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

CSV NETWORK ASSURANCE EXPORT TASKS

CSV – Network Assurance Export tasks save device summary information from selected networks to a CSV file.

When you run a **CSV – Network Assurance Export** task, a file is created in the specified directory. The file is named:

- (All networks) `network_assurance_All_<date>--<time>.csv`
- (Multiple networks) `network_assurance_<date>--<time>.csv`
- (Single networks) `network_assurance_<network name>_<date>--<time>.csv`

Task properties

The properties that control **CSV – Network Assurance Export** tasks are described in the following table.

Property	Description
Network Scope	The networks and network folders whose data is exported.
Device Type	The device types whose data is exported.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Export File Properties	
Directory	The directory under <Skybox_Home> where the output file is saved.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Row Count Limit	The maximum number of rows to output to the CSV file.
Header Row	Specifies whether to add a header row to the output file.
Encoding	The character set to use for encoding the output file.
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Mail to Recipients	

Property	Description
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

CSV OPTIMIZATION AND CLEANUP EXPORT TASKS

CSV – Optimization and Cleanup Export tasks save optimization and cleanup information (either shadowed and redundant rules, rule usage data, duplicate objects, or unreferenced objects) from selected firewalls to a CSV file.

When you run a **CSV – Optimization and Cleanup Export** task, a file is created in the specified directory. The file is named:

- (All firewalls) `fw_<report type>_All_Firewalls_<date>--<time>.csv`
- (Multiple firewalls) `fw_<report type>_<date>--<time>.csv`
- (Single firewall) `fw_<report type>_<firewall name>_<IP address>_<date>--<time>.csv`

Task properties

The properties that control **CSV – Optimization and Cleanup Export** tasks are described in the following table.

Property	Description
Report Type	The type of report whose data is exported.
Firewall Scope	The firewalls and firewall folders whose data is exported.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.

Property	Description
Period	This field is hidden if **Report Type** = **Unreferenced Objects** or **Report Type** = **Duplicate Objects**. The time frame of the data to export. • **Custom**: Select **Specific** or **Relative** start and end times.
Global Rules and Objects	This field is displayed only if **Report Type** = **Rule Usage**. Specifies whether, when global rules and objects are used in the firewall, all the information for each rule or object is consolidated to 1 line in the output file.
Global Rules	This field is displayed only if **Report Type** = **Rule Usage with Trace Data**. Specifies whether, when global rules are used in the firewall, all the information for each rule is consolidated to 1 line in the output file.
Export File Properties	
Directory	The directory under <Skybox_Home> where the output file is saved.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Row Count Limit	The maximum number of rows to output to the CSV file.
Header Row	Specifies whether to add a header row to the output file.
Encoding	The character set to use for encoding the output file.
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

CSV SECURITY METRICS EXPORT TASKS

CSV – Security Metrics Export tasks save the security metrics information of a Business Unit or Business Asset Group to a CSV file.

When you run a **CSV – Security Metrics Export** task, a file named `security_profile_<business unit>_<date>--<time>.csv` is created in the specified directory (`<business unit>` is the Business Asset Group or Business Unit selected in **Business Unit**).

Task properties

The properties that control **CSV – Security Metrics Export** tasks are described in the following table.

Property	Description
Security Metric Type	The type of security metrics information to export.
Business Unit	The Business Unit or Business Asset Group for which to export the security metrics information.
CSV Columns	Specifies the information to export and its order in each row. Click the **Browse** button to open the CSV Columns dialog box.
Export File Properties	
Directory	The directory under <Skybox_Home> where the output file is saved.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Row Count Limit	The maximum number of rows to output to the CSV file.
Header Row	Specifies whether to add a header row to the output file.
Encoding	The character set to use for encoding the output file.
Delimiter	The CSV file delimiter. For tab-separated files, use the 2-character string `\t`.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.
Elasticsearch	This section is displayed if Skybox is configured to work with Elasticsearch.
Export to Elasticsearch	Specifies whether to index the data into Elasticsearch.

Property	Description
Add Date to Index Name	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to add the date of the export to the Elasticsearch index name.
MSSP Mode	This field is enabled only if **Export to Elasticsearch** is selected. Specifies whether to work in *MSSP mode*. In MSSP mode, your documents are reindexed; documents of other users are not affected.

ELASTICSEARCH INDEX EXPORT TASKS

You can generate Elasticsearch indices using an **Elasticsearch – Index Export** task.

Note: The task is only available after you configure Skybox to work with an Elasticsearch server; see the Elasticsearch and Skybox topic in the Skybox Installation and Administration Guide.

Task properties

The properties that control **Elasticsearch – Index Export** tasks are described in the following table.

Property	Description
Elasticsearch Indices	The entities to index
Add Date to Index Name	Specifies whether to add the current date to the generated index name
Asset Geolocations	Specifies whether to perform geolocation on the IP addresses of the indexed assets
Force Indexing	Specifies whether to index even if no changes to the data values are detected
Update Mode	Specifies whether to index in *update mode*. In update mode new entities are added to the index, existing entities are updated in the index, and deleted entities are kept as is.
Indexing target	Specifies whether to index into an external Elasticsearch instance or the internal instance.

SPLUNK EXPORT TASKS

You can export Skybox database indices to a Splunk HTTP Event Collector (HEC) using a **Backup and Export Tasks – Export to Splunk** task.

Task properties

The properties that control **Backup and Export Tasks – Export to Splunk** tasks are described in the following table.

Property	Description
Host	The IP address of the machine hosting the Splunk HEC.
Port	The port of the Splunk HEC.
Token	The token for connecting to the Splunk HEC.
Use SSL	Specifies whether the Splunk HEC is configured via HTTPS.
Debug	Specifies whether to print to a debug log the JSONs sent to the Splunk HEC.
Indices	The Skybox data types to index into Splunk.

QUALYS FORMAT XML VULNERABILITY OCCURRENCES EXPORT TASKS

XML Vulnerability Occurrence (Qualys Format) Export tasks save information from a vulnerability occurrences analysis to an XML file in Qualys format.

When you run an **XML Vulnerability Occurrence (Qualys Format) Export** task, a file named `<analysis name>_<date>--<time>.xml` is created in the specified directory.

Task properties

The properties that control **XML Vulnerability Occurrence (Qualys Format) Export** tasks are described in the following table.

Property	Description
Analysis Definition	The vulnerability occurrences analysis whose results are exported.
Directory	The directory under <Skybox_Home> where the output file is saved.
Encoding	The character set to use for encoding the output file.
Row Count Limit	The maximum number of rows to output to the XML file.
Timestamp	Specifies whether to add a timestamp to each row of the output file.
Mail to Recipients	
Skybox Users	The Skybox users who receive the output file as an email attachment.
External Email Addresses	External users (represented by a comma-separated list of email addresses) who receive the output file as an email attachment.
Compress File	Specifies whether email recipients receive the output file in compressed (ZIP) format.

Part II: Tickets, reports, and notifications

This part describes Skybox analyses, tickets, reports, and triggers.

Chapter 18

Analyses

This chapter describes Skybox *analyses*—queries about entities in your network.

In this chapter

SKYBOX ANALYSES

A Skybox *analysis* is a query about a type of entity in your network. When you select an analysis, Skybox checks for entities of the selected type that meet the specified criteria. Entities that meet all criteria specified in the analysis are listed in the Table pane.

Regular expression support in analyses

All analysis types support both string values (including wildcards) and full regular expressions for string fields.

- T in a string field means that the value of the field is interpreted as a text string.
- .* in a string field means that the value of the field is interpreted as a regular expression.

Click the icon to toggle to the other icon.

CUSTOMIZING THE DISPLAY OF AN ANALYSIS

You can customize the view of an analysis by hiding columns, displaying additional columns, or repositioning columns in the display. The available columns depend on the analysis type.

To customize the display of an analysis:

- Right-click a column header and select from the following options:
  - **Remove This Column**
  - **Customize Current View**: The Customize Current View dialog box lists the columns that can be displayed in this analysis. Use this to:
    - Display additional columns
    - Hide multiple columns
    - Reposition columns in the display
  - **Sort**: Sort the list by the selected column

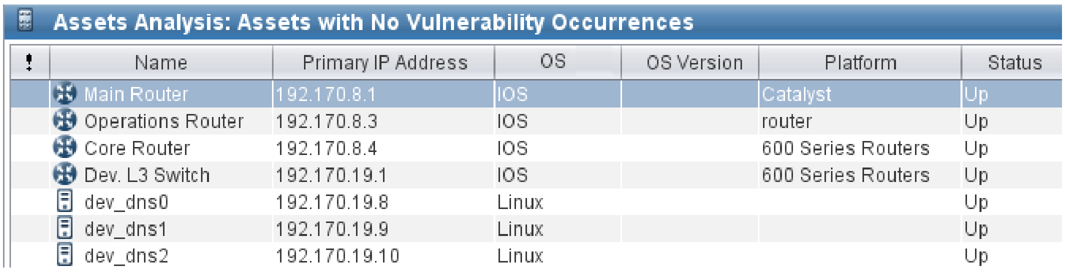
- **Group**: Group the entities in the table according to the content of the selected column
- **AutoFilter**: Filter the table by a value in the selected column

TYPES OF ANALYSES

Skybox includes the analyses listed in the following tables.

Model workspace (all products)

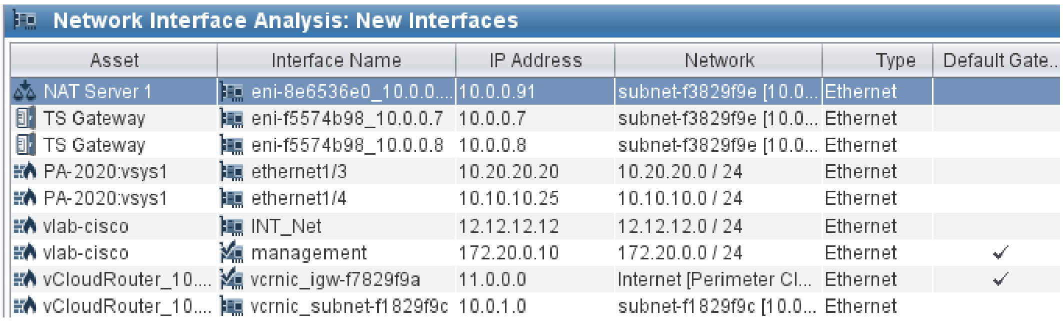
Analysis type	Displays a list of...
Assets validation	Assets, including servers, gateways, and workstations. For each asset, you can see its name, primary IP address, operating system and platform information, and network status. You can view asset information in the context of risk in the Exposure workspace.



Assets Analysis: Assets with No Vulnerability Occurrences

!	Name	Primary IP Address	OS	OS Version	Platform	Status
	Main Router	192.170.8.1	IOS		Catalyst	Up
	Operations Router	192.170.8.3	IOS		router	Up
	Core Router	192.170.8.4	IOS		600 Series Routers	Up
	Dev. L3 Switch	192.170.19.1	IOS		600 Series Routers	Up
	dev_dns0	192.170.19.8	Linux			Up
	dev_dns1	192.170.19.9	Linux			Up
	dev_dns2	192.170.19.10	Linux			Up

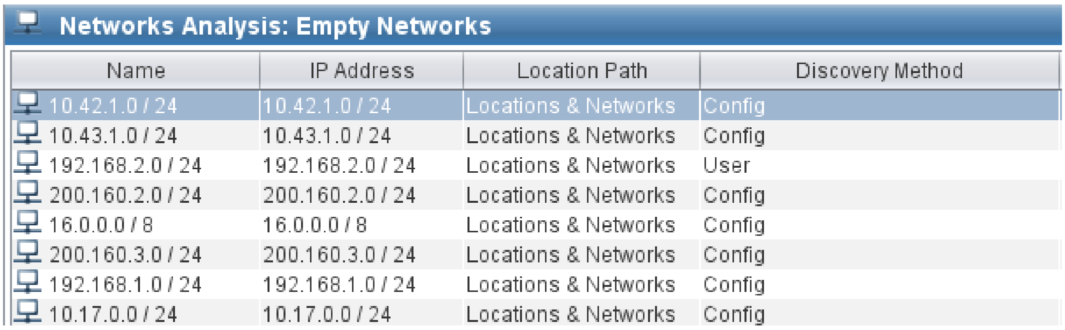
Analysis type	Displays a list of...
Network interfaces validation	Network interfaces. Use these analyses to complete and fix the network model. For example, use them to find network interfaces with missing next hops, to help identify edges of the model, and to help discover missing networks. For each network interface, you can see its IP address, location path, and discovery method.



Network Interface Analysis: New Interfaces

Asset	Interface Name	IP Address	Network	Type	Default Gate..
NAT Server 1	eni-8e6536e0_10.0.0....	10.0.0.91	subnet-f3829f9e [10.0...	Ethernet	
TS Gateway	eni-f5574b98_10.0.0.7	10.0.0.7	subnet-f3829f9e [10.0...	Ethernet	
TS Gateway	eni-f5574b98_10.0.0.8	10.0.0.8	subnet-f3829f9e [10.0...	Ethernet	
PA-2020:vsys1	ethernet1/3	10.20.20.20	10.20.20.0 / 24	Ethernet	
PA-2020:vsys1	ethernet1/4	10.10.10.25	10.10.10.0 / 24	Ethernet	
vlab-cisco	INT_Net	12.12.12.12	12.12.12.0 / 24	Ethernet	
vlab-cisco	management	172.20.0.10	172.20.0.0 / 24	Ethernet	✓
vCloudRouter_10....	vcrnic_igw-f7829f9a	11.0.0.0	Internet [Perimeter Cl...	Ethernet	✓
vCloudRouter_10....	vcrnic_subnet-f1829f9c	10.0.1.0	subnet-f1829f9c [10.0...	Ethernet	

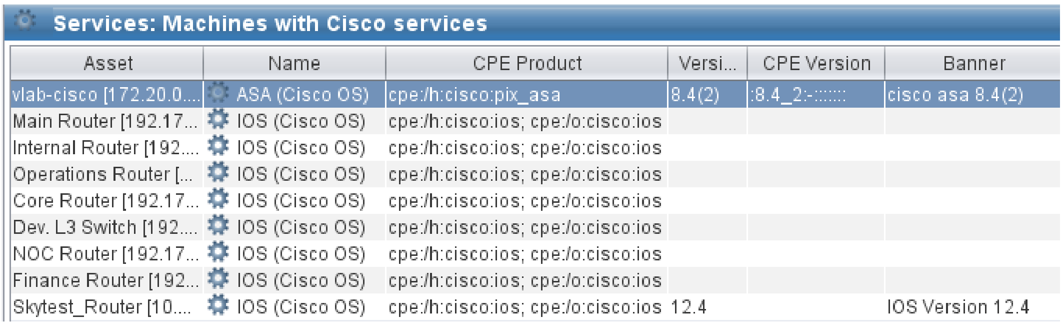
Analysis type	Displays a list of...
Networks validation	Networks. These analyses check for problems in networks, typically to verify whether the networks were imported correctly. For each network, you can see its IP address, location path, and discovery method. To view network information in the context of risk, use the Exposure workspace.



Networks Analysis: Empty Networks

Name	IP Address	Location Path	Discovery Method
10.42.1.0 / 24	10.42.1.0 / 24	Locations & Networks	Config
10.43.1.0 / 24	10.43.1.0 / 24	Locations & Networks	Config
192.168.2.0 / 24	192.168.2.0 / 24	Locations & Networks	User
200.160.2.0 / 24	200.160.2.0 / 24	Locations & Networks	Config
16.0.0.0 / 8	16.0.0.0 / 8	Locations & Networks	Config
200.160.3.0 / 24	200.160.3.0 / 24	Locations & Networks	Config
192.168.1.0 / 24	192.168.1.0 / 24	Locations & Networks	Config
10.17.0.0 / 24	10.17.0.0 / 24	Locations & Networks	Config

Analysis type	Displays a list of...
Services validation	Services. Use these analyses after import to review the products (installed on assets) that exist in the model and their level of identification.

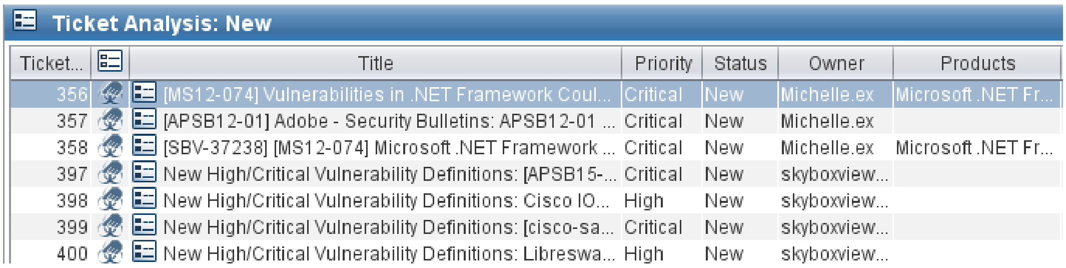


Services: Machines with Cisco services

Asset	Name	CPE Product	Versi...	CPE Version	Banner
vlab-cisco [172.20.0....	ASA (Cisco OS)	cpe:/h:cisco:pix_asa	8.4(2)	:8.4_2:-::::::	cisco asa 8.4(2)
Main Router [192.17...	IOS (Cisco OS)	cpe:/h:cisco:ios; cpe:/o:cisco:ios			
Internal Router [192....	IOS (Cisco OS)	cpe:/h:cisco:ios; cpe:/o:cisco:ios			
Operations Router [...	IOS (Cisco OS)	cpe:/h:cisco:ios; cpe:/o:cisco:ios			
Core Router [192.17...	IOS (Cisco OS)	cpe:/h:cisco:ios; cpe:/o:cisco:ios			
Dev. L3 Switch [192....	IOS (Cisco OS)	cpe:/h:cisco:ios; cpe:/o:cisco:ios			
NOC Router [192.17...	IOS (Cisco OS)	cpe:/h:cisco:ios; cpe:/o:cisco:ios			
Finance Router [192...	IOS (Cisco OS)	cpe:/h:cisco:ios; cpe:/o:cisco:ios			
Skytest_Router [10....	IOS (Cisco OS)	cpe:/h:cisco:ios; cpe:/o:cisco:ios	12.4		IOS Version 12.4

Tickets workspace (all products)

Analysis type	Displays a list of...
Tickets	Tickets. For each ticket, you can see the ticket ID, ticket type, title, asset, vulnerability occurrence or Vulnerability Definition, owner, priority, due date, and status.

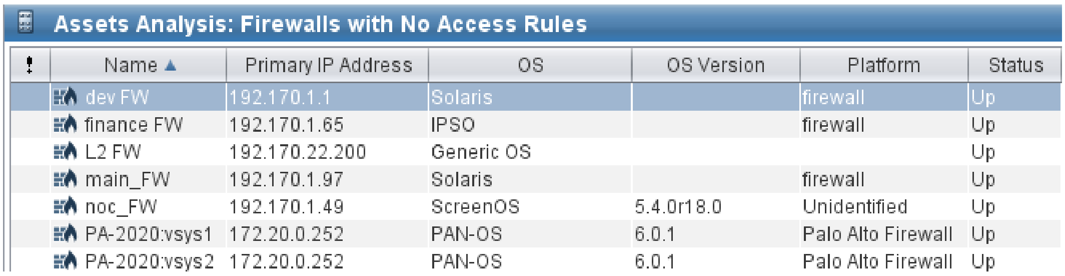


Ticket Analysis: New

Ticket...	☰	Title	Priority	Status	Owner	Products
356		[MS12-074] Vulnerabilities in .NET Framework Coul...	Critical	New	Michelle.ex	Microsoft .NET Fr...
357		[APSB12-01] Adobe - Security Bulletins: APSB12-01 ...	Critical	New	Michelle.ex	
358		[SBV-37238] [MS12-074] Microsoft .NET Framework ...	Critical	New	Michelle.ex	Microsoft .NET Fr...
397		New High/Critical Vulnerability Definitions: [APSB15-...	Critical	New	skyboxview...	
398		New High/Critical Vulnerability Definitions: Cisco IO...	High	New	skyboxview...	
399		New High/Critical Vulnerability Definitions: [cisco-sa...	Critical	New	skyboxview...	
400		New High/Critical Vulnerability Definitions: Libreswa...	High	New	skyboxview...	

Firewall Assurance workspace

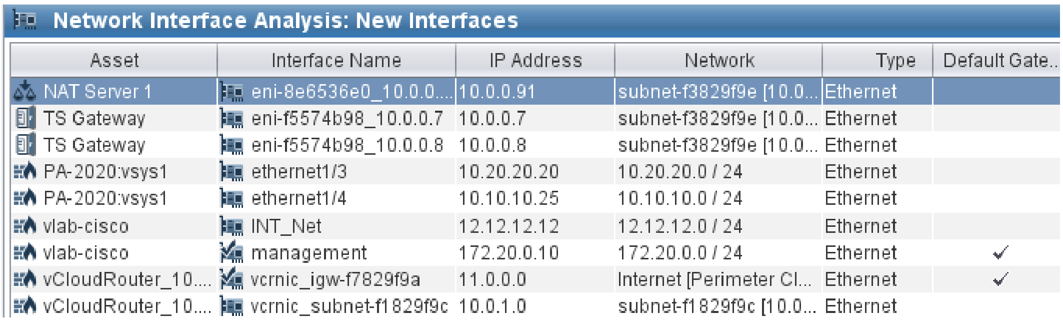
Analysis type	Displays a list of...
Assets	Assets, usually firewalls. For each asset, you can see its name, primary IP address, operating system and platform information, and network status.



Assets Analysis: Firewalls with No Access Rules

!	Name ▲	Primary IP Address	OS	OS Version	Platform	Status
	dev FW	192.170.1.1	Solaris		firewall	Up
	finance FW	192.170.1.65	IPSO		firewall	Up
	L2 FW	192.170.22.200	Generic OS			Up
	main_FW	192.170.1.97	Solaris		firewall	Up
	noc_FW	192.170.1.49	ScreenOS	5.4.0r18.0	Unidentified	Up
	PA-2020:vsys1	172.20.0.252	PAN-OS	6.0.1	Palo Alto Firewall	Up
	PA-2020:vsys2	172.20.0.252	PAN-OS	6.0.1	Palo Alto Firewall	Up

Analysis type	Displays a list of...
Network interfaces	Network interfaces. Use these analyses to complete and fix the network model. For example, use them to find network interfaces with missing next hops, to help identify edges of the model, and to help discover missing networks. For each network interface, you can see its IP address, location path, and discovery method.

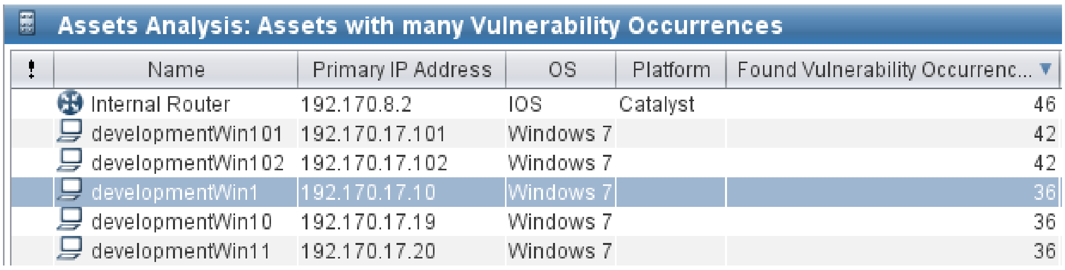


Network Interface Analysis: New Interfaces

Asset	Interface Name	IP Address	Network	Type	Default Gate..
NAT Server 1	eni-8e6536e0_10.0.0....	10.0.0.91	subnet-f3829f9e [10.0...	Ethernet	
TS Gateway	eni-f5574b98_10.0.0.7	10.0.0.7	subnet-f3829f9e [10.0...	Ethernet	
TS Gateway	eni-f5574b98_10.0.0.8	10.0.0.8	subnet-f3829f9e [10.0...	Ethernet	
PA-2020:vsys1	ethernet1/3	10.20.20.20	10.20.20.0 / 24	Ethernet	
PA-2020:vsys1	ethernet1/4	10.10.10.25	10.10.10.0 / 24	Ethernet	
vlab-cisco	INT_Net	12.12.12.12	12.12.12.0 / 24	Ethernet	
vlab-cisco	management	172.20.0.10	172.20.0.0 / 24	Ethernet	✓
vCloudRouter_10....	vcrnic_igw-f7829f9a	11.0.0.0	Internet [Perimeter Cl...	Ethernet	✓
vCloudRouter_10....	vcrnic_subnet-f1829f9c	10.0.1.0	subnet-f1829f9c [10.0...	Ethernet	

Exposure workspace

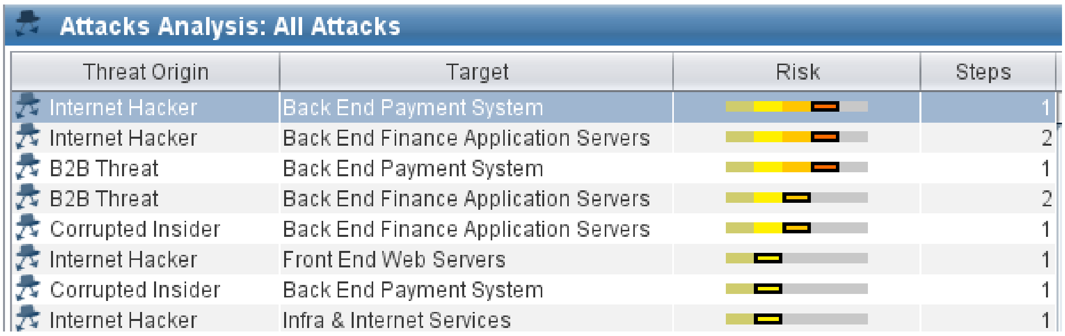
Analysis type	Displays a list of...
Assets	Assets, including servers, gateways, and workstations. For each asset, you can see its name, primary IP address, operating system and platform information, and network status. To view validation information about assets (for example, a list of assets with no vulnerability occurrences or gateways with no routing rules) use Asset validation analyses.



Assets Analysis: Assets with many Vulnerability Occurrences

!	Name	Primary IP Address	OS	Platform	Found Vulnerability Occurrenc... ▼
	Internal Router	192.170.8.2	IOS	Catalyst	46
	developmentWin101	192.170.17.101	Windows 7		42
	developmentWin102	192.170.17.102	Windows 7		42
	developmentWin1	192.170.17.10	Windows 7		36
	developmentWin10	192.170.17.19	Windows 7		36
	developmentWin11	192.170.17.20	Windows 7		36

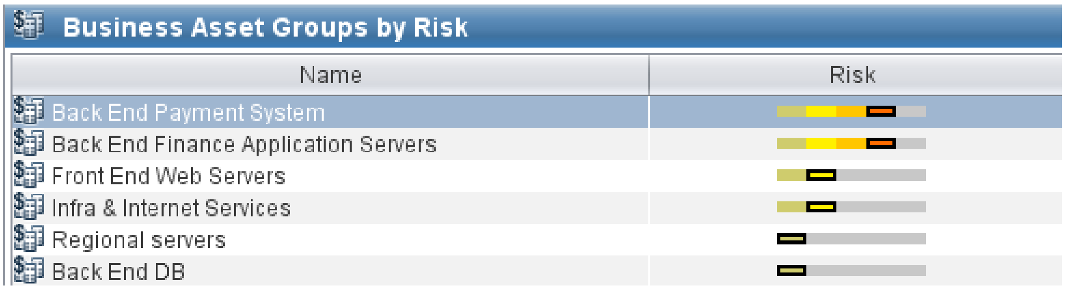
Analysis type	Displays a list of...
Attacks	Attacks. For each attack, you can see the Threat Origin, the destination, the risk, and the shortest number of steps it takes to get from the Threat Origin to the destination.



Attacks Analysis: All Attacks

Threat Origin	Target	Risk	Steps
Internet Hacker	Back End Payment System		1
Internet Hacker	Back End Finance Application Servers		2
B2B Threat	Back End Payment System		1
B2B Threat	Back End Finance Application Servers		2
Corrupted Insider	Back End Finance Application Servers		1
Internet Hacker	Front End Web Servers		1
Corrupted Insider	Back End Payment System		1
Internet Hacker	Infra & Internet Services		1

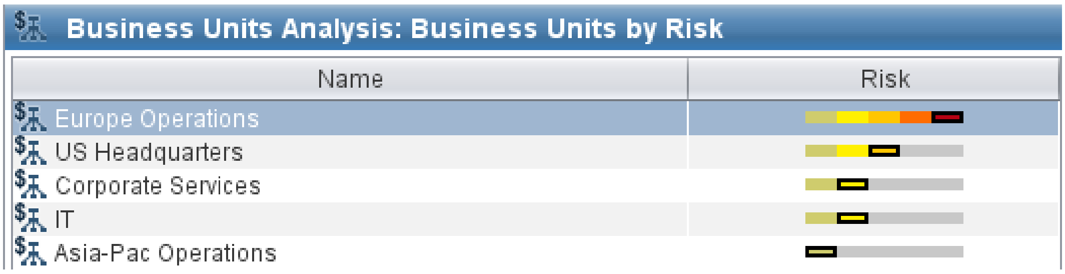
Analysis type	Displays a list of...
Business Asset Groups	Business Asset Groups. For each Business Asset Group, you can see its total risk.



Business Asset Groups by Risk

Name	Risk
Back End Payment System	
Back End Finance Application Servers	
Front End Web Servers	
Infra & Internet Services	
Regional servers	
Back End DB	

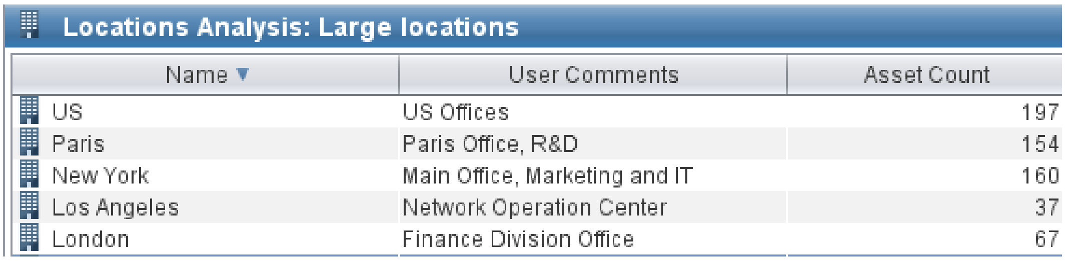
Analysis type	Displays a list of...
Business Units	Business Units. For each Business Unit, you can see its total risk.



Business Units Analysis: Business Units by Risk

Name	Risk
Europe Operations	
US Headquarters	
Corporate Services	
IT	
Asia-Pac Operations	

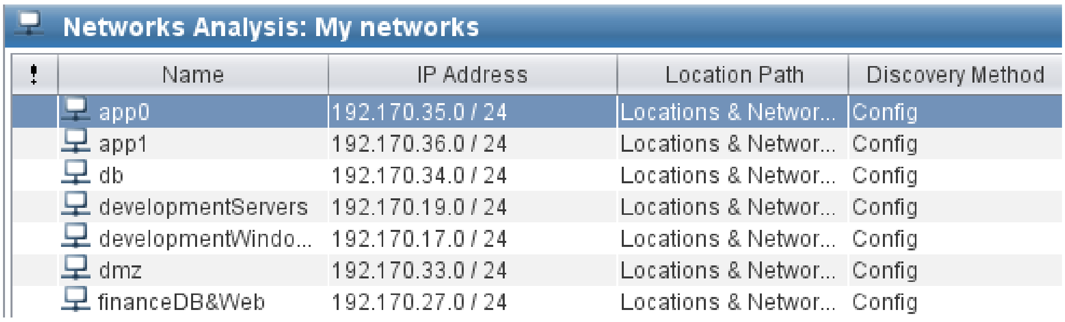
Analysis type	Displays a list of...
Locations	Locations. For each location, you see the user comment (description).



Locations Analysis: Large locations

Name ▼	User Comments	Asset Count
US	US Offices	197
Paris	Paris Office, R&D	154
New York	Main Office, Marketing and IT	160
Los Angeles	Network Operation Center	37
London	Finance Division Office	67

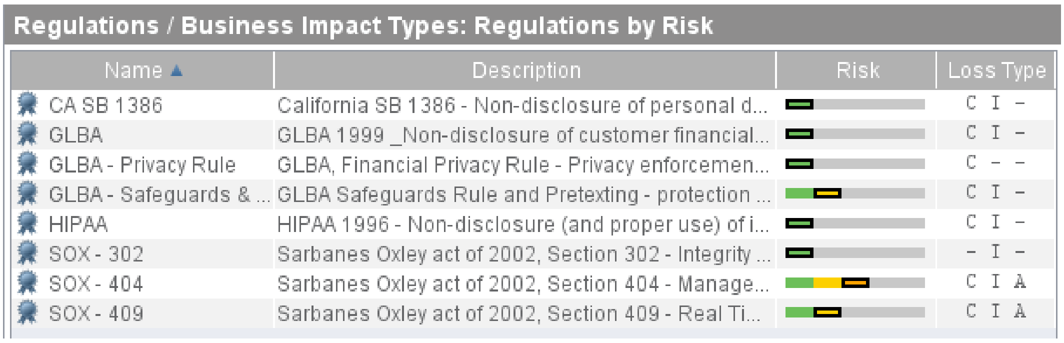
Analysis type	Displays a list of...
Networks	Networks. For each network, you can see its IP address, location path, and discovery method. You can filter the analysis to display only specific network types, only segmented networks, and so on.



Networks Analysis: My networks

!	Name	IP Address	Location Path	Discovery Method
	app0	192.170.35.0 / 24	Locations & Networ...	Config
	app1	192.170.36.0 / 24	Locations & Networ...	Config
	db	192.170.34.0 / 24	Locations & Networ...	Config
	developmentServers	192.170.19.0 / 24	Locations & Networ...	Config
	developmentWindo...	192.170.17.0 / 24	Locations & Networ...	Config
	dmz	192.170.33.0 / 24	Locations & Networ...	Config
	financeDB&Web	192.170.27.0 / 24	Locations & Networ...	Config

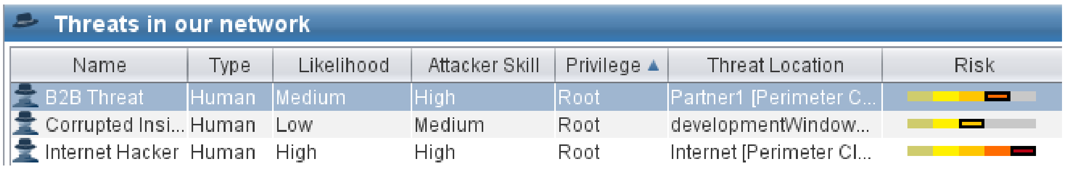
Analysis type	Displays a list of...
Regulation Compliance	Regulations and Business Impacts. For each Regulation or Business Impact, you can see its description, risk, and loss type (CIA).



Regulations / Business Impact Types: Regulations by Risk

Name ▲	Description	Risk	Loss Type
CA SB 1386	California SB 1386 - Non-disclosure of personal d...		C I -
GLBA	GLBA 1999 _Non-disclosure of customer financial...		C I -
GLBA - Privacy Rule	GLBA, Financial Privacy Rule - Privacy enforcemen...		C - -
GLBA - Safeguards & ...	GLBA Safeguards Rule and Pretexting - protection ...		C I -
HIPAA	HIPAA 1996 - Non-disclosure (and proper use) of i...		C I -
SOX - 302	Sarbanes Oxley act of 2002, Section 302 - Integrity ...		- I -
SOX - 404	Sarbanes Oxley act of 2002, Section 404 - Manage...		C I A
SOX - 409	Sarbanes Oxley act of 2002, Section 409 - Real Ti...		C I A

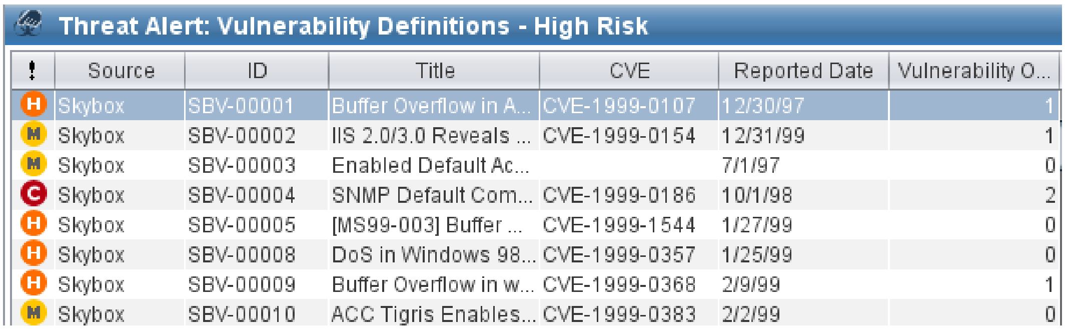
Analysis type	Displays a list of...
Threat Origins	Threat Origins. For each Threat Origin, you can see its likelihood to attack, attacker skill, attacker privilege, and risk.



Threats in our network

Name	Type	Likelihood	Attacker Skill	Privilege ▲	Threat Location	Risk
B2B Threat	Human	Medium	High	Root	Partner1 [Perimeter C...	
Corrupted Insi...	Human	Low	Medium	Root	developmentWindow...	
Internet Hacker	Human	High	High	Root	Internet [Perimeter Cl...	

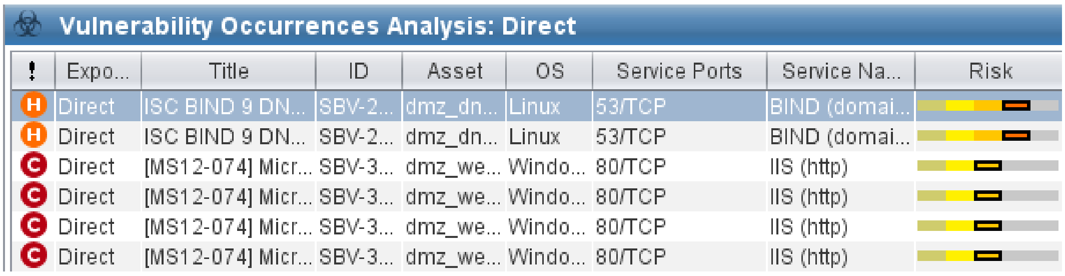
Analysis type	Displays a list of...
Vulnerability Definitions	Vulnerability Definitions. For each Vulnerability Definition, you can see severity, title, ID of the Vulnerability Definition in the Skybox Vulnerability Dictionary and CVE ID, reported date, vulnerability occurrence count, and so on. **Note**: The severity indicator (Critical, High, Medium, and so on) uses Skybox severity levels. However, in some cases the source may have marked the Vulnerability Definition with a different severity that does not match the Skybox severity.



Threat Alert: Vulnerability Definitions - High Risk

!	Source	ID	Title	CVE	Reported Date	Vulnerability O...
H	Skybox	SBV-00001	Buffer Overflow in A...	CVE-1999-0107	12/30/97	1
M	Skybox	SBV-00002	IIS 2.0/3.0 Reveals ...	CVE-1999-0154	12/31/99	1
M	Skybox	SBV-00003	Enabled Default Ac...		7/1/97	0
C	Skybox	SBV-00004	SNMP Default Com...	CVE-1999-0186	10/1/98	2
H	Skybox	SBV-00005	[MS99-003] Buffer ...	CVE-1999-1544	1/27/99	0
H	Skybox	SBV-00008	DoS in Windows 98...	CVE-1999-0357	1/25/99	0
H	Skybox	SBV-00009	Buffer Overflow in w...	CVE-1999-0368	2/9/99	1
M	Skybox	SBV-00010	ACC Tigris Enables...	CVE-1999-0383	2/2/99	0

Analysis type	Displays a list of...
Vulnerability occurrences	Vulnerability occurrences. For each vulnerability occurrence, you can see severity, exposure, title, ID of the Vulnerability Definition in the Skybox Vulnerability Dictionary and CVE ID, information about the asset on which the vulnerability occurrence is found, risk, and whether a ticket is already open for this vulnerability occurrence.

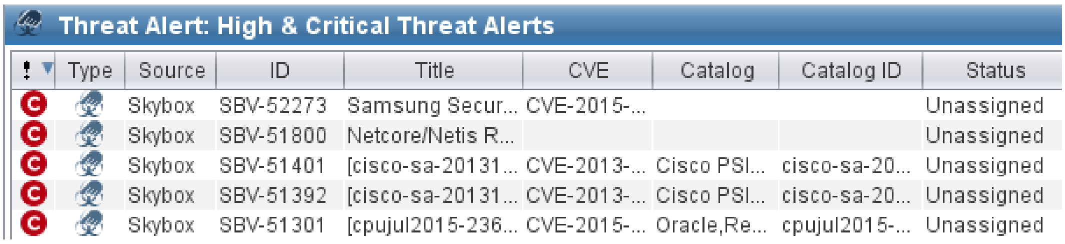


Vulnerability Occurrences Analysis: Direct

!	Expo...	Title	ID	Asset	OS	Service Ports	Service Na...	Risk
H	Direct	ISC BIND 9 DN...	SBV-2...	dmz_dn...	Linux	53/TCP	BIND (domai...	
H	Direct	ISC BIND 9 DN...	SBV-2...	dmz_dn...	Linux	53/TCP	BIND (domai...	
C	Direct	[MS12-074] Micr...	SBV-3...	dmz_we...	Windo...	80/TCP	IIS (http)	
C	Direct	[MS12-074] Micr...	SBV-3...	dmz_we...	Windo...	80/TCP	IIS (http)	
C	Direct	[MS12-074] Micr...	SBV-3...	dmz_we...	Windo...	80/TCP	IIS (http)	
C	Direct	[MS12-074] Micr...	SBV-3...	dmz_we...	Windo...	80/TCP	IIS (http)	

Threat Manager workspace

Analysis type	Displays a list of...
Threat alerts	Threat alerts. For each threat alert, you can see severity, source, source ID, title, CVE ID, reported date and modification date, status, and whether the threat alert is marked as **For Review**.



Threat Alert: High & Critical Threat Alerts

!	Type	Source	ID	Title	CVE	Catalog	Catalog ID	Status
C		Skybox	SBV-52273	Samsung Secur...	CVE-2015-...			Unassigned
C		Skybox	SBV-51800	Netcore/Netis R...				Unassigned
C		Skybox	SBV-51401	[cisco-sa-20131...	CVE-2013-...	Cisco PSI...	cisco-sa-20...	Unassigned
C		Skybox	SBV-51392	[cisco-sa-20131...	CVE-2013-...	Cisco PSI...	cisco-sa-20...	Unassigned
C		Skybox	SBV-51301	[cpujul2015-236...	CVE-2015-...	Oracle,Re...	cpujul2015-...	Unassigned

Chapter 19

Tickets reference

This chapter describes how to set the properties for Skybox tickets and policies.

In this chapter

TICKETS

This section describes how to set the properties for Skybox tickets.

Tickets in Skybox represent action items that must be implemented in your organization’s network. After you ascertain the critical issues, you can create tickets and assign them. Tickets can be created automatically using policies (see page 357).

Skybox includes the ticket types listed in the following table.

Ticket type	Used to...
Skybox Vulnerability Control and Skybox Threat Manager	
Vulnerability occurrence (on page 352)	Mitigate specific vulnerability occurrences
Threat alert (on page 353)	(Exposure feature): Describe a mitigation process for all vulnerability occurrences of the Vulnerability Definition (Threat Manager feature): Assess the Vulnerability Definition risk and start an organization-wide remediation process
Skybox Change Manager	
Access Change	Change connectivity (for example, enabling a user to access a specific server)

Ticket properties

All ticket types include an Attributes pane. Possible properties are described in the following table. Not all properties are relevant to all ticket types.

Property	Description
Title	The title of the ticket. In some cases, Skybox creates a title, but you can modify or change it.
Ticket ID	(Read-only) A unique number that identifies the ticket.
Status	The status of the ticket.
Closure Reason	(Read-only) The reason that the ticket was closed; this field is empty until the ticket is closed.

Property	Description
Priority	The priority of the ticket.
Phase (ticket types with phases)	The phase of the ticket.
Phase Due Date (ticket types with phases)	(Read-only) The due date of the current phase. • For information about defining phases, see Defining ticket phases (on page 356).
Due Date	The date by which to implement the solution.
Done Date	(Read-only) For tickets whose solutions are implemented, shows the date on which the status of the ticket was changed to **Closed**, **Resolved**, or **Verified**.
Owner	The user who is responsible for implementing the solution on the organization's network.
CC	Additional users or email addresses of people who are to receive alerts about the ticket.
Network Scope (threat alert tickets only)	The assets and container entities for which to create the ticket.
Vendor Reference (threat alert tickets only)	A specific vendor ID. For example, if the Vulnerability Definition has a Microsoft ID, type the value **MS1<n>-<nnn>**.
External Ticket ID	If there is a parallel ticket in an external ticketing system, this field contains the ID of the ticket in the external system.
External Ticket Status	If there is a parallel ticket in an external ticketing system, this field contains the status of the ticket in the external system.

The Ticket dialog box also contains properties specific to each type of ticket. For information about these properties, see:

- Vulnerability occurrence ticket properties (on page 352)
- Threat alert ticket properties (on page 353)
- Rule recertification ticket properties (on page 355)

Skybox Vulnerability Control and Skybox Threat Manager tickets

The Vulnerability occurrence (on page 352) and Threat alert (on page 353) ticket types are available when working with Skybox Vulnerability Control and Skybox Threat Manager.

Vulnerability occurrence ticket properties

Vulnerability occurrence tickets are action items for mitigating specific vulnerability occurrences.

Naming convention

If you create a ticket for a vulnerability occurrence, the title of the ticket is the title of the Vulnerability Definition with the asset on which it is found. If you create a set of tickets for multiple vulnerability occurrences, you must add a prefix; the title of each ticket is a string consisting of the prefix, the title of the Vulnerability Definition, and the asset on which the vulnerability occurrence is found.

Properties

For information about standard ticket properties, see Ticket properties (on page 351).

The tabs and properties in vulnerability occurrence tickets are described in the following table.

Property	Description
Phases tab	If you use phases for vulnerability occurrence tickets, use this tab to: • View the list of phases for this ticket • Change owners and due dates of phases
Vulnerability Definition tab	(Read-only) Information about the Vulnerability Definition on which this ticket is based.
Solutions tab	Use this tab to select or create solutions for the vulnerability occurrence on which this ticket is based.
Show only selected solutions	Specifies whether to display selected solutions only. This field is useful if there is a long list of known solutions and you want to view only the selected solutions.
Solutions table	The known solutions for the vulnerability occurrence, including those from the Skybox Vulnerability Dictionary and any custom solutions created for your organization. Select solutions that might work for this vulnerability occurrence or click **Add Custom** to add an additional custom solution. (**Add Custom** is not displayed for **Closed** tickets.)
Comments tab	Use this tab to: • Provide additional information about your recommended solution • Add workflow-related comments between the person who assigns the ticket and the ticket owner When a comment is added, Skybox labels it with a user name and timestamp.
Attachments tab	Lists all attachments to the ticket.
History tab	Lists all events for this ticket.

For additional information about creating vulnerability occurrence tickets, see the Creating tickets manually section in the Skybox Vulnerability Control User Guide.

Threat alert ticket properties

Threat alert tickets are action items that can be used for:

- Assessing the risk of a vulnerability occurrence and starting an organization-wide remediation process.
- Describing a mitigation process for all vulnerability occurrences of the selected Vulnerability Definition.

For information about standard ticket properties, see Ticket properties (on page 351).

The tabs and properties in threat alert tickets are described in the following table. Note that not all tabs are relevant to all threat alert tickets.

Property	Description
Phases tab	If you use phases for threat alert tickets, use this tab to: • View the list of phases for the ticket • Change owners and due dates of phases
Threat Alert tab	(Read-only) Information about the threat alert on which the ticket is based.
Related Vulnerability Definitions tab or **Related Security Bulletins tab**	For threat alerts that are in the form of a security bulletin, this tab shows Vulnerability Definitions that are part of the security bulletin. For threat alerts that are a Vulnerability Definition, this tab shows any security bulletins to which the Vulnerability Definition is related.
Vulnerable Assets tab	Lists all assets that are vulnerable to the threat alert.
Vulnerability Occurrences tab	Lists all occurrences of the threat alert, including the asset on which they are found.
Solutions tab	
Show only selected solutions	Specifies whether to display selected solutions only. This field is useful if there is a long list of known solutions and you want to view only the selected solutions.
Solutions	The known solutions for the threat alert, including solutions from the alert service and any custom solutions created for your organization. Select solutions that might work for the threat alert or click **Add Custom** to add an additional custom solution.
Comments tab	Use this tab to: • Provide additional information about your recommended solution • Add workflow-related comments between the person who assigns the ticket and the ticket owner When a comment is added, Skybox labels it with a user name and timestamp.
Products tab	Lists the product or products to associate with the ticket. The products are selected from the Product List.
CVSS tab	(Read-only) The CVSS values for the threat alert.
External URLs tab	Links to websites that might offer additional information about the threat alert.
Deployment tab	Information about the number of assets on which the threat alert is found.

Property	Description
	Note: This tab is displayed when working with ticket phases only.
Total Assets	The total number of assets on which the threat alert is found.
Fixed Assets	The number of assets that are fixed (for example, updated with a service patch or the vulnerable product removed).
% Fixed	(Read-only) The number of fixed assets as a percentage of the total number of assets.
Attachments tab	Lists all attachments to the ticket.
History tab	Lists all events for the ticket.

For information about threat alert tickets:

- If you are working with the Exposure feature of Skybox Vulnerability Control, see the Creating threat alert tickets topic in the Skybox Vulnerability Control User Guide.
- If you are working with Skybox Threat Manager without ticket phases, see the Working with tickets section in the Skybox Threat Manager User Guide.
- If you are working with Skybox Threat Manager using ticket phases, see the Working with tickets and phases section in the Skybox Threat Manager User Guide.

Skybox Change Manager tickets

The Access Change ticket type is available when working with Skybox Change Manager.

Skybox Firewall Assurance, Network Assurance, and Change Manager

The Rule Recertification ticket type is available when working with Skybox Firewall Assurance, Network Assurance, and Change Manager.

Note: You can create tickets for rule recertification in Firewall Assurance and Network Assurance and you can view them in the Tickets workspace. However, they are managed via Skybox Change Manager.

Rule recertification ticket properties

Rule recertification tickets are action items for recertifying access rules. The tickets are created in Firewall Assurance but managed in Change Manager.

Note: The workflows for these tickets are defined in **Tools** > **Options** > **Change Manager Settings** > **Workflows**.

Properties

For information about standard ticket properties, see Ticket properties (on page 351).

The tabs and properties in Rule recertification tickets are described in the following table.

Property	Description
Title	If you are creating a ticket for a single access rule, the default title of the ticket is the name of the firewall and access rule. If you are creating a set of tickets for multiple access rules, the default title of the ticket comprises the number of access rules and number of firewalls (or the firewall name, if all the rules are on the same firewall). You can change the title.
Workflow	The recertification workflow to use for the ticket. The predefined recertification workflow is named *Recertification*.
Description	A description of the rules to be recertified.
Priority	The priority of the ticket.
Owner	The owner of the ticket.

For additional information about rule recertification tickets see the Rule recertification topic in the Skybox Change Manager User Guide.

Defining ticket phases

Skybox includes a ticketing system to manage the workflow for vulnerability occurrence remediation, firewall changes, and so on.

Ticket workflow can be simple—tickets are opened, in progress, and then closed. However, some ticket workflows must support a process that involves several departments or employees—each is responsible for a different aspect. In Skybox, you can define phases that describe the workflow for each (relevant) ticket type. In each phase, the ticket owner is responsible for a specific task.

You can use phases with the following ticket types:

- Threat alert

  We recommend **Assess Risk**, **Develop Solution**, **Deployment**, and **Verification** phases for Threat alert tickets.

- Vulnerability occurrence
- Access Change
- Rule recertification

  For information about the phases of Access Change and rule recertification tickets, refer to the Workflow overview topic in the Skybox Change Manager User Guide.

In Skybox, each phase has an owner, due date, start date and end date, and the phase owners can promote or demote the ticket through the phases, until completion. Each type of ticket can have its own set of phases or you can use the same phase names for all entities.

When a ticket is created, it contains the list of its relevant phases. Initially, the ticket is assigned to the 1st phase and the 1st phase owner. During the life cycle of the ticket, the ticket can progress to the next phase or go back to the previous phase.

Phase permissions

By default, all editable ticket fields can be edited in all phases. However, you can limit the ability to update solutions and deployment information to specific phases.

Note: If you limit the ability to update solutions or deployment to 1 phase, the fields in these areas become read-only for other phases until they are specifically permitted (that is, until you permit them for other phases as well).

To define phases for Threat alert and Vulnerability occurrence tickets

1 Navigate to **Tools** > **Options** > **Server Options** > **Ticket Configuration** > **General**.

2 In the **Ticket Type** field, select the type of ticket for which you want to define phases.

3 For each phase to be added:

a. Click **Add**.

b. In the New Phase dialog box, type a name and (optionally) a comment about the phase.

c. In the Permissions pane, specify the permissions for this phase.

d. Click **OK**.

Note: The phases are stored in the order that you add them; you cannot change the order except by deleting phases and then adding them in the correct order.

As soon as you add a 1st phase, a final phase is added to the list automatically. By default, this phase is named **Verification**. You can rename it, but it cannot be deleted. This phase is the final step in the life cycle of each ticket; tickets that are completed are automatically passed to this phase.

In some organizations, the administrator uses this phase to review the work and validate its completion. If your organization is not interested in using this final check, you can complete the work by moving the ticket to the **Verification** phase.

POLICIES

Policies specify entities that are to be handled automatically.

- **Tickets – Auto Generation** tasks work with policies involving tickets. They check all entities against the relevant policies and create tickets as necessary.

This section describes how to set the properties for Skybox policies.

The policy types included in Skybox are listed in the following table.

Policy type	Used to...
Skybox Vulnerability Control	
Vulnerability occurrences ticket (on page 360)	Trigger creation of vulnerability occurrence tickets (on page 352)
Skybox Vulnerability Control and Skybox Threat Manager	

Policy type	Used to...
Threat alerts ticket (on page 358)	Trigger creation of threat alert tickets (on page 353)
Skybox Firewall Assurance and Skybox Change Manager	
Recertification (on page 361)	Trigger creation of Rule Recertification tickets

Setting policy properties

> Note: A ticket is created for an entity only if the entity matches all properties of the policy in the **General** and **History** tabs.

To change policy properties

1. Select **Tools** > **Administrative Tools** > **Policies**.
2. Select the policy type.
3. In the Skybox Admin window, double-click the policy in the Table pane.
4. Make the necessary changes.

To create a policy

1. Select **Tools** > **Administrative Tools** > **Policies**.
2. Select the type of policy to create:
   - On the toolbar, click Policy ▾ and then select a policy type.
   - In the Admin tree, right-click **Policies** and select **New** > **New <Policy Type> Generation Policy**.

For information about the properties of each policy type, see:

- Threat alerts ticket policies (on page 358)
- Vulnerability occurrences ticket policies (on page 360)
- Recertification (on page 361)

Threat alerts ticket policies

Threat alerts ticket policies are triggers for the creation of threat alert tickets (see page 353).

The properties of threat alerts ticket policies are described in the following table.

Property	Description
General	
Name	A name for the policy.
Properties	
Scope tab	
Vulnerability Definitions	The Vulnerability Definitions (threat alerts) for which to create tickets.
Severity	The severity levels of threat alerts for which to create tickets.

Property	Description
Commonality	The commonality of threat alerts for which to create tickets.
Vulnerability Count Threshold	The minimum number of occurrences of a threat alert in the model for a ticket to be created for the threat alert.
Asset Count Threshold	The minimum number of assets in the model that are vulnerable to a threat alert for a ticket to be created for the threat alert.
Imposed Risk Scale	Specifies how to display risk in tickets and alerts created by this policy.
Reported Date	Only threat alerts created in the specified time frame are ticketed.
Source	The source or sources for which to create threat alert tickets.
CVSS Base Score	The range of CVSS base scores of threat alerts for which to create tickets.
CVSS Temporal Score	The range of CVSS temporal scores of threat alerts for which to create tickets.
Product List Items	The affected products for which to create tickets.
Version	The OS versions for which to create tickets. • T: The value is a text string • .*: The value is a regular expression
Business Attributes	The business attributes for which to create tickets. **Note**: You must have defined business attributes for Vulnerability Definitions to use this field.
Vulnerability Occurrences Filter tab	
Imposed Risk	The minimum exposure and risk value of vulnerability occurrences to include in the tickets.
Network Scope	The network scope for the vulnerability occurrences to include in the tickets.
Operating System	The operating system of the vulnerability occurrences to include in the tickets.
Asset Type	The asset type of the vulnerability occurrences to include in the tickets.
Exploitability	The exploitability level of the vulnerability occurrences to include in the tickets.
Participation in Attacks	
Business Asset Groups	Only include vulnerability occurrences if the specified Business Asset Groups participate in attacks on them.
Regulation Compliance	Only include vulnerability occurrences if the specified regulations and business impact participate in attacks on the vulnerability occurrences.
Threat Origins	Only include vulnerability occurrences if the specified threat origins participate in attacks on the vulnerability occurrences.

Property	Description
Ticket tab	
Owner	A comma-separated list of threat alert owners. Tickets are only created for threat alerts with these owners.
Ticket's Priority By	Specifies how to set the priority of tickets created by this policy. • A specific priority: This priority is assigned to all tickets created by the policy. • **Imposed Risk**, **Severity**, or **Commonality**: The priority of each assigned ticket is set to the value of the selected field of the ticketed threat alert.
Threat Alerts per Ticket	Specifies the number of threat alerts to include in each ticket. The default is 1 per ticket (a separate ticket is created for each threat alert/Vulnerability Definition).

Vulnerability occurrences ticket policies

Vulnerability occurrences ticket policies are triggers for the creation of vulnerability occurrence tickets (see page 352).

The properties of vulnerability occurrences ticket policies are described in the following table.

Property	Description
General	
Name	A name for the policy.
Properties	
Scope tab	
Imposed Risk	The exposure level and minimum risk value of vulnerability occurrences to ticket. Usually, the imposed risk relates to total risk, but you can specify a source. Open the Imposed Risk dialog box (see page 393) to set these values.
Network Scope	The assets and container entities that this policy checks.
Operating System	The operating systems for which to create tickets; tickets are created for vulnerability occurrences on assets with the selected operating systems.
Vulnerability Definitions	The Vulnerability Definitions for which to create tickets. Open the Vulnerability Definition Finder dialog box (see page 387) to specify the Vulnerability Definitions.
Severity	The severity levels of vulnerability occurrences for which to create tickets.
Commonality	The commonality of vulnerability occurrences for which to create tickets.
Imposed Risk Scale	Specifies how to display risk in tickets and alerts created by this policy.

Property	Description
Ticket tab	
Owner	A comma-separated list of vulnerability occurrence owners. Tickets are only created for vulnerability occurrences with these owners.
Ticket's Priority By	Specifies how to set the priority of tickets created by this policy. • A specific priority: This priority is assigned to all tickets created by the policy. • **Imposed Risk**, **Severity**, or **Commonality**: The priority of each assigned ticket is set to the value of the selected field of the ticketed threat alert.

Recertification

The goal of automated recertification is to ensure that access rules in your organization are recertified on a regular basis.

You can automate 2 parts of the recertification process:

- Rule review policies (see page 361) update the next review date of access rules
- Rule recertification ticket policies (see page 362) open recertification tickets for access rules (whose next review dates are coming up)

Rule review policies

A rule review policy is a policy that defines when to update the next review date of access rules. These policies are run by **Rule Recertification** tasks.

The parameters of rule review policies are described in the following table.

Property	Description
General	
Name	A name for the policy.
Properties	
Condition tab	
Firewall Scope	The firewalls and firewall folders whose access rules are checked by this policy.
Violation Severity	Only check access rules whose highest-severity Configuration Policy or Rule Policy violation is one of the selected severity levels.
Rule Usage	Only check access rules with the selected type of usage.
Rule Usage Period	Only check access rules that collected rule usage data for at least this period.
Recertification Status	Only check access rules with the selected recertification statuses.
Rule Owners	A comma-separated list of rule owners. Only check access rules with these rule owners.
Rule Business Function	Only check access rules whose business function matches the specified string.

Property	Description
	Note: Wildcards are supported.
Result tab	
Next Review Date	The relative time after the most recent certification date (of each access rule) to review the rule. **Note**: For new rules that were not yet certified, the relative time after the rule creation date.
Rule Comment	A comment to add to the access rule business attributes (in Skybox) about the change in the next review date. **Note**: “<date>” is the new next review date; “<name>” is the name of the rule review policy.

For additional information, see the Automatic update of next review dates section in the Skybox Firewall Assurance User Guide.

Rule recertification ticket policies

A rule recertification ticket policy is a policy that defines when to open recertification tickets for access rules with approaching review dates. These policies are run by **Tickets – Auto Generation** tasks.

The parameters of rule recertification ticket policies are described in the following table.

Property	Description
General	
Name	A name for the policy.
Properties	
Condition tab	
Firewall Scope	Tickets are opened only for access rules in these firewalls and firewall folders.
Violation Severity	Only check rules whose highest-severity Access Policy or Rule Policy violation is one of the selected severity levels.
Next Review Date	Tickets are opened only for access rules whose next review date is within the specified time frame.
Optimization Status	Only check rules who optimization status is one of the selected optimization statuses.
Rule Owners	A comma-separated list of rule owners. Tickets are opened only for access rules with these rule owners.
Rule Business Function	Tickets are opened only for access rules whose business functions match the specified string. Wildcards are supported.
Custom Business Attributes	Tickets are opened only for access rules whose business attributes match the specified values. Click the **Browse** button to open the Custom Business Attributes dialog box. For information about defining custom business attributes, see the Access Rules topic in the Installation and Administration Guide.

Property	Description
Result- Ticket Creation tab	
Workflow	The workflow of the tickets that are opened.
According to rule owner	The owner of the ticket is the same as the owner of each access rule. If there are multiple owners, a separate ticket is opened for each owner.
Default owner	This field is enabled only if you select **According to rule owner**. The person on whom tickets are opened for rules that have no owner.
Specific	The user on whom all tickets from this policy are to be opened.
Priority	The priority of the tickets opened by this policy.
Advanced	
Maximum number of rules per ticket	The maximum number of rules to include in a ticket. If more than this number of rules match the ticket, multiple tickets are opened.

For additional information, see the Automatic ticket creation for rules needing review section in the Skybox Firewall Assurance User Guide.

Chapter 20

Reports reference

This chapter describes how to use and customize Skybox reports.

Reports in Skybox are detailed accounts of data in the model (for example, high-risk entities, firewall changes, overdue tickets, or top 10 entities).

In this chapter

WORKING WITH REPORTS

You work with report definitions in the Reports tree and workspace.

Skybox includes the report types listed in the following table.

Report type	**Used to present...**
All products	
Tickets (on page 371)	Information about tickets, including status, priority, and assigned owner
Skybox Vulnerability Control	
FISMA/NIST (on page 373)	Information about systems, threat statements, risk assessment, and actions with milestones; used to meet FISMA risk reporting requirements **Note**: FISMA/NIST reports and Risk Assessment reports provide the same information using different terminology. FISMA/NIST reports use terminology that meets the FISMA requirements.
Security Metrics (on page 381)	Security metrics information for a specific scope
Risk Assessment (on page 377)	Information about systems, threat statements, risk assessment, and actions with milestones; used to meet FISMA risk reporting requirements **Note**: Risk Assessment reports and FISMA/NIST reports provide the same information using different terminology. FISMA/NIST reports use terminology that meets the FISMA requirements.

Report type	Used to present...
Risks (on page 379)	Information about entities that have the highest potential risk of being compromised
PCI DSS (on page 375)	Information about vulnerability occurrences found on system components, including Business Asset Groups, networks, and network devices
Vulnerability Management (on page 391)	Information about the vulnerability and risk management process in a format similar to that displayed in Skybox Manager.
Skybox Threat Manager	
Threat Alert Management (on page 382)	Information about Vulnerability Definitions for which threat alerts were issued
Skybox Vulnerability Control and Skybox Threat Manager	
Vulnerabilities (on page 384)	Information about vulnerability occurrences found in the model; you can use these reports to review the vulnerability occurrences in a specific network segment, to filter exposed vulnerability occurrences, to show vulnerability occurrences with a specified severity level, or to show the vulnerability occurrences that impose the highest risk on your organization
Skybox Firewall Assurance	
Access Compliance (on page 395)	Policy-related information about firewalls, to help you to understand the compliance status of your policy as applied to each of the specified firewalls and to identify problematic access configuration in your firewalls
Change Tracking (on page 397)	Information about changes to access rules and firewall objects in firewalls, to help you to understand the changes made in your firewalls during a specified time frame
Firewall Assurance (on page 398)	Overall information about of the state of firewalls in the network, including any combination of: • Compliance for Access and Rule Policy • Configuration Compliance • Optimization & Cleanup • Change Tracking
Firewall Changes (on page 403)	Information about changes to firewalls in the network, by comparing the firewall access rules and objects between 2 different models and presenting the changes
NERC Compliance (on page 404)	NERC Compliance reports present information about the compliance of network devices with the following NERC Critical Infrastructure Protection (CIP) standards of cyber security for the identification and protection of cyber assets: • CIP-002-3 – Critical Cyber Asset Identification • CIP-003-3 – Security Management Controls • CIP-005-3 – Electronic Security Perimeters • CIP-007-3 – Systems Security Management

Report type	Used to present...
PCI Firewall Compliance (on page 405)	Information about compliance of firewalls with PCI DSS Requirement 1: "Install and maintain a firewall configuration to protect cardholder data, a sensitive area within the trusted network of a company"
Rule Usage Analysis (on page 407)	Rule usage information for firewalls to help you to understand the usage patterns of the access rules
Skybox Firewall Assurance and Skybox Network Assurance	
Access Checks (on page 394)	Information about the Access Checks in your Access Policy
Skybox Network Assurance	
Network Access Compliance (on page 408)	Policy-related information about your organization's network, to help you to understand the compliance status of your network to your Access Policy and to identify problematic access configuration in your network
Network Configuration Compliance (on page 409)	Information about the compliance status of your network to your Configuration Policy.

Skybox reports

Skybox reports are generated from *report definitions*. Report definitions are templates for reports that specify:

- The information to include in the report
- How to display the information
- The output format to use for the report
- (Optional) A list of users who are to receive the report by email
- (Optional) Where to save an additional copy of the report (1 copy is always saved)

Skybox includes many predefined report definitions. You can:

- Generate reports from these report definitions without making changes to the definition
- Customize the predefined reports or create other report definitions to suit your requirements

Note: The predefined report definitions are in the **Public Reports** folder. Users without access to this folder can create their own report definitions in the **Private Reports** folder.

You can generate reports automatically (using tasks) and manually.

Generating reports manually

You can generate any report in the Reports workspace. Reports about entities can often be generated by right-clicking the entity in the Tree pane (in other workspaces) and selecting **Reports**.

To generate a report from a report definition

1 In the Reports tree, select the desired report definition.

2 Either right-click the report definition in the tree and select **Generate** or click **Generate** in the workspace.

3 Select the desired generation method (background or foreground) and click **OK**.

It can take time to generate large reports—it is often useful to generate reports in the background and keep working. If the report is generated in the background, you can double-click Currently 1 task is running in the status bar to open the Operational Console and follow the task's progress (using the displayed messages).

A report is generated from the report definition. When generation finishes, the report is displayed in the workspace.

Changing the default report generation method

Report generation can take time, especially for reports with large amounts of information. When you generate reports manually, you can generate the report in the foreground or in the background (as a temporary task). Generating in the foreground is slightly faster, but you cannot do other work in Skybox until the report is generated. If you generate in the background, you can keep working at the same time. Reports generated by tasks are always generated in the background.

To toggle the default report generation method

1 Navigate to **Tools** > **Options** > **Manager Options** > **Reports Configuration**.

2 In the Default Report Generation Method area, select **Generate in the background as a Report Generation task** or **Generate in the foreground**.

3 Click **OK**.

Distributing reports

Reports are listed in the workspace but are only distributed to users if you specify email recipients in the report definition. When a report is generated from the selected report definition, a copy is sent to each specified recipient.

Email recipients are specified in the **Email Recipients** field of the report definition (see Report properties (on page 370)).

Automating reports

You can automate report generation using **Report – Auto Generation** tasks (see Report generation tasks (on page 326)).

Each report type (that is, each report definition) requires a separate task. You might need to have multiple schedules for a report in a task. For example, to generate a report on the 1st and 15th of each month requires 2 schedules.

Note: To send the report to users every time that it is generated, edit the **Email Recipients** field of the report definition when you define the task.

You can schedule report generation on a regular basis or after you update specific types of data (for example, you can schedule a Vulnerability Occurrences (Overview) report after a vulnerability occurrence scan or a New Tickets report after new tickets are created) by including the report generation task in a task sequence after the triggering task.

For information about scheduling tasks and using task sequences, see the Scheduling tasks and task sequences (on page 17) topic in the Skybox Vulnerability Control User Guide, the Skybox Threat Manager User Guide, the Skybox Firewall Assurance User Guide, or the Skybox Network Assurance User Guide.

Creating and editing report definitions

Report definitions define the content and look-and-feel of reports.

You can create a report definition based on an existing definition or from scratch.

To create a report definition

1. In the Reports tree, right-click the parent node of the report definition and select **New** > **Report Definition**.

   Note: **Users** can create report definitions in the **Private Report Definitions** folder. **Admins** can create report definitions in any folder.

2. In the New Report Definition dialog box:

   a. In the **Name** field, type a name for the new report definition and select a **Report Type**.

      The Properties pane of the dialog box changes to display the relevant fields for the selected report type.

   b. Fill in the fields (see Report properties (on page 370)).

   c. Save the report definition:

      – Click **OK** to save the report definition without generating a report.

      – Click **Generate** to save the report definition and generate a report.

To create a report definition based on an existing definition

› Right-click a report definition and select **Create Report Definition Like**.

To edit a report definition

› Right-click the report definition and select **Properties**.

Note: If you change a report definition, we recommend that you also change its name, so that you know what the report is about.

Report formats

You can generate reports in 3 formats:

› PDF (default): The best visual format

› HTML: You can embed the report into a website or intranet site

› RTF: You can edit the report and include it in other reports

The selected format follows the name of the report definition at the top of the pane.

You can change the format of a report using the **Format** field of the report Properties dialog box. For information about report properties, see Report properties (on page 370).

Customizing Skybox reports

You can customize Skybox reports by changing:

- The Skybox logo to your organization logo
- The background image

To change the logo

1. Prepare the logo file: Use a graphic of 738 x 138 pixels, and save it in GIF format with the name **RP_Logo.gif**.
2. Replace the file `<Skybox_Home>\server\conf\report\images\oem1\RP_Logo.gif` with your logo file.

Note: Restart the Skybox Server to apply this change.

To change the background image

1. Prepare the image file: Use a graphic of 654 x 802 pixels, and save it in JPG format with the name **RP_Background.jpg**.
2. Replace the file `<Skybox_Home>\server\conf\report\images\oem1\RP_Background.jpg` with your file.

Note: Restart the Skybox Server to apply this change.

Accessing copies of a generated report

Using the Reports tree, you can view the most recent report generated from each report definition.

You can access any version of a report on the Skybox Manager machine under `<Skybox_Home>\data\[Live | What_If | Forensics]\reports`

Note: All reports are saved as ZIP files; if you distribute an HTML report from the Skybox Server, use the ZIP file (and not individual files from it) and unzip all the files at the destination location to view the complete report afterwards.

Adding a location for saved reports

You can add the user home directory as an additional location for saved reports. This is useful if a user does not have write-access to all locations on the computer or if multiple users are working on the same computer.

Note: Per report definition, you can also save a copy of a report to the Skybox Server machine (by providing the full path for the report in the **Save Copy To** field).

To save reports in the user home directory

1. Navigate to **Tools** > **Options** > **Manager Options** > **Reports Configuration**.
2. Select **Save generated reports in the %HOMEPATH% directory**.
   - If you select this option, reports are also saved at `C:\Users\<user name>\Skybox\[Live | What_If | Forensics]\temp\clientreports`

REPORT PROPERTIES

To open the Report Properties dialog box of a report definition, right-click the report definition in the tree and select **Properties**.

The Report Properties dialog box has 2 tabs:

- **General** tab

  The **General** tab consists of 2 panes:

  - The General pane contains properties common to all Skybox report types.
    - You can specify the **Report Type** for a new report definition only.
    - You can determine the format of the report: PDF, HTML, or RTF.
    - You can specify email recipients.
    - You can specify where on the Server to save a copy of the reports (reports are always saved on Skybox Manager at `<Skybox_Home>\data\Live\reports`).
  - The Properties pane contains properties specific to each type of report. The properties are described in the topics listed in the following table.

    For a new report definition, the Properties pane is empty until you specify the **Report Type** field in the General pane.

- **Comments** tab

  The **Comments** tab contains information about reports generated from this report definition. This information is displayed next to each report in the Table pane of Skybox.

The report types for each Skybox product are listed in the following table.

Skybox product	Report
All products	Tickets (on page 371)
Skybox Vulnerability Control and Threat Manager	FISMA/NIST (on page 373)
	Security Metrics (on page 381)
	Risk Assessment (on page 377)
	Risks (on page 379)
	PCI DSS (on page 375)
	Threat Alert Management (on page 382)
	Vulnerabilities (on page 384)
Skybox Firewall Assurance	Access Checks (on page 394)
	Access Compliance (on page 395)

Skybox product	Report
	Change Tracking (on page 397)
	Firewall Assurance (on page 398)
	Firewall Changes (on page 403)
	NERC Compliance (on page 404)
	PCI Firewall Compliance (on page 405)
	Rule Usage Analysis (on page 407)
Skybox Network Assurance	Access Checks (on page 394)
	Network Access Compliance (on page 408)
	Network Configuration Compliance (on page 409)

TICKETS REPORTS

Tickets reports contain information about tickets, including their status, priority, and assigned owner.

Report sections

The following sections are included in tickets reports:

- **Tickets Status and Priority**: Ticket lifecycle statuses and their priorities. The information is displayed using pie charts.
- **Tickets Status per Owner**: Ticket statuses for each Skybox user to whom tickets are assigned. The information is displayed using a bar chart and a table.
- **Tickets List**: Tickets in the scope of the report. The tickets are grouped by priority, status, owner, or user group. The information is displayed using pie charts and tables.

  Detailed reports include links from each ticket in this section to the detailed information about the ticket in the **Ticket Details** section.

The following section can optionally be included in a tickets report:

- **Tickets Details**: Detailed information about each ticket, including information about the entity for which the ticket was created.

Report properties

The properties that control tickets reports are described in the following table.

Property	Description
Basic tab	
Detail Level	The level of detail about tickets in the report: • **Overview**: Summary information about tickets • **Details**: Summary information about tickets and detailed information about each ticket
Network Scope	The assets and container entities whose tickets are included in the report.

Property	Description
Grouped by	Specifies how to group the tickets in the **Tickets List** section and the **Ticket Details** section.
Ticket Attribute Filter	
Ticket Type	The type of tickets to include in the report.
Ticket Phases	The phases of tickets to include in the report.
Status	The statuses of tickets to include in the report.
Priority	The minimum priority of tickets to include in the report.
Ticker Owner	The ticket owners to include in the report. Tickets owned by other Skybox users are not included in the report.
Creation Date	Only tickets created in the specified time frame are included in the report.
Due Date	Only tickets with dues dates in the specified time frame are included in the report.
Done Tickets Since	Only tickets with end dates in the specified time frame are included in the report.
Modified Since (days)	The number of days (up to the current date) since the ticket was modified. Only tickets with a modification date in the specified time frame are included in the report.
Ticket Generation Policy	The policy that created tickets. Only tickets created by this policy are included in the report. If you do not select a policy, all tickets (created by a policy or created manually) are considered for the report.
Advanced tab	
Products	The products or product groups to include in the report.
Display Sections	
Open Tickets	Specifies whether the **Tickets List** and **Tickets Details** sections include a subsection for open tickets.
Overdue Tickets	Specifies whether the **Tickets List** and **Tickets Details** sections include a subsection for overdue tickets.
Invalid Tickets	Specifies whether the **Tickets List** and **Tickets Details** sections include a subsection for invalid tickets.
Done Tickets	Specifies whether the **Tickets List** and **Tickets Details** sections include a subsection for completed tickets.
Show User Comments	Specifies whether user comments on the tickets appear in the **Tickets Details** section. • **All**: Show all user comments on each ticket • **None**: Hide all user comments on each ticket • **Last**: Show only the most recent user comment on each ticket
Show Vulnerability Occurrences	Specifies whether vulnerability occurrence information is included in the **Ticket Details** section for each vulnerability occurrence ticket or threat alert ticket.

Property	Description
Show Solutions	Specifies whether vulnerability occurrence solutions are included in the **Ticket Details** section for each vulnerability occurrence ticket or threat alert ticket. • **All**: Show all known solutions for each vulnerability occurrence • **Selected**: Show only the selected solutions for each vulnerability occurrence • **Selected. If none**: Show only the selected solutions for each vulnerability occurrence; if no solutions are selected, show all known solutions for each vulnerability occurrence This is useful when you are using the report to see all vulnerability occurrences for each ticket and their solutions.
Max. Number of Services	The maximum number of services to display in the details section for each Access Policy compliance tickets. If an Access Policy compliance ticket includes more than this number of services, Skybox does not include all the services for this Access Policy compliance ticket in the report.

SKYBOX VULNERABILITY CONTROL AND SKYBOX THREAT MANAGER REPORTS

The Vulnerabilities (on page 384) report type is available when working with Skybox Vulnerability Control and Skybox Threat Manager.

The following report types are available when working with Skybox Vulnerability Control:

- FISMA/NIST (on page 373)
- Security Metric (on page 381)
- Risk Assessment (on page 377)
- Risks (on page 379)
- PCI DSS (on page 375)
- Vulnerability Management (on page 391)

The Threat Alert Management (on page 382) report type is available when working with Skybox Threat Manager.

FISMA/NIST reports

FISMA/NIST reports present information about systems, threat statements, risk assessment, and actions with milestones. Use these reports to meet FISMA risk reporting requirements.

Note: FISMA/NIST reports and Risk Assessment reports (see page 377) provide the same information using different terminology. FISMA/NIST reports use terminology that meets the FISMA requirements.

Report sections

The following sections are included in FISMA/NIST reports:

- **Introduction**: The purpose of the report, the staff members involved, and the tools used.

  The introductory text is completely customizable.

- **System Characterization**: An overview of the system and its components, including a list of the information systems, a list of assets for each information system, and a list of network devices.
- **Threat Statements**: The threats to the system and their risk levels.
- **Risk Assessments**: The threat observations for each information system, including risk level, origins, and impacts. In detailed reports, there is a link from each observation to a list of vulnerability occurrences that would enable the observed threat.
- **Summary**: Information about each threat observation (threat, attacker location, destination, and risk) and a list of recommended actions for each observation, in the form of Skybox tickets.

Report properties

The properties that control FISMA/NIST reports are described in the following table.

Property	Description
Basic tab	
Detail Level	The level of detail about risk observations in the report: • **Overview**: Summary information about risk and risk observations • **Details**: Summary information about risk and risk observations, and detailed information about each risk observation and the vulnerability occurrences that caused the risk
Introductory Text	
Report Introductory Text	A free-form field that holds the introductory text for the report.
Report Risk Assessment Text	A free-form field that holds the risk assessment text for the report.
Threat Properties	
Risk Threshold	The minimum risk threshold to use. Open the Risk Threshold dialog box to specify: • A source: Only risk caused by threats from the specified source (Threat Origin Category) is included in the report. • The minimum value to use for the report. **Note**: Only Business Asset Groups that have at least the minimum risk for the selected source are included in the report.
Vulnerability Occurrence Properties	
Vulnerability Occurrence Status	The status of vulnerability occurrences to include in the report; only vulnerability occurrences with a specified status are included in the report. Open the Vulnerability Occurrence Status dialog box (see

Property	Description
	page 389) to specify statuses.
Imposed Risk	Filters vulnerability occurrences according to the threat category to which they are exposed, their exposure level, and their imposed risk value. Open the Imposed Risk dialog box (see page 393) to set these values.
Severity	The severity levels of vulnerability occurrences to include in the report; vulnerability occurrences with other severity levels are not included in the report.
POA&M Properties	
Status	The ticket statuses to include in the report.
Advanced tab	
Max Vulnerability Occurrences	The maximum number of vulnerability occurrences to include in the report for each observation.
Severity Source	(Read-only) The Skybox Vulnerability Dictionary is always used as the source of risk severity for the report.
Severity Score Threshold	The minimum severity score (CVSS) of vulnerability occurrences to include in the report.

PCI DSS reports

PCI DSS reports present information about vulnerability occurrences found on system components, including Business Asset Groups, networks, and network devices. The vulnerability occurrences are listed as action items according to their exposure. Use these reports to meet PCI DSS Requirement 6.1 (6.2 in PCI DSS v3.2); you can use them to meet reporting requirements for other standards.

Report sections

The following sections are included in PCI DSS reports:

- **Introduction**: The purpose of the report.

  The introduction explains how the report provides evidence that the system meets (or does not meet) PCI DSS Requirement 6.1. However, the text is completely customizable and you can change it if you use the report for other purposes.

- **System Components**: The system components that are included in the report scope, include Business Asset Groups, networks (if any), and network devices.
- **Vulnerabilities**: The vulnerability occurrences present on the system components. The vulnerability occurrences are grouped by exposure to the potential attackers. Vulnerability occurrences with an exposure level of direct, indirect, or other are action items that require mitigation. Fixed and blocked vulnerability occurrences, if included, do not require mitigation.

The following sections can optionally be included in a PCI DSS report:

- **Threat Origins**: The Threat Origins that can affect the system components.
- **Asset Lists**: The assets (non-network devices) and the network devices in the scope of the report, showing their compliance with PCI DSS Requirement 6.1. Compliant assets are assets with no direct, indirect, or unknown vulnerability occurrences.

Report properties

The properties that control PCI DSS reports are described in the following table.

Property	Description
Basic tab	
Report Sections	
Network and Asset Group Scope Summary	(Read-only) The **System Components** section is always included in the report.
Vulnerability Occurrences	(Read-only) The **Vulnerabilities** section is always included in the report.
Mitigated Vulnerability Occurrences	Specifies whether to include mitigated vulnerability occurrences as a subsection of the **Vulnerabilities** section.
Threat Origins	Specifies whether to include the **Threat Origins** section in the report. **Note**: This section is not required for PCI DSS Requirement 6.1.
Asset Lists	Specifies whether to include the **Asset Lists** section in the report.
Report Scope	
Business Asset Groups & Units	The Business Units or Business Asset Groups to include in the report.
Card Holder impacts	The Business Impacts and Regulations that, if present on a Business Asset Group, mean that card holder data is stored in this Business Asset Group.
Networks & Locations	The networks and locations to include in the report.
Threat Origins	This field is enabled only if you select **Threat Origins** as a report section. The Threat Origins to include in the report.
Vulnerability Occurrence Severity	The severity levels (or scores) of vulnerability occurrences to include in the report; vulnerability occurrences with other severity levels are not included in the report.
Advanced tab	
Introductory Text	A free-form field that holds the introductory text for the report.
Severity Source	(Read-only) The Skybox Vulnerability Dictionary is always used as the source of risk severity for the report.
Table Limits	

Property	Description
Max Asset Groups in Asset Group Table	The maximum number of Business Asset Groups to display in the list of Business Asset Groups in the **System Components** section.
Max Vulnerability Occurrences per Table	The maximum number of vulnerability occurrences to display in each list of vulnerability occurrences in the **Vulnerability Occurrences** section.
Max assets per table	The maximum number of assets per table in the **Asset Lists** section.
Additional Vulnerability Occurrence Filters	
CVSS Base Score	Only vulnerability occurrences with CVSS base scores in the specified range are included in the report.
CVSS Temporal Score	Only vulnerability occurrences with CVSS temporal scores in the specified range are included in the report.
Vulnerability Occurrence Creation Date	Only vulnerability occurrences created in the specified time frame are included in the report.
Vulnerability Occurrence Modification Date	Only vulnerability occurrences modified in the specified time frame are included in the report.

Risk Assessment reports

Risk Assessment reports present information about systems, threat statements, risk assessment, and actions with milestones. Use these reports to meet FISMA risk reporting requirements.

Note: FISMA/NIST reports (see page 373) and Risk Assessment reports provide the same information using different terminology. FISMA/NIST reports use terminology that meets the FISMA requirements.

Report sections

The following sections are included in Risk Assessment reports:

- **Introduction**: The purpose of the report, the staff members involved, and the tools used

  The introductory text is completely customizable.

- **System Characterization**: An overview of the system and its components, including a list of the Business Asset Groups, a list of assets for each Business Asset Group, and a list of network devices
- **Threat Statements**: The threats to the system and their risk levels
- **Risk Assessments**: The possible attacks for each Business Asset Group, including risk level, origins, and impacts. Detailed reports include a link from each attack to a list of vulnerability occurrences that would enable such an attack
- **Summary**: Information about each attack (threat, attacker location, destination, and risk)

Report properties

The properties that control Risk Assessment reports are described in the following table.

Property	Description
Basic tab	
Detail Level	The level of detail about risks in the report: • **Overview**: Summary information about risks and attacks • **Details**: Summary information about risks and attacks and detailed information about each attack and the vulnerability occurrences that caused the attack
Introductory Text	
Report Introductory Text	A free-form field that holds the introductory text for the report.
Report Risk Assessment Text	A free-form field that holds the risk assessment text for the report.
Threat Properties	
Risk Threshold	The minimum risk threshold to use. Open the Risk Threshold dialog box to specify: • A source: Only risk caused by threats from the specified source (Threat Origin Category) is included in the report. • The minimum value to use for the report. **Note**: Only Business Asset Groups that have at least the minimum risk for the selected source are included in the report.
Vulnerability Occurrence Properties	
Vulnerability Occurrence Status	The status of vulnerability occurrences to include in the report; only vulnerability occurrences with a specified status are included in the report. Open the Vulnerability Occurrence Status dialog box (see page 389) to specify the desired statuses.
Imposed Risk	Filters vulnerability occurrences according to the threat category to which they are exposed, their exposure level, and their imposed risk value. Open the Imposed Risk dialog box (see page 393) to specify the desired exposure levels or imposed risk.
Severity	The severity levels of vulnerability occurrences to include in the report; vulnerability occurrences with other severity levels are not included in the reports.
Ticket Properties	
Status	The ticket statuses to include in the report.
Advanced tab	
Max Vulnerability Occurrence	The maximum number of vulnerability occurrences to include for each attack in the report.
Severity Source	(Read-only) The Skybox Vulnerability Dictionary is always used as the source of risk severity for the report.

Property	Description
Severity Score Threshold	The minimum severity score (CVSS) of vulnerability occurrences to include in the report.
Include section of vulnerability occurrences on Business Asset Groups	Specifies whether to include a section in the report that lists individual vulnerability occurrences on Business Asset Groups.

Risks reports

Risks reports contain information about entities that have the highest potential risk of being compromised.

Usually risks reports highlight the Business Asset Groups with the highest risk and present the risk factors that caused the risk on these Business Asset Groups.

For information about predefined risks reports, see the Risks reports topic in the Skybox Vulnerability Control User Guide.

Report sections

The following sections are included in risks reports:

- **Business Assets Count per Risk Level**: The number of Business Asset Groups per risk level in the selected scope. (A Business Asset Group is a group of assets that serve a common business purpose.)

  The information is displayed using a bar graph and text.

- **Business Assets at Risk – Count over Time**: The number of Business Asset Groups at each risk level for each specified period (quarter or month).

The following sections can optionally be included in a risks report:

- **Business Unit Risks**, **Business Asset Risks**, **Regulation Compliance Risks**, and **Threat Origin Risks** sections: The risk levels of the Business Units, Business Asset Groups, Regulations, or Threat Origins in the selected scope.

  Detailed reports include links from each entity in these sections to the detailed information about the entity in the **Risk Factors** sections.

  Note: In this report, the term *Regulation* refers to Regulations and Business Impacts.

  You can view trend data for Regulations and Threat Origins.

- **Threat Origins by Business Assets**: The Business Asset Groups that can potentially be damaged by each Threat Origin. Each entry presents a different Business Asset Group and the potential risk that could be caused to it by the Threat Origins listed in **Threat Origin Risks** section.
- **Risk Factors**: Detailed information about the entities listed in the corresponding overview sections and an explanation of the factors used in analyzing their risk.

The risk of a Regulation is calculated by aggregating the risk of the associated Business Asset Groups. For each Business Asset Group, only the risk portion calculated by this Regulation is considered.

The risk of a Threat Origin is calculated by aggregating the risks of the possible Business Impacts of attacks starting at that Threat Origin.

Report properties

The properties that control risks reports are described in the following table.

Property	Description
Basic tab	
Detail Level	The level of detail about risks in the report: • **Overview**: Summary information about risk levels for entities • **Details**: Summary information about risk levels and detailed information about each entity including an explanation of the risk factors for the entity
Risk Threshold	The minimum risk value of entities to include in the report. Open the Risk Threshold dialog box to specify: • A source: Only risk caused by threats from the specified source (Threat Origin Category) is included in the report. • The minimum value to use for the report.
Risk Scale	The type of risk scale to use.
Business Units and Asset Groups	
Display 'Business Units'	Specifies whether the report includes sections about Business Units.
Display 'Business Asset Groups'	Specifies whether the report includes sections about Business Asset Groups.
Display Trends for Business Asset Groups	This field is disabled if **Display 'Business Asset Groups'** = **None**. If this field has a value of **Yes**, additional sections with information about Business Asset Group risk trends are included in the report.
Business Unit Scope	This field is disabled if **Display 'Business Asset Groups'** = **None**. The Business Units and Business Asset Groups to include in the report.
Display 'Asset Group Count Over Time'	This field is disabled if **Display 'Business Asset Groups'** = **None**. Specifies whether the report includes the **Business Assets at Risk – Count over Time** section, which displays the risk levels of Business Asset Groups over time.
Display 'Regulation Compliance'	Specifies whether the report includes sections about Regulations (and Business Impacts).

Property	Description
Regulation Compliance Scope	This field is disabled if **Display 'Regulation Compliance'** = **No**. The Regulations and Business Impacts to include in the report. If **Display 'Regulation Compliance'** = **Yes (With Trend)**, an additional section with information about regulation compliance trends is included in the report.
Advanced tab	
Threats	
Display 'Threat Origins'	Specifies whether the report includes sections about Threat Origin risk. If you select **Yes (With Trend)**, an additional section with information about Threat Origin risk trends is included in the report.
Trend	
Trend Frequency	The frequency—quarterly or monthly—of trend samples for the report when trend sections are displayed.
Trend Sample Count	Number of samples to show in the trends.
Trend End Date	The most recent date for which to show trend data in the report. This is useful for history reports.

Security Metric reports

Security Metric reports display security metric information for the specified scope and provide another way to view this information.

For information about analyzing security metrics, see the Analyzing security metrics section in the Skybox Vulnerability Control User Guide.

Report sections

The following sections are included in Security Metric reports:

- **<Selected unit>**: A snapshot of the security metric score for the selected unit. The section includes a breakdown per subunit of the selected unit and a graph of the score over time.

  The subunits in the table are sorted by their contribution to the overall score. If you choose to display 2 levels of security metrics in the report, each subunit in the table is linked to a subsection displaying a snapshot of the security metrics for that subunit.

- **Top-10 Vulnerability Types**: The 10 vulnerability occurrences that contribute the most to the VLI score of the selected unit.

Report properties

The properties that control Security Metric reports are described in the following table.

Property	Description
Basic tab	
Network Scope	The Business Unit or Business Asset Group whose security metrics are included in the report. If you do not select an entity, the report is generated for the whole organization. **Note**: These reports include security metrics for the selected entity and optionally for its child subunit (1 level down). They do not include information for additional levels.
Security Metric Properties	
Security Metric	The security metric type to include in the report.
Exploitability	The exploitability levels of security metrics to include in the report.
Trend Period	The trend frequency to use for security metric trend information (weekly or monthly).
Number of Levels	The number of levels in the business hierarchy to include in the report (1 or 2). • 1: The report includes information about the selected entity only • 2: The report includes information about the selected entity and its child subunits
Advanced tab	
Max. Number of Units	The maximum number of Business Units to include in the report (as children of the selected entity). If **Network Scope** includes more than this number of Business Units, Skybox does not include all the Business Units in the report.

Threat Alert Management reports

Threat Alert Management reports contain information about Vulnerability Definitions for which threat alerts were issued.

Report sections

The following section is included in Threat Alert Management reports:

- **Vulnerability Definitions List**: The Vulnerability Definitions included in the report sorted by status.

The following section can optionally be included in a Threat Alert Management report:

- **Vulnerability Definitions Details**: Detailed information about the Vulnerability Definitions and the known solutions for each, as listed in the Skybox Vulnerability Dictionary. This section is not displayed in overview reports.

Report properties

The properties that control Threat Alert Management reports are described in the following table.

Property	Description
Basic tab	
Detail Level	The level of detail about Vulnerability Definitions in the report: • **Overview**: Summary information about the Vulnerability Definitions • **Details**: Summary information about the Vulnerability Definitions and detailed information about each Vulnerability Definition, including known solutions
ID	The ID numbers of the Vulnerability Definitions (in the alert source) to include in the report.
Title	A string for filtering the titles of Vulnerability Definitions to include in the report. Use the characters **?** and ***** for standard pattern matching.
Status	The statuses of the Vulnerability Definitions to include in the report (Irrelevant, Resolved, In Progress, or Unassigned).
Severity	The severity levels or minimum severity score of the Vulnerability Definitions to include in the report.
CVSS Base Score	The range of CVSS base scores of the Vulnerability Definitions to include in the report.
CVSS Temporal Score	The range of CVSS temporal scores of the Vulnerability Definitions to include in the report.
Creation & Modification	
Reported Date	Only Vulnerability Definitions reported in the specified time frame are included in the report.
Modification Date	Only Vulnerability Definitions modified in the specified time frame are included in the report.
Sort	Specifies how to sort the Vulnerability Definitions in the report.
Advanced tab	
Vulnerability Count Threshold	The minimum number of occurrences on the network that a Vulnerability Definition must have for the Vulnerability Definition to be included in the report.
Asset Count Threshold	The minimum number of occurrences on assets that a Vulnerability Definition must have for the Vulnerability Definition to be included in the report.
Severity Source	(Read-only) The Skybox Vulnerability Dictionary is always used as the source of risk severity for the report.
Max Displayed Solutions	The maximum number of solutions to include in each detailed section.
Custom Vulnerability Definitions	
Created by	The creators of custom Vulnerability Definitions to include in the report.
Custom	Specifies whether to include only custom Vulnerability

Property	Description
Vulnerabilities only	Definitions in the report.

Vulnerabilities reports

Vulnerabilities reports contain information about vulnerability occurrences found in the model.

Use these reports to review the vulnerability occurrences in a specific network segment or location, to filter exposed vulnerability occurrences, to show vulnerability occurrences with a specified severity level, or to show vulnerability occurrences that impose the highest risk on your organization.

- For additional information about Vulnerabilities reports, see the Limiting the scope of vulnerabilities reports topic in the Skybox Vulnerability Control User Guide.
- For information about predefined Vulnerabilities reports, see the Predefined vulnerabilities report definitions topic in the Skybox Vulnerability Control User Guide.

Report sections

The following sections can optionally be included in a vulnerabilities report:

- **Vulnerabilities – Severity, Risk and Exposure**: The vulnerability occurrences included in the report grouped by severity, risk, and exposure level. The information is displayed using pie charts and tables.
- **Vulnerability Count over Time**: Trends in the vulnerability occurrence count. The graph refers to all vulnerability occurrences in the network scope of the report, regardless of Vulnerability Occurrence Attribute filters defined in the report.
- **Vulnerabilities – By Operating System** / **By Location** / **By Business Unit** / **By Business Asset Group** / **By Type**: The vulnerability occurrences included in the report grouped by the selected entity. The information in each section is displayed as a bar chart of the top 5 entities with the most vulnerability occurrences, followed by a table.
- **Vulnerabilities per Host Grouped by Host**: Detailed information about the vulnerability occurrences on each asset. The section is not displayed in overview reports. For reports that include solutions, each vulnerability occurrence is linked to a list of known solutions (in the **Vulnerabilities and Solutions** section).
- **Vulnerabilities and Solutions**: Known solutions for each Vulnerability Definition in the report, as listed in the Skybox Vulnerability Dictionary, and the assets on which the Vulnerability Definition is found. Each asset is linked to a vulnerability occurrence in the **Vulnerabilities per Host Grouped by Host** section, so that you can view information about the vulnerability occurrence on that asset.

  This section is included if **Detail Level** = **Details & Solutions**.

Report properties

The properties that control vulnerabilities reports are described in the following table.

Property	Description
Basic tab	
Detail Level	The level of detail about vulnerability occurrences in the report: • **Overview**: Summary information about the vulnerability occurrences • **Details**: Summary information about the vulnerability occurrences and detailed information about each vulnerability occurrence • **Details & Solutions**: Summary information about the vulnerability occurrences, and detailed information and known solutions for each vulnerability occurrence **Important**: Overview information is provided for all vulnerability occurrences that meet the report criteria. Detailed information and solutions are only provided for the first 50 vulnerability occurrences; for **Details** or **Details & Solutions** reports, we recommend that you narrow the criteria so that the report includes fewer than 50 vulnerability occurrences.
Network Scope	The assets and container entities whose vulnerability occurrences are included in the report.
Operating System	The operating systems to include in the report.
Asset Type	The asset types to include in the report.
Assets Grouped by	Specifies how to group the assets in the **Vulnerability Occurrences per Asset** section. If you select **None**, the assets are listed alphanumerically (and not grouped). **Note**: The **Vulnerability Occurrences per Asset** section is only included if **Detail Level** = **Details** or **Detail Level** = **Details & Solutions**.
Vulnerability Occurrence Attribute Filter	
Vulnerability Definitions	The Vulnerability Definitions to include in the reports. Open the Vulnerability Definition Finder dialog box (see page 387) to specify Vulnerability Definitions.
Vulnerability Occurrence Status	The vulnerability occurrence statuses to include in the report. Open the Vulnerability Occurrence Status dialog box (see page 389) to select basic and advanced statuses.
Status Change Date	Only vulnerability occurrences whose status changed in the specified time frame are included in the report. Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time
Imposed Risk	The source (Threat Origin Category), exposure level, and minimum risk value to use in the report. Open the Imposed Risk dialog box (see page 393) to set these values.
Severity Source	The source against which to check the severity of the Vulnerability Definitions.

Property	Description
Severity Level	The severity levels of vulnerability occurrences to include in the report.
Severity Score Threshold	The minimum severity score (CVSS) of vulnerability occurrences to include in the report.
Scan Time	
Filtering Mode	Specifies the vulnerability occurrences to include: • **Not Scanned in**: Vulnerability occurrences that were not scanned in the time frame specified by **Scan Time** • **Scan Time**: Vulnerability occurrences that were most recently scanned in the time frame specified by **Scan Time**
Scan Time	A time frame used by **Filtering Mode**. Select **Custom** to define a date range by: • Specifying starting and ending dates for the scan • Specifying starting and ending times relative to the current time
Created Since	Only vulnerability occurrences created in the specified time frame are included in the report. Select **Custom** to define a date range by: • Specifying starting and ending dates for the scan • Specifying starting and ending times relative to the current time
Advanced tab	
Risk Scale	The risk scale to use for displaying risk values.
Commonality	The commonality values of vulnerability occurrences to include in the report.
Solution Types	The solution types of vulnerability occurrences to include in the report.
Display Sections	
Max Displayed Solutions	• The maximum number of solutions to include in each detailed section (if **Detail Level** = **Details and Solutions**).
Vulnerability Occurrences – By Operating System	Specifies whether to include the **Vulnerabilities – By Operating System** section in the report: • **No**: Do not include this section. • **Yes (By Family)**: Include this section and group the vulnerability occurrences by operating system families. • **Yes (By Product)**: Include this section and group the vulnerability occurrences by products (specific operating system).
Vulnerability Occurrences – By Location	Specifies whether to include the **Vulnerabilities – By Location** section in the report.
Vulnerability Occurrences – By Business Units	Specifies whether to include the **Vulnerabilities – By Business Unit** section in the report.
Vulnerability Occurrences – By	Specifies whether to include the **Vulnerabilities – By Business Asser** section in the report.

Property	Description
Business Asset Groups	
Vulnerability Occurrences – By Vulnerability	Specifies whether to include the **Vulnerabilities – By Type** section in the report.
Vulnerability Occurrences Grouped by	Specifies how to show the breakdown of vulnerability occurrences in the report sections: • **Severity**: Show the breakdown of the vulnerability occurrences in each section by severity. • **Risk**: Show the breakdown of the vulnerability occurrences in each section by risk level.
Vulnerability Occurrences Detailed Format	Specifies how to list the vulnerability occurrences in the **Vulnerabilities per Host Grouped by Host** section. • **No**: List all vulnerability occurrences for an asset together in a table containing the main information about each vulnerability occurrence). • **Yes**: List each vulnerability occurrence for an asset separately with its details.
Trend	
Display Trend	Specifies whether to include trend information in the report. **Note**: The only trend available is **Vulnerability Count over Time**.
Trend Frequency	This field is enabled only if **Display Trend** = **Yes**. The frequency of trends included in the reports.
Trend Sample Count	This field is enabled only if **Display Trend** = **Yes**. The number of samples included in the trend graphs.

Vulnerability Definition Finder dialog box

Use the Vulnerability Definition Finder dialog box to specify the Vulnerability Definitions to fill the **Vulnerability Definitions** field of a Properties dialog box for:

- vulnerability occurrences analyses
- vulnerability occurrences ticket policies
- Vulnerabilities reports
- Vulnerability occurrences

The properties of the Vulnerability Definition Finder dialog box are described in the following table (these are also the properties of Vulnerability Definition analyses).

Property	Description
Basic tab	
Severity Source	The source against which to check the severity of the Vulnerability Definitions.
Severity	The severity levels of the Vulnerability Definitions or the minimum severity score (0-10).

Property	Description
Exploitability	The exploitability levels of the Vulnerability Definitions.
Title	A string for filtering the Vulnerability Definition titles. Use the characters **?** and ***** for standard pattern matching.
Sort	Specifies how to sort the Vulnerability Definitions that are returned after doing a search.
Advanced tab	
ID	A Vulnerability Definition ID. The prefix cannot be changed.
External Catalog	The external vulnerability database in which the Vulnerability Definitions have an ID.
External Catalog ID	The ID number of the Vulnerability Definitions in the selected external vulnerability database.
CVSS Base Score	The range of CVSS base scores of the Vulnerability Definitions.
CVSS Temporal Score	The range of CVSS temporal scores of the Vulnerability Definitions.
Vulnerability Count Threshold	The minimum number of occurrences of a Vulnerability Definition in the network for the Vulnerability Definition to be returned.
Asset Count Threshold	The minimum number of assets with an occurrence of a Vulnerability Definition for the Vulnerability Definition to be returned.
Product search string	Only Vulnerability Definitions that affect products whose title includes the specified string are returned.
Creation & Modification	
Reported Date	Only Vulnerability Definitions reported in the specified time frame are returned. Select **Custom** to define a date range by: • Specifying the earliest report date for Vulnerability Definitions • Specifying the earliest report time relative to the current time for Vulnerability Definitions
Modification Date	Only Vulnerability Definitions modified in the specified time frame are returned. Select **Custom** to define a date range by: • Specifying the earliest modification date • Specifying the earliest modification time relative to the current time
Last Modified by System	Only Vulnerability Definitions modified by the system in the specified time frame are returned. Select **Custom** to define a date range by: • Specifying the earliest modification date • Specifying the earliest modification time relative to the current time

Property	Description
Last Modified by User	Only Vulnerability Definitions modified by a user in the specified time frame are returned. Select **Custom** to define a date range by: • Specifying the earliest modification date • Specifying the earliest modification time relative to the current time

To select Vulnerability Definitions

1 Determine the values to use for the search and enter the values in the dialog box.

If you do not enter a value for a property, that property is not used in the search.

2 Click **Search**.

All Vulnerability Definitions that match the specified properties are listed in the **Search Results** field and the number of matching Vulnerability Definitions is displayed above the field.

3 Select required Vulnerability Definitions from the list in the **Search Results** field and click ︾ to copy them to the **Selected Vulnerability Definitions** field.

4 Make additional searches by refining the search or using different criteria. Add the desired results from each search to the **Selected Vulnerabilities** field.

5 Click **OK**.

The Vulnerability Definitions listed in the **Selected Vulnerabilities** field are returned to the **Vulnerability Definitions** property of the calling dialog box.

Vulnerability Occurrence statuses

Use the Vulnerability Occurrence Status dialog box to specify the vulnerability occurrence statuses for the **Status** field of a Properties dialog box of, for example, a vulnerability occurrences analysis, a vulnerability occurrences ticket policy, or a Vulnerabilities report.

There are 2 levels of vulnerability occurrence status:

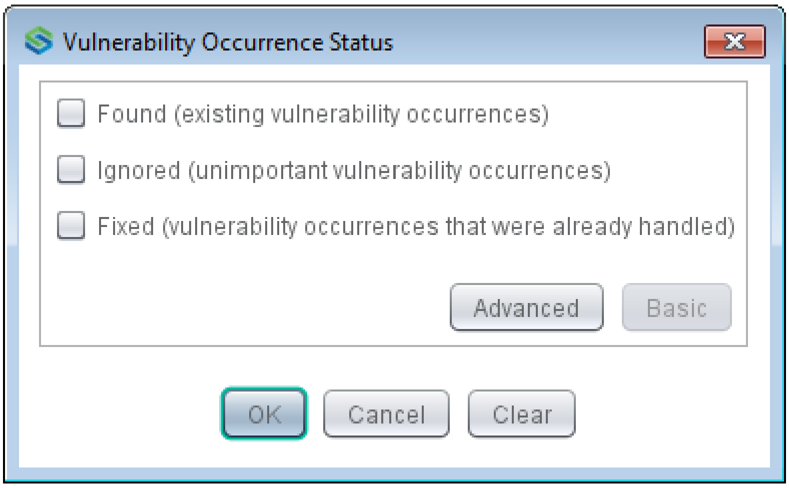
- **Basic** statuses (found, ignored, and fixed) are displayed in Skybox Manager.
- **Advanced** statuses are specific instances of the basic statuses that are stored internally but not usually displayed. For example, the basic status of **Found** is divided into 3 advanced statuses:
  - The vulnerability occurrence was rediscovered after it was considered fixed.
  - The vulnerability occurrence was found by a scanner.
  - The vulnerability occurrence was added by a user.

You can select any combination of basic and advanced statuses.

To select the vulnerability occurrence statuses to fill the Status field

1 Click the **Browse** button of a (vulnerability occurrence) **Status** field:

- If the **Status** field is empty, a Vulnerability Occurrence Status dialog box appears.



Vulnerability Occurrence Status

□ Found (existing vulnerability occurrences)

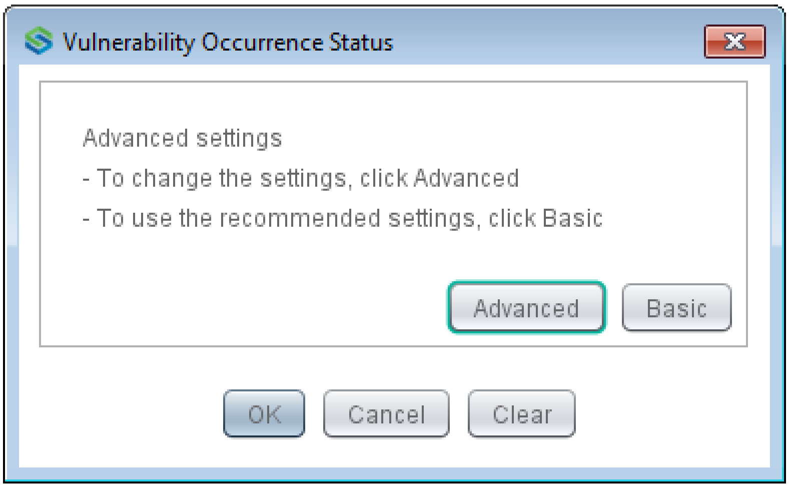
□ Ignored (unimportant vulnerability occurrences)

□ Fixed (vulnerability occurrences that were already handled)

As required:

  - Select a basic status and click **OK**. Ignore the remaining instructions in this section.
  - Select a basic status and then click **Advanced** to fine-tune your selection; the relevant advanced statuses are selected.
  - Click **Advanced** to select specific advanced statuses.

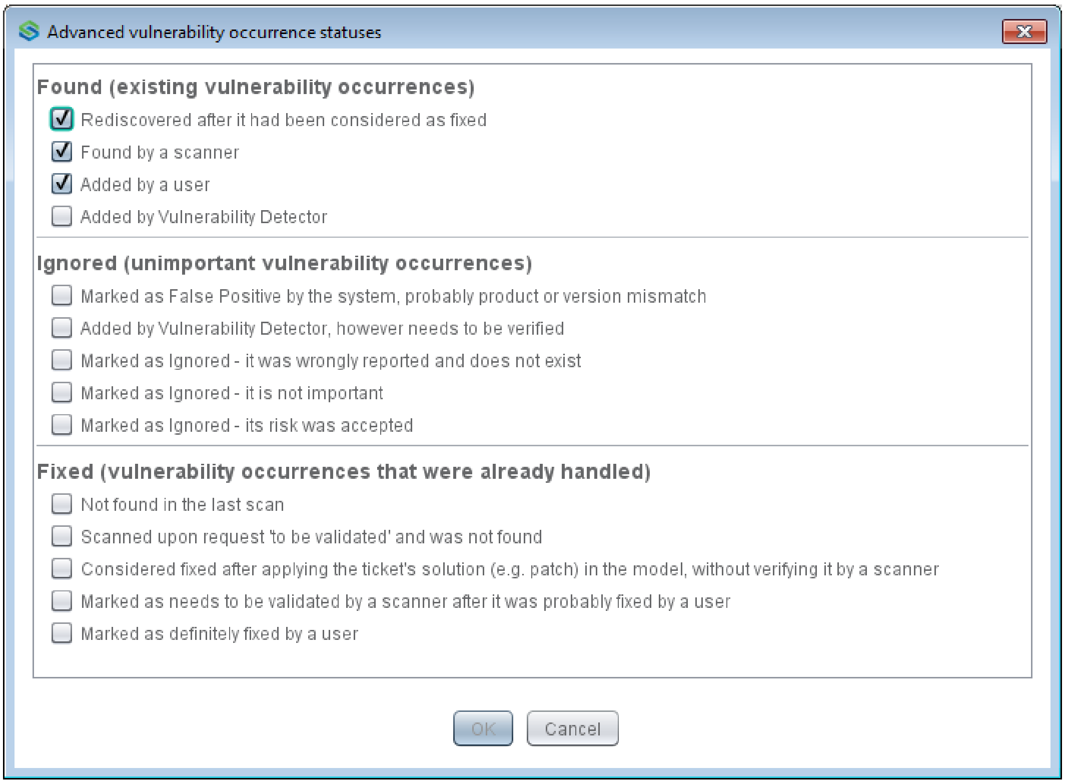
- If the **Status** field contains a value or if you changed any field in the **Advanced** settings, a different Vulnerability Occurrence Status dialog box appears.



Vulnerability Occurrence Status

Advanced settings
- To change the settings, click Advanced
- To use the recommended settings, click Basic

- To select advanced statuses, click **Advanced**.



Found (existing vulnerability occurrences)

☑ Rediscovered after it had been considered as fixed

☑ Found by a scanner

☑ Added by a user

□ Added by Vulnerability Detector

Ignored (unimportant vulnerability occurrences)

□ Marked as False Positive by the system, probably product or version mismatch

□ Added by Vulnerability Detector, however needs to be verified

□ Marked as Ignored - it was wrongly reported and does not exist

□ Marked as Ignored - it is not important

□ Marked as Ignored - its risk was accepted

Fixed (vulnerability occurrences that were already handled)

□ Not found in the last scan

□ Scanned upon request 'to be validated' and was not found

□ Considered fixed after applying the ticket's solution (e.g. patch) in the model, without verifying it by a scanner

□ Marked as needs to be validated by a scanner after it was probably fixed by a user

□ Marked as definitely fixed by a user

2 Select or clear statuses and click **OK**.

3 In the Vulnerability Occurrence Status dialog box, click **OK** to accept the advanced statuses that you selected.

Vulnerability Management reports

Vulnerability Management reports provide an overview of the vulnerability and risk management process in a format similar to the overview in the Vulnerability Control workspace. These reports can contain information about:

- Discovery: The age and status of vulnerability occurrences and assets (including an indication of overdue assets)
- Analytics: Security metrics that need remediation and exposed vulnerability occurrences

Report sections

The following section is included in Vulnerability Management reports:

- **Summary**: The information provided in the main Discovery Center and Analytics Center pages.

You specify the additional information to include in the report.

Report properties

The properties that control Vulnerability Management reports are described in the following table.

Property	Description
Basic tab	
Vulnerability Management Features	

Property	Description
Discovery Summary	Specifies whether the report includes information from the Discovery Center dashboard.
Prioritization Summary	Specifies whether the report includes information from the Prioritization Center dashboard.
Security Metric Details	This field is enabled only if you select **Prioritization Summary**. Specifies whether the report includes details about security metrics.
Select Security Metrics	This field is enabled only if you select **Security Metric Details**. The security metrics to include in the report.
Exploitability	The exploitability levels of security metrics to include in the report.
Change Period	This field is enabled only if you select **Security Metric Details**. Only changes made in the specified time frame are included in the report. Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time
Exposure by Threat Summary	Specifies whether the report includes exposure information from the Prioritization Center dashboard.
Advanced tab	
Report Introductory Text	A free-form field that holds the introductory text for the report.
Max. Number of New Vulnerability Occurrences	The maximum number of new Vulnerability Occurrences to include in the list of new Vulnerability Occurrences. If there are a greater number of new Vulnerability Occurrences, they are not included in the report.
Max. Number of Business Asset Groups	The maximum number of Business Asset Groups to include in the Exposure Analysis section.
Max. Number of Threat Origins	The maximum number of Threat Origins to include in the Exposure Analysis section.
Max. Number of Regulation Types	The maximum number of regulation types to include in the Exposure Analysis section.
Max. Number of Units	The maximum number of Business Units to include in the list of Business Units.
Max. Number of Vulnerability Definitions by Contribution to Security Metric	The maximum number of Vulnerability Definitions or security bulletins per security metric to include in the Key Performance Indicators section.

Imposed risk properties

Use the Imposed Risk dialog box to define the source, exposure levels, and risk value properties of vulnerability occurrences.

The properties of the Imposed Risk dialog box are described in the following table.

Property	**Description**
Source	The Threat Origin Category that imposes the risk. Skybox does not use risk from other Threat Origins Categories for this analysis.
Exposure Levels	You can select multiple exposure levels: • **Direct**: Vulnerability occurrences that the Threat Origin can exploit in 1 step. • **Indirect**: Vulnerability occurrences that the Threat Origin can exploit, but only in more than 1 step. • **Protected**: Vulnerability occurrences that cannot be accessed by an attacker because they are protected by an IPS device. • **Potential**: Vulnerability occurrences that have an accessible service but might not be accessible because of other exploit conditions that cannot be guaranteed (for example, authentication might be required). • **Inaccessible**: A vulnerability occurrence that cannot be accessed by an attacker (for example, the vulnerable service is disabled, or the vulnerability occurrence is blocked by a firewall). • **Excluded**: Vulnerability occurrences excluded from attack simulation. (Attack simulation excludes vulnerability occurrences with the statuses **False Positive**, **Fixed**, or **Ignored**.) • **Unknown**: Vulnerability occurrences with unknown exposure. The exploit conditions of these vulnerability occurrences are irrelevant for attack simulation (for example, a browser weakness that might cause damage to a workstation if its user surfs to a hostile website). • **User interaction**: Vulnerability occurrences that require user interaction via email or XSS. Exposure for these vulnerability occurrences is unknown.
Value	The minimum imposed risk of the vulnerability occurrences. Skybox only uses vulnerability occurrences whose risk value is at least the specified value. • **Any**: Risk value is not used to select vulnerability occurrences • **Monetary** • **Level** • **Score (0-100)** If **Monetary** is specified, type a number representing the monetary value in the default currency. If **Level** or **Score** is specified, select a value.

SKYBOX FIREWALL ASSURANCE REPORTS

The following report types are available when working with Skybox Firewall Assurance:

Note: Firewall Assurance reports can provide any combination of change tracking, Access Compliance, Rule Compliance, Configuration Compliance, and rule usage analysis information in a report. Most of this information is also available in separate reports.

Access Checks reports

Access Checks reports provide information about the Access Checks in your Access Policy.

Report sections

The following section is included in all Access Checks reports:

- **Access Checks – Overview**: The Access Checks by policy section. The information is displayed using tables.

  Detailed reports include links from each Access Check in this section to detailed information about the Access Check in the next section.

The following sections can optionally be included in an Access Checks report:

- **Access Checks – Details**: Detailed information about each Access Check, using the same order used in the previous section.

Report properties

The properties that control Access Checks reports are described in the following table.

Property	Description
Basic tab	
Detail Level	The level of detail about Access Checks in the report: • **Overview**: Summary information about the Access Policy, including a list of the Access Checks in each policy section • **Details**: Summary information about the Access Policy and detailed information about each Access Check
Access Policy Scope	The parts of the Access Policy (policy folders, policy sections, or Access Checks) to include in the report.
Severity Threshold	The minimum severity of Access Checks to include in the report.
Sort by	Specifies how to sort the policy sections in the report.

Property	Description
Advanced tab	
Max. Number of Services	This field is enabled only if **Detail Level** = **Details**. The maximum number of destination services to include in the report for each Access Check in the **Details** section. If an Access Check includes more than this number of destination services, Skybox does not include all the destination services for this Access Check in the report.
Length of Rule Description	The maximum length of the description of each Access Check to include in the **Details** section.

Access Compliance reports

Access Compliance reports provide policy-related information about selected firewalls and help you to understand the compliance status of your policy as applied to each firewall and to identify problematic access configuration in these firewalls.

For additional information about the content of Access Compliance reports, see the Access Compliance reports topic in the Skybox Firewall Assurance User Guide.

Report sections

The following sections are included in all Access Compliance reports:

- **Summary**: The number of firewalls in the report scope, a pie chart displaying a breakdown of access tests and violations for the firewalls in the scope, and a list of links to firewalls in the report, with the firewall name, IP address, and compliance percentage.
- Sections for each firewall separately: These sections are described in the following table.

Report properties

The properties that control Access Compliance reports are described in the following table.

Property	Description
Basic tab	
Firewall Scope	The firewalls and firewall folders to include in the report.
Group by Policy Sections	Specifies whether to group the information about each firewall by policy sections.
Report Sections	The sections to display for each firewall in the report
Overview	(Read-only) Access Compliance reports always include a section named **<firewall name>** for each firewall. The section includes the firewall name and IP address, and a table of each policy sections with its compliance rate for this firewall.
Filter by Severity	Specifies whether to include only violations of specific severities in the report.

Property	Description
Display Violations	Specifies whether to include a section containing information about violations for each firewall. The names of the sections and their content depend on the value selected for this field: - **New Violations**: The sections are named **Violations for <firewall name>** and contain only new violations (according to the definition in **Options** > **Server Options** > **Entity Settings**). - **Violations Only**: The sections are named **Violations for <firewall name>** and contain only violations. - **All Tests**: The sections are named **Access Tests for <firewall name>** and list all access tests (compliant tests and violations) for each firewall.
Violating Access Rules	Specifies whether to include a section named **Violating Access Rules for <firewall name>** for each firewall. This section contains a table listing the violating access rules for the firewall. The table is followed by detailed information about each violating access rule, including a list of Access Checks violated by the access rule.
Exceptions	Specifies whether to include a section named **Exceptions for <firewall name>** for each firewall. This section lists the exceptions for the firewall.
Access Rules	Specifies whether to include a section named **Access Rules for <firewall name>** for each firewall. This section lists the access rules (grouped by rule chain) for each firewall in the report.
Advanced tab	
Introductory Text	A free-form field that holds the introductory text for the report.
Access Policy Scope	The parts of the Access Policy (policy folders, policy sections, or Access Checks) to include in the report.
Split if scope greater than	For detailed reports, specifies the maximum number of firewalls to present in 1 report. If there are more firewalls than this in a detailed report, all the summaries are presented together in the report, but all the detailed information for each firewall is saved as a smaller, linked report.
Include only Non-compliant Firewalls	Specifies whether to include all firewalls in the scope that match the firewall filters or only firewalls that have compliance metrics and do not meet the Compliance Threshold.
Compliance Threshold (%)	This field is enabled only if you select **Include only Non-compliant Firewalls**. Only firewalls whose compliance level is equal to or less than this threshold are included in the report.
Firewall Filters	
Firewall Type	The firewall types to include in the report.
Operating System	The operating systems to include in the report.
Exception Filters: These fields are enabled only if you select **Exceptions** in	

Property	Description
the **Basic** tab.	
Created Since	Only exceptions created in the specified time frame are included in the report. Select **Custom** to define a date range by: • Specifying the earliest creation date for exceptions in the report • Specifying the earliest creation time relative to the current time for exceptions in the report
Expiration Date	Only exceptions that expire in the specified time frame are included in the report. Select **Custom** to define a date range by: • Specifying the earliest expiration date for exceptions in the report • Specifying the earliest expiration time relative to the current time for exceptions in the report

Change Tracking reports

Change Tracking reports provide information about changes to access rules and firewall objects in specified firewalls and help you to understand the changes made in your firewalls during a specified time frame.

For information about the content of Change Tracking reports, see the Change Tracking reports topic in the Skybox Firewall Assurance User Guide.

Report sections

The following sections are included in Change Tracking reports:

- **Summary**: A list of changed firewalls followed by a list of all the changes included in the report.
- For each firewall in the report:
  - **<firewall name>**: The number of changed access rules and objects found for this firewall.
  - **Changed Access Rules**: The changed access rules for the firewall with the main properties of each access rule.

    Detailed reports include links from each access rule in this section to detailed information in the **Changed Access Rules – Details** section.
  - **Changed Objects**: The changed firewall objects for the firewalls with the main properties of each firewall object.

    Detailed reports include links from each object in this section to detailed information in the **Changed Objects – Details** section.

The following sections can optionally be included in a Change Tracking report:

- For each firewall in the report:
  - **Changed Access Rules – Details**: Information about each changed access rule (including deleted rules).
  - **Changed Objects – Details**: Information about each changed firewall object (including deleted objects).

Report properties

The properties that control Change Tracking reports are described in the following table.

Property	Description
Basic tab	
Tracking Period	Only changes made in the specified time frame are included in the report. Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time
Firewalls Scope	
Firewall Scope	The firewalls and firewall folders to include in the report.
Firewall Type	The firewall types to include in the report.
Report Sections	
All Changes	(Read-only) The report always includes a section that lists all the changes in the scope of the report.
Changes By FW	Lists all the changes for each firewall, with a separate section in the report for each firewall.
Details	Lists detailed information about each change for each firewall, with a separate section in the report for each firewall.

Firewall Assurance reports

Firewall Assurance reports provide a complete overview of the state of firewalls in the network and can include detailed information. You can generate the report for any combination of:

- Compliance for Access and Rule Policy
- Configuration Compliance
- Optimization & Cleanup
- Change Tracking
- Vulnerability Occurrences

Report sections

The following sections are included in Firewall Assurance reports:

- Introduction
- **Folder Summary**: Summary information similar to that found on the folder summary page.
- **Compliance Summary**: Summary information about each feature in the report scope.

The following sections can optionally be included in a Firewall Assurance report:

- For each firewall in the report

- **Summary: <firewall name>**: Basic information about this firewall, and overview information about each feature in the report scope, similar to that displayed on the firewall summary page.

› If any detailed information is requested, a separate section for each firewall in the report (named **Details: <firewall name>**) includes the relevant detailed information divided by features.

Report properties

The properties that control Firewall Assurance reports are described in the following table.

Property	Description
Basic tab	
Firewall Scope	The firewalls and firewall folders to include in the report. **Note**: If the report is generated for a firewall folder, there is a folder summary section at the beginning of the report.
Report Level	The detail level of the report: • **Overview**: High-level report that summarizes compliance by feature for all firewalls. If the scope is a folder, the folder summary is included. • **Firewall Summary**: Overview information and summary information for each firewall per compliance feature. • **Details**: Firewall summary information and detailed information for each firewall per compliance feature.
Compliance Features	
Access Compliance	Specifies whether to include information about Access Compliance.
Access Policy Scope	This field is displayed only if **Report Level** = **Details**. The parts of the Access Policy (policy folders, policy sections, or Access Checks) to include in the report.
Display Violations	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a section containing information about Access Policy violations for each firewall. The name of the section and its content depend on the value selected for this field: • **New Violations**: The sections are named **Violations for <firewall name>** and contain only new violations (according to the definition in **Tools** > **Options** > **Server Options** > **Entity Settings**). • **Violations Only**: The sections are named **Violations for <firewall name>** and contain only violations. • **All Tests**: The sections are named **Access Tests for <firewall name>** and list all access tests (compliant tests and violations) for each firewall.
Filter Violations by Severity	This field is displayed only if **Report Level** = **Details**. Specifies whether to include only violations of specific severities in the report.
Violating Access Rules	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a section named **Violating**

Property	Description
	Access Rules for <firewall name> for each firewall. This section contains a table listing the violating access rules for the firewall Access Policy. The table is followed by detailed information about each violating access rule, including a list of Access Checks that are violated by the access rule.
Exceptions	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a section named **Exceptions for <firewall name>** for each firewall. This section lists the exceptions for the firewall.
Rule Compliance	Specifies whether to include information about Rule Compliance.
Rule Policy Scope	This field is displayed only if **Report Level** = **Details**. The parts of the Rule Policy (policy folders or Rule Checks) to include in the report.
Display Rule Checks	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a section containing information about Rule Policy violations for each firewall. The name of the section and its content depend on the value selected for this field: • **Violations Only**: The sections are named **Violating Rule Checks for <firewall name>** and contain only violations. • **All Tests**: The sections are named **Rule Checks for <firewall name>** and list all rule checks (compliant checks and violations) for each firewall. • **New Violations**: The sections are named **Violating Rule Checks for <firewall name>** and contain only new violations (according to the definition in **Tools** > **Options** > **Server Options** > **Entity Settings**).
Violating Access Rules	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a section named **Violating Access Rules for <firewall name>** for each firewall. This section contains a table listing the violating access rules for the firewall Rule Policy. The table is followed by detailed information about each violating access rule, including a list of Rule Checks that are violated by the access rule.
Filter Violations by Severity	This field is displayed only if **Report Level** = **Details**. Specifies whether to include only violations of specific severities in the report.
Exceptions	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a section named **Exceptions for <firewall name>** for each firewall. This section lists the Rule exceptions for the firewall.
Configuration Compliance	Specifies whether to include information about Configuration Compliance.
Configuration Policy Scope	This field is displayed only if **Report Level** = **Details**. The parts of the Configuration Policies (policy folders, policies, or Configuration Checks) to include in the report.

Property	**Description**
Display Violations	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a section containing information about Configuration Policy violations for each firewall. The name of the section and its content depend on the value selected for this field: • **Violations Only**: The sections are named **Violations for <firewall name>** and contain only violations. • **All Tests**: The sections are named **Access Tests for <firewall name>** and list all access tests (compliant tests and violations) for each firewall. • **New Violations**: The sections are named **Violations for <firewall name>** and contain only new violations (according to the definition in **Tools** > **Options** > **Server Options** > **Entity Settings**).
Filter Violations by Severity	This field is displayed only if **Report Level** = **Details**. Specifies whether to include only violations of specific severities in the report.
Display Configuration Checks	This field is displayed only if **Report Level** = **Details**. Specifies whether to include Configuration Check information for violations that are included in the report.
Optimization & Cleanup	Specifies whether to include information about: • Rule usage • Shadowed and redundant rules
Rule Usage Analysis Period	The time frame to use for rule usage analysis information in the report. Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time
Rule Created Since	This field is displayed only if **Report Level** = **Details**. This field does not affect the rules that are included in the report; rules created in the specified time frame are marked with an asterisk and displayed at the bottom of each table in the Optimization & Cleanup section of the report. (Recently created rules usually have little data for rule usage analysis.) Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time
Rule Modified Since	This field is displayed only if **Report Level** = **Details**. This field does not affect the rules that are included in the report; rules modified in the specified time frame are marked with an asterisk and displayed at the bottom of each table in the Optimization & Cleanup section of the report. (Recently modified rules usually have little data for rule usage analysis.) Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time

Property	Description
Rule Detail Level	This field is displayed only if **Report Level** = **Details**. Specifies the amount of rule information to include in detailed reports.
Rule Usage	This field is displayed only if **Report Level** = **Details**. Specifies whether to include information about rule usage in detailed reports.
Object Usage	This field is displayed only if **Report Level** = **Details**. Specifies whether to include information about object usage in detailed reports.
Shadowed	This field is displayed only if **Report Level** = **Details**. Specifies whether to include information about shadowed rules in detailed reports.
Redundant	This field is displayed only if **Report Level** = **Details**. Specifies whether to include information about redundant rules in detailed reports.
Change Tracking	Specifies whether to include information about change tracking.
Analysis Period	The time frame to use for change tracking information in the report. Select **Custom** to specify a start time relative to the current time.
Appendix: list of all changes	This field is not displayed if **Report Level** = **Overview**. Specifies whether to include an overall list of changes for all firewalls at the end of the report.
Rule Changed	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a list of changes to access rules in detailed reports.
Object Changed	This field is displayed only if **Report Level** = **Details**. Specifies whether to include a list of changes to firewall objects in detailed reports.
Detailed Rule Changed	This field is displayed only if **Report Level** = **Details**. Specifies whether to include detailed information about changes to access rules in detailed reports.
Detailed Object Changed	This field is displayed only if **Report Level** = **Details**. Specifies whether to include detailed information about changes to firewall objects in detailed reports.
Include Ignored Changes	This field is displayed only if **Report Level** = **Details**. Specifies whether to include information about changes that have **Ignored** reconciliation status.
Vulnerabilities	Specifies whether to include information about vulnerability occurrences.

Property	Description
Vulnerability Occurrences	This field is displayed only if **Report Level** = **Details**. Specifies whether to include information about all vulnerability occurrences or only new vulnerability occurrences (according to the definition in **Tools** > **Options** > **Server Options** > **Entity Settings**).
Filter by Severity	This field is displayed only if **Report Level** = **Details**. Specifies whether to include only violations of specific severities in the report.
Advanced tab	
Introductory Text	A free-form field that holds the introductory text for the report.
Max Number of Detailed Records	The maximum number of records to include in each detailed section.
Split if scope greater than	For detailed reports, specifies the maximum number of firewalls to present in 1 report. If there are more firewalls than this in a detailed report, all the summaries are presented together in the report, but all the detailed information for each firewall is saved as a smaller, linked report.
Firewall Filters	
Firewall Type	Only firewalls of the selected vendors are included in the report.
Operating System	Only firewalls running the selected operating systems are included in the report.

Firewall Changes reports

Firewall Changes reports provide information about changes to firewalls in the network. The firewalls' access rules and objects are compared between 2 different models (usually Live compared with What If or Live compared with Forensics) and any changes are listed in the report.

Report sections

The following section is included in Firewall Changes reports:

- **Summary**: The changed and unchanged firewalls included in the scope of the report.

The following sections can optionally be included in a Firewall Changes report:

- For each firewall in the report:
  - **<firewall name>**: The number of changed access rules and objects found for this firewall.
  - **Changed Access Rules**: The changed access rules for the firewall with the main properties of each rule.

    Detailed reports include links from each access rule in this section to the detailed information about the access rule in the next section.
  - **Changed Access Rules – Details**: Information about each changed access rule, including deleted rules. For modified access rules, information

about the changed properties is listed in 2 columns (current model and comparison model).

Report properties

The properties that control Firewall Changes reports are described in the following table.

Property	Description
Basic tab	
Compare to	The model with which to compare the current model for reports.
Firewalls Scope	
Firewall Scope	The firewalls and firewall folders to include in the report.
Firewall Type	Only firewalls of the selected vendors are included in the report.
Report Sections	
Overview	(Read-only) The report always includes overall information about firewall changes.
Details	Specifies whether to include detailed information about firewall changes.
Advanced tab	
Display Unreferenced Objects	Specifies whether to display only referenced objects in the report.
Display Description in Summary	Specifies whether to display the comments from the access rules as part of the report; the comments can contain important information.
Max. Number of Changes per Firewall	The maximum number of changes per firewall to include in the report. If the number of changes in a firewall is larger than this value, the report states that the firewall has too many changes and no changes are included. This usually means that there is a configuration problem on the firewall. To include all the changes, increase the value of this property.

NERC reports

NERC Compliance reports present information about the compliance of network devices with the following NERC Critical Infrastructure Protection (CIP) standards of cyber security for the identification and protection of cyber assets:

- CIP-002-3 – Critical Cyber Asset Identification
- CIP-003-3 – Security Management Controls
- CIP-005-3 – Electronic Security Perimeters
- CIP-007-3 – Systems Security Management

For information about the content of NERC reports, see the NERC Compliance reports topic in the Skybox Firewall Assurance User Guide.

Report sections

The following sections are included in NERC Compliance reports:

- **Introduction**: The purpose of the report.
- **Security Perimeter Compliance**: Identification of security perimeters (zones) and the security levels of their critical firewalls (cyber assets).
- **Cyber Asset Compliance**

  For each firewall (cyber asset) in the report:

  - Summary of NERC compliance

  Optionally, for each firewall (cyber asset) in the report:

  - Access Compliance
  - Exceptions
  - Change tracking
  - Configuration Compliance

Report properties

The properties that control NERC Compliance reports are described in the following table.

Property	Description
Basic tab	
Firewall Scope	The firewalls and firewall folders to include in the report.
Report Sections	
Overview	(Read-only) The report always includes summary information about NERC Compliance.
Details	Specifies whether to include detailed information in the report.
Advanced tab	
Split if scope greater than	For detailed reports, specifies the maximum number of firewalls to present in a report. If there are more firewalls than this in a detailed report, all the summaries are presented together in the report, but all the detailed information for each firewall is saved as a smaller, linked report.

PCI Firewall Compliance reports

PCI Firewall Compliance reports present information about compliance of firewalls with PCI DSS Requirement 1: “Install and maintain a firewall configuration to protect cardholder data, a sensitive area within the trusted network of a company.”

PCI DSS Requirement 1 is represented in Skybox as an Access Policy. To maintain a protected system, the requirements are checked against the corresponding policy sections for each firewall that is in the scope of the report.

For additional information about the content of PCI Firewall Compliance reports, see the PCI Firewall Compliance reports topic in the Skybox Firewall Assurance User Guide.

Report sections

The following sections are included in PCI Firewall Compliance reports:

- **Introduction**: The purpose of the report.

  The introduction explains PCI DSS Requirement 1 and how it is modeled in Skybox. You can customize the text.

- **Summary**: The compliance for each firewall in the report, with a link to additional information.
- For each firewall in the report:
  - **Summary**: A list of the subsections of PCI DSS Requirement 1 with compliance indications for this firewall. If detailed information is included in the report, each subsection has a link to additional information.

The following sections can optionally be included in a PCI Firewall Compliance report:

- For each firewall in the report:
  - **Details**: For each subsection of PCI DSS Requirement 1, the following information is provided:
    - Folder name (in the Access Policy)
    - Description
    - Number of policy exceptions

    If there are violating access rules, they are listed in a table with links to additional information about the access rule and the PCI policy rules that the access rule violated.
  - **Exceptions**: A list of the firewall’s exceptions
- **Appendix**: The description of PCI DSS Requirement 1, including all its subsections. The text is taken directly from *PCI DSS Requirements and Security Assessment Procedures*.

Report properties

The properties that control PCI Firewall Compliance reports are described in the following table.

Property	Description
Basic tab	
PCI Policy	The PCI policy to use for the report. **Note**: If you are not using the default policy or if you made changes to the hierarchy of the policy, you must map the policy to the requirement sections.
Firewall Scope	The firewalls and firewall folders to include in the report. **Note**: The network interfaces of these firewalls must be mapped to PCI zone types.
Report Sections	
Overview	(Read-only) The report always includes a summary section for each firewall.

Property	Description
Details	Specifies whether to include detailed information about each firewall's compliance.
Exceptions	Specifies whether to include an exceptions section for each firewall.
PCI Requirement 1 Description	Specifies whether to include the description of PCI DSS Requirement 1 (for the PCI DSS version you are using) as an appendix.
Advanced tab	
Introductory Text	A free-form field that holds the introductory text for the report.
Max. Number of Firewalls	The maximum number of firewalls to include in the report. If **Firewall Scope** includes more than this number of firewalls, Skybox does not include all the firewalls in the report.
Max. Number of Violating ACLs	
Show N/A Requirements	Specifies whether to include subsections of the requirement that are not modeled in Skybox as part of the **Details** section.

Rule Usage Analysis reports

Rule Usage Analysis reports present rule usage information for firewalls to help you to understand the usage patterns of the access rules. The reports present all firewalls in the selected scope that have unused access rules or access rules with unused objects.

The properties that control Rule Usage Analysis reports are described in the following table.

Property	Description
Basic tab	
Firewall Scope	The firewalls and firewall folders to include in the report. **Note**: The selected firewalls are only included in the report if there were changes to their access rules or to the objects in the access rules during the analyzed period.
Rule Properties	
Analysis Period	The time frame of data to include in the report. Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time
Advanced tab	
Show Original Text	Specifies whether to display, in the report, the *original text* (found in the firewall configuration) of the source, destination, and service fields of the access rules. If cleared, the resolved IP addresses are used in the report.

SKYBOX NETWORK ASSURANCE REPORTS

The following report types are available when working with Skybox Network Assurance:

- Access Checks (on page 394)
- Network Access Compliance (on page 408)
- Network Configuration Compliance (on page 409)

Network Access Compliance reports

Network Access Compliance reports provide policy-related information about the compliance of your organization’s network and help you to understand the compliance status of your network to your Access Policy and to identify problematic access configuration in your network.

For information about predefined Network Access Compliance reports, see the Network Access Compliance reports topic in the Skybox Network Assurance User Guide.

Report sections

The following sections are included in Network Access Compliance reports:

- **Access Policy Compliance – Summary**: Compliance violations, including the number of access tests and the number of violations. The section also displays Access Policy tests by compliance (compliant tests compared with non-compliant / violating tests) and by severity. The information is displayed using text and pie charts.
- **Policy Sections Compliance**: The policy sections in the scope of the report and their compliance. Each policy section is linked to the list of its violations in the next section.

You must include at least 1 of the following sections in a Network Access Compliance report:

- **Violating Access Rules**: All violations (or access tests) for each policy section in the scope of the report. The violations or access tests are sorted by Access Check and then by test ID.
- **Violations**: Detailed information about each violation, including the violation properties and access results.
- **Exceptions**: The exceptions for each policy section in the scope of the report.

Report properties

The properties that control Network Access Compliance reports are described in the following table.

Property	Description
Basic tab	
Access Policy Scope	The parts of the Access Policy (policy folders, policy sections, or Access Checks) to include in the report. **Note**: Access queries are not included in Network Access Compliance reports.
Report Level	Specifies whether to include only summary information

Property	Description
	about Access Compliance, violations, and exceptions or also detailed information about each violation in the report.
Report Sections	
Violating Access Rules	
Violations	Specifies whether to include violations and access tests in the report: • **New Violations**: Include only new violations (according to the definition in **Options** > **Server Options** > **Entity Settings**) • **Violations Only**: Include all violations • **All Tests**: Include violations and successful access tests
Exceptions	Specifies whether to include exceptions in the report.
Advanced tab	
Max. Number of Services	The maximum number of services to display in the **Policy Violations – Details** section for each violation. If a violation includes more than this number of services, Skybox does not include all the services for this violation in the report.
Exception Filters: These fields are enabled only if you select **Exceptions** in the **Basic** tab.	
Created Since	Only exceptions created in the specified time frame are included in the report. Select **Custom** to define a date range by: • Specifying the earliest creation date • Specifying the earliest creation time relative to the current time
Expiration Date	Only exceptions that expire in the specified time frame are included in the report. Select **Custom** to define a date range by: • Specifying the earliest expiration date • Specifying the earliest expiration time relative to the current time

Network Configuration Compliance reports

Network Configuration Compliance reports help you to understand the compliance status of your network to your Configuration Policy and to identify problematic device configurations in your network.

Report sections

The following section is included in Network Configuration Compliance reports:

- **Summary for All Devices**: Compliance violations (including the number of Configuration Checks and the number of violations), top violations, and devices by compliance level. The information is displayed using text and pie charts.

The following sections can optionally be included in a Network Configuration Compliance report:

- **Configuration Compliance – Summary**: For each Configuration Policy in the scope, shows how many devices failed each Configuration Check.
- **Configuration Compliance – Details**: For each Configuration Policy in the scope, detailed information about each Compliance Check according to the scope.

Report properties

The properties that control Network Configuration Compliance reports are described in the following table.

Property	Description
Basic tab	
Network Scope	The parts of your network to include in the report.
Configuration Scope	The parts of the Configuration Policy (folders, Configuration Policies, or Configuration Checks) to include in the report.
Report Level	Specifies whether to include only summary compliance information or also detailed information in the report.
Report Sections	
Include Configuration Compliance Summary	Specifies whether to include a summary of compliance for each Configuration Policy.
Display Configuration Checks	(For detailed reports only) Specifies whether to include violations and Configuration Checks in the report: • **New Violations**: Include only new violations (according to the definition in **Tools** > **Options** > **Server Options** > **Entity Settings**) • **Violations Only**: Include all violations • **All Checks**: Include violations and successful Configuration Checks
Filter Checks by Severity	Specifies whether to include only Configuration Checks with the selected severity.
Include Analyzed Devices	Specifies whether to include detailed information about Configuration Checks for all analyzed devices or only for devices that have violations for that Configuration Check.
Advanced tab	
Introductory Text	A free-form field that holds the introductory text for the report.
Max. Number of detailed records	The maximum number of records to include in each detailed section.

Chapter 21

Triggers reference

This chapter describes how to use and customize Skybox triggers, and how to modify the content of the alerts that they send.

In this chapter

TRIGGERS

Triggers in Skybox are rules that cause email messages (notifications or alerts) to be sent to users to inform them of events that occurred in Skybox (for example, new or modified threat alerts, or increases in security metrics scores). In some cases, triggers can also cause a Skybox task to run a specified script. This is useful if you are working with an external ticketing system.

The types of triggers included in Skybox are listed in the following table.

Trigger type	Triggered by...
Skybox Firewall Assurance	
Change tracking (on page 412)	**Analysis – Change Tracking** tasks
Firewall Access Compliance Violation (on page 413)	**Analysis – Policy Violation** tasks
Firewall Rule Compliance Violation (on page 413)	**Analysis – Policy Violation** tasks
Skybox Network Assurance	
Network Compliance Violation (on page 414)	**Analysis – Policy Violation** tasks
Skybox Vulnerability Control	
Security Metric (on page 414)	**Analysis – Security Metrics** tasks
Threat Alert (on page 415)	Threat alert update events

Trigger type	Triggered by...
All products	
Ticket (on page 416)	Ticket update events

To create a trigger

1. Select **Tools** > **Administrative Tools** > **Triggers**.
2. In the Skybox Admin window, right-click the **Triggers** node and select **New Trigger**.
3. Select the **Trigger Type**.
4. Fill in the fields according to the trigger type.
5. Click **OK**.

Change Tracking trigger properties

Email notifications are created from change tracking triggers when **Analysis – Change Tracking** tasks are run.

Property	Description
Events tab	
New Firewall Changes	(Read-only) Specifies whether a notification is sent every time that a change to an access rule or object occurs on a firewall, including new and deleted access rules and objects.
Notify on Status Change	Specifies whether a notification is sent when the status of an access rule is changed.
Statuses	This field is enabled only if you select **Notify on Status Change**. The statuses for which notifications are sent.
Change Record Filter tab	
Firewalls	Sends notifications for the selected firewalls.
Changes created by	Sends notifications for changes made by specific users. Specify users as a comma-separated list of names or partial names. Use the characters **?** and ***** for standard pattern matching.
Notify changes in rules marked for review	Sends notifications for changes on access rules that are marked as **For Review**.
Trigger Notification tab	
Skybox Users	Sends notifications to the selected Skybox users.
External Email Addresses	Sends notifications to the specified email addresses.

For information about these triggers, see the Triggers section in the Skybox Firewall Assurance User Guide.

Firewall Access Compliance Violation trigger properties

Email notifications are created from Access Compliance violation triggers when **Analysis – Policy Violation** tasks are run.

Property	Description
Events tab	
New Firewall Violations	(Read-only) Specifies whether notifications are sent every time that a new Access Policy violation occurs on a firewall (that is, between 2 network interface zones on the same firewall).
Error Access Tests	Specifies whether to send notifications for access tests (Access Checks run on a specific device) that had an error during calculation.
Policy Violation Filter	
Firewalls	The firewalls and firewall folders for which to send notifications.
Access Policy Scope	The parts of the Access Policy (policy folders, policy sections, or Access Checks) for which to send notifications.
Severity	The severities of Access Checks for which to send notifications.
Trigger Notification tab	
Skybox Users	Sends notifications to the selected Skybox users.
External Email Addresses	Sends notifications to the specified email addresses.
Trigger Program tab	
Tasks	Specifies the **Tools – Script Invocation** tasks that are run when the triggering specifications are met.

For additional information about these notifications, see the Triggers section in the Skybox Firewall Assurance User Guide.

Firewall Rule Compliance Violation trigger properties

Email notifications are created from firewall rule compliance violation triggers when **Analysis – Policy Violation** tasks are run.

Property	Description
Events tab	
New Rule Check Violations	(Read-only) Specifies whether notifications are sent every time that a new rule policy violation occurs on a firewall (that is, between 2 network interface zones on the firewall).
Error Access Tests	Specifies whether to send notifications for tests (of a rule check on a device) that had an error during calculation.
Rule Violation Filter	
Firewalls	The firewalls and firewall folders for which to send notifications.
Rule Check Scope	The parts of the Rule Policy (policy folders, policy

	sections, or Rule Checks) for which to send notifications.
Severity	The severities of Rule Checks for which to send notifications.
Trigger Notification tab	
Skybox Users	Sends notifications to the selected Skybox users.
External Email Addresses	Sends notifications to the specified email addresses.
Trigger Program tab	
Tasks	Specifies the **Tools – Script Invocation** tasks that are run when the triggering specifications are met.

For additional information about these notifications, see the Triggers section in the Skybox Firewall Assurance User Guide.

Network Compliance Violation trigger properties

Email notifications are created from Access Compliance violation triggers when **Analysis – Policy Violation** tasks are run.

Property	Description
Events tab	
New Network Violations	(Read-only) Specifies whether notifications are sent every time that a new Access Policy violation occurs on the specified networks.
Error Access Tests	Specifies whether to send notifications for access tests (Access Checks run on a specific device) that had an error during calculation.
Policy Violation Filter	
Networks	The networks, asset groups, and assets for which to send notifications.
Access Policy Scope	The parts of the Access Policy (policy folders, policy sections, or Access Checks) for which to send notifications.
Severity	The severities of Access Checks for which to send notifications.
Trigger Notification tab	
Skybox Users	Sends notifications to the selected Skybox users.
External Email Addresses	Sends notifications to the specified email addresses.
Trigger Program tab	
Tasks	Specifies the **Tools – Script Invocation** tasks that are run when the triggering specifications are met.

Security Metric trigger properties

Security Metric triggers define the security metric events that trigger an email notification and who receives the notification. The notifications are created when **Analysis – Security Metrics** tasks are run.

Notifications can be sent when a security metric increases or decreases. You can select units and score thresholds to be the triggers. (For example, if you select Business Units, notifications are only sent if the security metric level for any of the selected Business Units changes.)

Note: A notification is sent for each Security Metric trigger, which lists all relevant changes. However, if you select **Notify on Security Metric Level Increase** and **Notify on Security Metric Level Decrease**, separate notifications are sent for increases and decreases.

Property	Description
Events tab	
Security Metric Level Increase	(Read-only) Notifications are always sent for security metric increases that match the filters.
Notification Comment	A statement to include with the notification about a security metric increase.
Security Metric Level Decrease	Specifies whether to send notifications when a security metric (that matches all the filters) decreases.
Notification Comment	A comment to include with the notification about a security metric decrease.
Security Metric Filter tab	
Security Metric Type	The type of security metric (VLI or RLI) for which notifications are sent.
Participating Units	Sends notifications if the security metric change is in a specified unit. Specify each unit separately; if you select a parent unit only, Skybox does not send notifications if the level of a child units changes.
Security Metric Threshold	Sends notifications if the security metric reaches or passes the selected level.
Trigger Notification tab	
Skybox Users	Sends notifications to the selected Skybox users.
External Email Addresses	Sends notifications to the specified email addresses.

For information about creating Security Metric triggers, see the Setting up Security Metric triggers topic in the Skybox Vulnerability Control User Guide.

Threat Alert trigger properties

Threat Alert triggers define the threat alert events that trigger an email notification and who receives it.

Notifications can be sent when threat alerts change in a specific way.

The properties of Threat Alert triggers are described in the following table.

Property	Description
Events tab	
New Threat Alerts	Specifies whether a notification is sent when a threat alert is created.

Updated Threat Alerts	Specifies whether a notification is sent when a threat alert is updated.
Status of Threat Alert Changed to	The changes that trigger notifications.
Threat Alerts not handled for more than <n> days	Sends a notification when a threat alert is overdue by the specified number of days.
Threat Alert Filter tab	
Severity	Sends a notification if the threat alert is at least the selected severity.
CVSS Base Score	Sends a notification if the threat alert's CVSS base score is in the selected range.
CVSS Temporal Score	Sends a notification if the threat alert's CVSS temporal score is in the selected range.
Products In List	Specifies the affected products for which to send notifications: • **Any**: Send notifications for all products. **Product List Items** is disabled. • **Yes**: Send notifications only if at least 1 affected product of the threat alert matches a product specified in the **Product List Items** field. • **No**: Send notifications only if at least 1 affected product of the threat alert *does not* match a product specified in the **Product List Items** field.
Product List Items	Used in conjunction with **Products In List**.
Product search string	Sends a notification if the name of any affected product of the threat alert matches the search string.
Custom threat alerts	
Created by	Sends a notification if the custom threat alerts that changed were created by specific users.
Custom threat alerts Only	Specifies whether notifications are sent only for custom threat alerts.
Trigger Notification tab	
Skybox Users	Sends notifications to the selected Skybox users.
External Email Addresses	Sends notifications to the specified email addresses.

For information about creating these notifications, see the Creating notifications topic in the Skybox Vulnerability Control User Guide.

Ticket trigger properties

Ticket triggers define the ticket events that trigger an email notification and who receives it; a notification can be sent when a ticket changes in a specific way.

The properties of ticket triggers are described in the following table.

Property	Description
Events tab	
Ticket Events	

Property	Description
Any ticket change (including creation and deletion)	Triggers notifications and scripts every time that a ticket (that matches all the filters) is created, changed, or deleted.
Specific actions and updates	Triggers notifications and scripts every time that a specified change occurs to a ticket that matches all the filters. Use the **Actions and Updates** property to specify the change types that trigger notifications.
Actions and Updates	A list of change types that, if selected, trigger notifications and scripts when they occur.
Overdue	
Notify on overdue tickets	Specifies whether notifications and scripts are triggered when a ticket becomes overdue (misses the due date for the current phase).
Ticket Filter tab	
Network Scope	(Skybox Vulnerability Control and Threat Manager only) The assets and container entities for which to send notifications.
Type	The type of ticket for which to trigger notifications and scripts.
Ticket Phases	Triggers notifications and scripts if the ticket is in a selected phase.
Ticket Owner	Triggers notifications and scripts if the ticket belongs to a selected owner.
Owner Lookup	If owners are specified in **Ticket Owner**, specifies whether to search for the selected ticket owners in the current phase of each ticket or in specific phases. If you select **Specific Phases**, select the desired phases in the **Owner Phases** field.
Owner Phases	The phases in which to search for the ticket owner.
Priority	Triggers notifications and scripts if the entity for which the ticket was created has the selected priority.
CVSS Base Score	(Skybox Vulnerability Control and Threat Manager only) Triggers notifications and scripts if the CVSS base score of the Vulnerability Definition for which the ticket was created is in the selected range.
CVSS Temporal Score	(Skybox Vulnerability Control and Threat Manager only) Triggers notifications and scripts if the CVSS temporal score of the Vulnerability Definition for which the ticket was created is in the selected range.
Trigger Notification tab	
Ticket's CC List	Sends notifications to all users listed in the cc list of the ticket.
Ticket Owner	Sends notifications to the owner (assignee) of the ticket.
Ticket Owner's	Sends notifications to all users who are in the same user

Property	Description
Group(s)	groups as the owner (assignee) of the ticket.
Ticket Requestor	Sends notifications to the user who created the ticket.
Skybox Users	Sends notifications to the selected Skybox users.
External Email Addresses	Sends notifications to the specified email addresses.
When the assignees or cc list recipients of this Ticket change, send notifications to:	
New Recipients	(Read-only) Sends notifications to users added to the ticket.
Former Recipients	Sends notifications to users removed from the ticket.
Change Manager Notification Recipients	If FA permissions are enabled for Change Manager, specifies who receives notifications about each derived change request.
User Groups Default Members	Specifies whether notifications about each derived change request are sent to the default member of all the user groups to which the relevant firewall owner belongs.
All Firewall Administrators	Specifies whether notifications about each derived change request are sent to all administrators for the relevant firewall.
Trigger Program tab	
Tasks	Specifies the **Tools – Script Invocation** tasks that are run when the triggering specifications are met.

You can customize the content of ticket notifications to suit your requirements (see Customizing ticket notifications (on page 418)).

Customizing ticket notifications

You can choose to create customized ticket notifications that are not based on the predefined notification templates, but rather use a different system. Custom notification templates are stored as part of the model and you can reuse, modify, and copy them from the Skybox Admin window.

To create a custom notification

1 Click the **Notification Templates** tab.

2 Select **Use Custom Notification**.

> Note: This specifies to Skybox to not use the default template that would usually be used for the selected event types. The notification contains only the information that you add.

3 Skybox uses the text in the **Subject** field as the subject header of the email notification:

a. Add appropriate text. For example, “`Subject: New Ticket ID `” (without the quotation marks but including the space at the end).

b. With the cursor placed after the text, click **Insert Label**.

See Keywords for notifications (on page 425) for a list of all possible keywords.

c. In the list that appears, double-click the name of the field to add. For this example, select **Ticket ID**.

   The relevant keyword (for this example, __TICKET_ID__) is inserted in the text.

d. Add any text to appear in the subject header after the keyword. In this example, you might add “ Notification” (again, without the quotation marks; remember to include a space).

4 Skybox uses the text in the **Primary Information** field as the body of the email notification. It should provide the changes that were made. Use the same steps that you used for the **Subject** field, adding lines of text and keywords.

Note: The **Details** field is not necessary in Change Manager notifications; it provides information used for other types of ticket notifications.

5 Click **OK**.

The new notification is added to the list of notifications.

Creating additional notifications for the same (or similar) event

You can create additional notifications for the same (or a similar) event. This can be useful if you need to create multiple notifications for an event. For example, you might want a very simple notification for the **Ticket Requestor** and a more detailed notification for the owner of the next phase, or you might have created a notification for ticket promotion and want a very similar notification for ticket demotion.

To create a custom notification based on an existing notification

1 Right-click the notification and select **Create Notification Like**.

2 Open the new (copy) notification from the list and make necessary changes.

CUSTOMIZING NOTIFICATION TEMPLATES

The texts of the email notifications sent by triggers are based on templates. There are separate templates for notification headers and for details (*sections*). Skybox provides default template files; you can create additional templates for notifications.

A complete notification for an event consists of a header and at least 1 section (usually 1 section per event). The following sample notification consists of 1 header and 3 sections.

```
Vulnerability Type Event: Updated Status for Vulnerability Type(s)
Notification Rule Name: Irrelevant Vulnerabilities
Number of Vulnerability Types whose status was updated: 3

Vulnerability Type(s) Details:
===========================================
#1
ID: SBV-17414
Title: Gforge <= 4.6.99 SQL Injection Allows Remote SQL Commands Execution
Severity: High (7.5)
CVSS Base Score: 7.5
CVSS Temporal Score: 6.7
Status: Irrelevant
```

```
Reported Date: 1/15/08
Modification Date: 1/28/09
CVE: CVE-2008-0173
Last Change: The Description of solution ID 60241 was Modified
-------------------------------------------

#2
ID: SBV-17429
Title: MyBB < 1.2.11 forumdisplay.php and search.php Scripts Allow Remote
Code Execution
Severity: High (7.5)
CVSS Base Score: 8.2
CVSS Temporal Score: 7.1
Status: Irrelevant
Reported Date: 1/16/08
Modification Date: 1/28/09
CVE: CVE-2008-0382
Last Change: New Related Source was added: CVE-2008-0382
-------------------------------------------

#3
ID: SBV-17441
Title: Sun Java System Access Manager 7.1 on Application Server 9.1
Container Authentication Bypass
Severity: High (7.5)
CVSS Base Score: 7.5
CVSS Temporal Score: 6.1
Status: Irrelevant
Reported Date: 10/1/07
Modification Date: 1/28/09
CVE: CVE-2007-5152
Last Change: The Description of solution ID 60359 was Modified
-------------------------------------------
```

To edit a notification template

1 Select the correct template (see page 420).

2 Modify the template (see page 423) and save it.

SELECTING THE CORRECT TEMPLATE

The notification templates are stored in the `<Skybox_Home>\server\conf\notification_templates` directory.

There are separate templates for each type of notification (Security Metric, Threat Alert, change tracking, firewall compliance violation, and ticket). The _header templates define how the main information about the notification appears in the email alert; the _section templates define how each event appears in the email notification.

The tables in subsequent sections explain which files are used for each type of notification.

To change the content of a template, see Editing templates (on page 423).

Files for change tracking notifications

The files that are used for change tracking notifications are listed in the following table.

Event	File name
Change to an access rule or firewall object	changetrackingnew_header.txt changetrackingnew_section.txt

For a list of keywords used in these files, see Keywords for change tracking notifications (on page 424).

Files for firewall compliance violation notifications

The files that are used for firewall compliance violation notifications are listed in the following table.

Event	File name
Firewall compliance violation	aprviolation_header.txt aprviolation_section.txt

For a list of keywords used in these files, see Keywords for firewall violation notifications (on page 424).

Files for Security Metric notifications

The files that are used for Security Metric notifications are listed in the following table.

Event	File name
Increase in security metrics levels	kpilevelincrease_header.txt kpilevelincrease_section.txt
Decrease in security metrics levels	kpileveldecrease_header.txt kpileveldecrease_section.txt

For a list of keywords used in these files, see Keywords for Security Metric notifications (on page 425).

Files for ticket notifications

The files that are used for ticket notifications are listed in the following table.

Event	File name
New ticket created	ticketcreated_header.txt ticketcreatedtypeaccesschange_header.txt ticketcreated_section.txt
Ticket updated	ticketupdated_header.txt ticketupdatedtypeaccesschange_header.txt ticketupdated_section.txt
Ticket updated (Used for updates other than change of phase, owner, or status)	ticketminorfieldsupdate_header.txt ticketminorfieldsupdatetypeaccesschange_header.txt ticketminorfieldsupdate_section.txt
Ticket cloned	ticketcloned_header.txt ticketclonedtypeaccesschange_header.txt ticketcloned_section.txt
Ticket closed	ticketclosed_header.txt

Event	File name
	ticketclosedtypeaccesschange_header.txt ticketclosed_section.txt
Ticket deleted	ticketdeleted_header.txt ticketdeletedtypeaccesschange_header.txt ticketdeleted_section.txt
Ticket demoted	ticketdemoted_header.txt ticketdemotedtypeaccesschange_header.txt ticketdemoted_section.txt
Overdue ticket	ticketoverdue_header.txt ticketoverduetypeaccesschange_header.txt ticketoverdue_section.txt
Ticket predue (coming due soon)	ticketpredue_header.txt ticketpreduetypeaccesschange_header.txt ticketpredue_section.txt
Ticket promoted	ticketpromoted_header.txt ticketpromotedtypeaccesschange_header.txt ticketpromoted_section.txt
Ticket reassigned (new owner)	ticketreassigned_header.txt ticketreassignedtypeaccesschange_header.txt ticketreassigned_section.txt
Ticket rejected	ticketrejected_header.txt ticketrejected_section.txt
Ticket reopened	ticketreopened_header.txt ticketreopenedtypeaccesschange_header.txt ticketreopened_section.txt
Request to close a ticket	ticketrequesttoclose_header.txt ticketrequesttoclosetypeaccesschange_header.txt ticketrequesttoclose_section.txt
Ticket resolved	ticketresolved_header.txt ticketresolved_section.txt
Ticket implementation verified	ticketverified_header.txt ticketverified_section.txt

For a list of keywords used in these files, see Keywords for ticket notifications (on page 425).

Files for Threat Alert notifications

The files that are used for Threat Alert notifications are listed in the following table.

Event	File name
Creation of new threat alert	vtcreation_header.txt vtcreation_section.txt

Event	File name
Threat alert not handled in a specific number of days	vtneglected_header.txt vtneglected_section.txt
Status change of a threat alert	vtstatuschange_header.txt vtstatuschange_section.txt
Update of a threat alert (new information)	vtupdate_header.txt vtupdate_section.txt
Update of significant fields of a threat alert (new information)	vtsignificantupdate_header.txt vtsignificantupdate_section.txt

Note: A significant field is a field that can change the ticket flow or priority—a change in severity or urgency, or a change in the list of affected products.

For a list of keywords used in these files, see Keywords for Threat Alert notifications (on page 428).

EDITING TEMPLATES

Each notification template consists of static text and keywords (variables) as in the following example.

```
ID: __TICKET_ID__
Ticket Type: __TICKET_TYPE__
Title: __TITLE__
Owner: __OWNER_NAME__
Phase: __CURRENT_PHASE__
Due Date: __DUE_DATE__
Pending Closure With Status: __STATUS__
```

The text in the template is the actual text that appears in each notification of the selected type.

The keywords are listed in the template as __<KEYWORD_NAME>__. The keywords are replaced by the value of the relevant field in Skybox when an alert is created.

The names of the keywords cannot be changed, but you can change the text and use different keywords. You can add text and keywords to a file or delete text and keywords. For example, if the owner is not necessary for the notification type that is defined by the template, delete the line:

```
Owner: __OWNER_NAME__
```

The keywords that you can use in the notifications and the fields from which the keywords are taken are listed in:

- Keywords for change tracking notifications (on page 424)
- Keywords for firewall compliance violation notifications (on page 424)
- Keywords for Security Metric notifications (on page 425)
- Keywords for ticket notifications (on page 425)
- Keywords for Threat Alert notifications (on page 428)
- For information about the template to use for each notification type, see Selecting the correct template (on page 420).

Keywords for change tracking notifications

Keywords that you can use for change tracking notifications are listed in the following table.

Change field	Keyword
Current date	__CURRENT_DATE__
Total number of changes	__TOTAL_NUMBER_OF_CHANGES__
Number of firewalls with changes	__FIREWALL_NUM__
The section in the alert (each firewall has its own section)	__SECTION_NUMBER__
The name of the firewall	__FW_NAME__
Total number of changes for this firewall	__TOTAL_FW_NUMBER_OF_CHANGES__
Number of access rules changed for this firewall	__ACL_NUMBER_OF_CHANGES__
Number of objects changed for this firewall	__OBJECT_NUMBER_OF_CHANGES__
Original Rule ID	__ORIGINAL_RULE_ID__
Original Text Before	__ORIGINAL_TEXT_BEFORE__
Original Text After	__ORIGINAL_TEXT_AFTER__
List of detailed changes for the firewall	__DETAILED_CHANGES_TABLE__

Keywords for firewall compliance violation notifications

Keywords that you can use for firewall compliance violation notifications are listed in the following table.

Violation field	Keyword
The name of the notification that created this alert	__NOTIFICATION_RULE_NAME__
The creation time of the violation	__CREATION_TIME__
The number of the violation	__NUMBER__
The test ID of the violation	__ID__
The importance of the violated Access Check	__IMPORTANCE__
The name of the firewall where the violation occurred	__FIREWALL_NAME__
The IP address of the firewall	__FIREWALL_IP__
The name of the Access	__APR_NAME__

Violation field	Keyword
Check	
The type of the Access Check (Limited, No-Access, or Full Access)	__APR_TYPE__
The path of the Access Check in the policy tree	__APR_PATH__
The source used in the Access Check	__SOURCE__
The destination used in the Access Check	__DESTINATION__

Keywords for Security Metric notifications

Keywords that you can use for Security Metric notifications are listed in the following table.

Security metrics field	Keyword
The notification type	__NOTIFICATION_TYPE__
Security metric short name	__KPI_SHORT_TYPE__
Security metric event type (increase or decrease)	__EVENT_TYPE__
The name of the notification that created this alert	__NOTIFICATION_RULE_NAME__
Security metric long name	__KPI_TYPE__
Last-but-one security metric calculation time	__PREV_KPI_CALC_TIME__
Most recent security metric calculation time	__LAST_KPI_CALC_TIME__
User comment	__USER_COMMENT__
Link to the security metrics web interface	__LINK_TO_WEB_UI__
The name of the security metric unit	__UNIT_NAME__
New security metrics score	__NEW_KPI_LEVEL__
Security metrics score from previous calculation	__OLD_KPI_LEVEL__

Keywords for ticket notifications

Keywords that you can use in all ticket notifications are listed in the following tables. You can also use all Threat Alert notifications fields for threat alert ticket notifications.

To include a Vulnerability Definition or threat alert field in the notification template, add the prefix “__VT” to the field name in the ticket notification template. For example, to include the reported date of the Vulnerability Definition in ticket notifications, include “__VT_Reported_Date__” in the template.

You can use the keywords in the following table in all ticket notifications.

Ticket field	Keyword
ID	__TICKET_ID__
Ticket type	__TICKET_TYPE__
Title	__TITLE__
Ticket description	__TICKET_DESCRIPTION__
Priority	__PRIORITY__
Phase	__CURRENT_PHASE__
Due date	__DUE_DATE__
Original phase due date (if it has changed)	__PHASES_ORIGINAL_DATES__
Ticket affected products	__TICKET_AFFECTED_PRODUCTS__
Names of additional changed fields	__ADDITIONAL_FIELDS_UPDATED__
<Name of changed field>	__UPDATED_FIELD__
<Old value of changed field>	__OLD_VALUE__
<New value of changed field>	__NEW_VALUE__

You can use the keywords in the following table in Access Change ticket notifications

Ticket field	Keyword
The importance of the violated Access Check	__IMPORTANCE__
The test ID of the violated Access Check	__VIOLATION_ID__
The name of the Access Check	__APR_NAME__
The type of the Access Check (Limited, No-Access, or Full Access)	__APR_TYPE__
The path of the Access Check in the policy tree	__APR_PATH__
The source used in the Access Check	__SOURCE__
The destination used in the Access Check	__DESTINATION__
The original change requests of the ticket	__ORIGINAL_CHANGE_REQUESTS__
The derived change requests of the ticket	__DERIVED_CHANGE_REQUESTS__

Keywords that you can use in ticket notifications for specific events are listed in the following table.

Ticket field	Keyword	Event / Note
Creation time	__CREATION_OF_TICKET__	Ticket creation (and other ticket events, when necessary)
Original ticket ID	__ORIGINAL_TICKET_ID__	Cloned ticket
URL	__URL__	Displays the URL of the Change Manager with the relevant ticket ID.
Done date	__DONE_DATE__	Ticket completion
Status	__STATUS__	Ticket completion (and other ticket status change notifications)
Closure type	__CLOSURE_TYPE__	Ticket closure (explains how the ticket was closed)
Deletion time	__DELETION_TIME__	Ticket deletion
Deleted by	__DELETED_BY__	Ticket deletion
Current owner	__CURRENT_OWNER__	Events (including promote, demote, or reassign)
Current owner with email	__CURRENT_OWNER_WITH_EMAIL__	The same as __CURRENT_OWNER__, but adds the email address in parentheses. If the user does not have an email address defined, the same as __CURRENT_OWNER__
Previous owner	__PREVIOUS_OWNER__	Events (including promote, demote, or reassign)
Previous owner with email	__PREVIOUS_OWNER_WITH_EMAIL__	The same as __PREVIOUS_OWNER__, but adds the email address in parentheses. If the user does not have an email address defined, the same as __PREVIOUS_OWNER__
Previous phase	__PREVIOUS_PHASE__	Phase-changing events (including promote or demote)
Current phase number	__CURRENT_PHASE_NUMBER__	Displays the number of the current phase. If there are no phases or if the ticket is closed, this field is empty.
Previous phase number	__PREVIOUS_PHASE_NUMBER__	For all phase-changing events. Displays the number of the previous phase. In all other cases, this field is empty.

Ticket field	Keyword	Event / Note
Total number of phases	__TOTAL_NUMBER_OF_PHASES__	Displays the total number of phases of the ticket. If there are no phases, this field is empty.
Latest user comment	__LAST_USER_COMMENT__	
Start time of the current phase	__CURRENT_PHASE_START_TIME__	
Phase due date	__CURRENT_PHASE_DUE_DATE__	Overdue ticket

Keywords for Threat Alert notifications

Keywords for Threat Alert notifications are listed in the following table.

Threat alert field	Keyword
Threat event type	__EVENT_TYPE__
Notification name	__NOTIFICATION_RULE_NAME__
Number of new threat alerts	__VT_NUMBER__
Threat types	__DETAILS__
(The number of the threat alert in the alert)	__NUMBER__
ID	__ID__
Title	__TITLE__
Severity	__SEVERITY_LEVEL__ __SEVERITY_SCORE__
CVSS base score	__CVSS_BASE_SCORE__
CVSS temporal score	__CVSS_TEMPORAL_SCORE__
Status	__STATUS__
Reported date	__REPORTED_DATE__
Modification date	__MODIFICATION_DATE__
CVE	__CVE__
Last change	__LAST_CHANGE__
Last modification source	__LAST_MODIFICATION_SOURCE__
Last modified by system	__LAST_MODIFIED_BY_SYSTEM__
Last modified by user	__LAST_MODIFIED_BY_USER__

Chapter 22

Exportable data

This chapter explains the information that you can retrieve from the Skybox database, and the formats in which you can retrieve it.

In this chapter

CSV-EXPORTABLE DATA

You can export most Skybox data in CSV format using shortcut menus. For some data types, you can automate the export using CSV export tasks.

The data that you can save to a CSV file by right-clicking an entity is listed in the following table.

Entity	Workspaces	Additional information
Tickets	Ticket, Threat Manager	
Model analyses • Networks • Assets • Network interfaces	Model	
Business Asset Groups	Exposure	For each Business Asset Group, the output includes a list of its member assets (in 1 field).
Vulnerability occurrences	Exposure	
Vulnerability Definitions	Threat Manager	
Security metrics information for Business Units and Business Asset Groups	Security Metrics	
Access rules	Firewall Assurance, Network Assurance	The output file includes all the access rules of the specified scope, with one row per access rule that includes information about the rule and all related Firewall Assurance information.
Firewall Access	Firewall	For each Access Check, the output file includes one row for each violation

Entity	Workspaces	Additional information
Compliance	Assurance	(<firewall identification details> <violation details> <violating rule>).
Rule Compliance	Firewall Assurance	For each Rule Check, the output file includes a row for each violation.
Rule usage data	Firewall Assurance	Each row in the output file represents an access rule.
Shadowed rules	Firewall Assurance	Each row displays a shadowed rule and its shadowing rules.
Redundant rules	Firewall Assurance	Each row displays a redundant rule and the rules that make it redundant.
Change tracking	Firewall Assurance	Each row describes a change in an access rule or object.
Access Compliance (by selecting a policy, folder, or section)	Network Assurance	The output might include multiple rows for each Access Check, each row representing a violation.

Note: You can save any table displayed in Skybox in the Table pane or the Details pane to a CSV file (from the **File** menu, select **Export Table to CSV**, with the table selected). Tables exported using this method are saved without any preprocessing.

CSV export tasks

Skybox has tasks that export CSV data on a regular basis. The files are stored, by default, on the Skybox Server machine at `<Skybox_Home>\data\csv`.

The available tasks are listed in the following table.

Skybox product	CSV export task	Comments
Skybox Firewall Assurance and Skybox Network Assurance	CSV compliance results export (on page 331)	
	CSV analysis export (on page 329)	Model analyses only
	CSV Configuration Compliance export (on page 332)	
	CSV access rules review export (on page 327)	
	CSV exception export (on page 334)	
Skybox Firewall Assurance	CSV change tracking export (on page 330)	
	CSV optimization and cleanup export (on page 338)	Exports rule usage data, and shadowed and redundant rules
	CSV firewall assurance export (on page 335)	

Skybox product	CSV export task	Comments
Skybox Vulnerability Control and Skybox Threat Manager	CSV analysis export (on page 329)	
Skybox Vulnerability Control	CSV security metrics export (on page 340)	

Note: In the task fields, you can specify that email recipients (if any) receive the file in compressed (ZIP) format.

OTHER EXPORTS

Some Skybox information is available by other means, including API, XML, and graphic files.

- You can use the Skybox web API for:
  - SOC integration: Retrieve Skybox events
  - Helpdesk integration: Synchronize tickets (unidirectional or bidirectional)
  - Access analysis: Remote activation of the Skybox Access Analyzer

  For information about the Skybox API, see the APIs part of the Skybox Developer Guide.

- You can export and import Firewall Assurance and Network Assurance policies in XML format. You can export the following policies from shortcut menus:
  - Access Policies
  - Rule Policies (Skybox Firewall Assurance only)
  - Configuration Policies (Skybox Firewall Assurance only)
- The Network Map can be exported in JPG and GraphML formats.
- You can export vulnerability occurrence analyses (lists of vulnerability occurrences) to XML files in Qualys format for integration with SIEM solutions; right-click the analysis in the tree and select **Export to XML – Vulnerability Occurrences** or use an **XML Vulnerability Occurrence (Qualys Format) Export** task.

Part III: Tools

This part describes the tools that are provided for use in Skybox Manager.

Chapter 23

Access Control List Editor

Use the Access Control List Editor to view and, in the What If model, add, modify, and delete access rules used by an asset in the model.

The Access Control List Editor is available on every asset that has access rules.

In this chapter

USING THE ACCESS CONTROL LIST EDITOR

To open the Access Control List Editor

› Right-click an asset in the Tree pane or the Table pane and select **Access Rules**.

  - Each rule chain in the device ACL is displayed in a separate tab. The number and names of the rule chains vary according to the device type.
  - Access rules with a green background are implicit rules on the firewall. Access rules with a gray background are disabled.
  - The **Original Rule ID** column shows the rule number in the original vendor application.

The Access Control List Editor allows the following actions:

› **Find**: Enables you to search for specific access rules.

  To use pattern matching in the search, select **Pattern match (? and *)** in the **Match Criteria** field; you can then use the characters **?** and ***** for standard pattern matching in the **Find What** string.

› **Show Object Names / Show Resolved Addresses**: Toggles the display in the **Source** and **Destination** columns between object names and resolved names (that is, how Skybox interpreted the object names based on the current model).

› **Object Tree**: If firewall objects are available, displays the object tree next to the list of rules.

› **Move Up**, **Move Down**, and **Move To**: These actions change the order of the access rules.

› **Move to Other Chain**: Enables you to move the selected access rule to a different rule chain.

- **Modify**: Enables you to edit the selected access rule in the Access Rule Properties dialog box (see page 434).
- **New**, **Remove**, **Disable** / **Enable**

Note: Disabled access rules are grayed and italicized.

ACCESS RULE PROPERTIES

The properties of access rules are described in the following table.

Property	Description
Action Type	The action to take on a packet (traffic) that matches the rule's criteria (properties). **Note**: If you select **Undefined**, the action taken is **Deny**.
Direction Type	The direction of the packets for which to apply the access rule.
Expiration Date	(Check Point firewalls only) The expiration date of the access rule. If a rule has passed its expiration date, Skybox does not use it in access analysis, Access Compliance, or attack simulation.
Original Rule ID	(Read-only) The original rule ID (name or number) found in the firewall configuration, if the ID exists. This information is retrieved by the task that reads the configuration.
Original Text	(Read-only) The original command for the access rule found in the device configuration, if the command exists. This information is retrieved by the task that reads the configuration.
Source Network Interfaces	The network interfaces on which to apply the rule only if the packet arrived from the specified interface.
Network Interfaces	The network interfaces on which to apply the rule (for any packet direction).
Routed Network Interface	(Cisco firewalls only) The egress interface configured in the NAT rule. **Note**: If you provide an egress interface, no route lookup is done.
Source	
Addresses	A comma-separated list of source IP addresses for which to match the rule (the permitted source addresses for a packet). • Separate the values of a range with a hyphen. • To permit all source addresses *except* those selected, select **NOT**.
Users	(Palo Alto Networks, Check Point, and FortiGate firewalls only) A list of users that get permissions in the rule; this field is populated when importing the firewall. A user applies to the firewall; the firewall identifies the user based on the IP address from LDAP (or the VPN login) and then permits the user to access the destination.

Property	Description
Objects	(Except Check Point firewalls) The original representation of the IP addresses in firewall objects.
Name	(Check Point firewalls only)
Destination	
Addresses	A comma-separated list of destination IP addresses for which to match the rule (the permitted destination addresses for a packet). • Separate the values of a range with a hyphen. • To permit all destination addresses *except* those selected, select **NOT**.
Objects	(Except Check Point firewalls) The original representation of the IP addresses in firewall objects.
Name	(Check Point firewalls only)
Services	
Services	The services for which to match the rule (the permitted services for a packet). To manage the services for the rule, click the **Browse** button to open the Services Selection dialog box and then click **Add** to open the New Service dialog box. • To permit all services *except* those selected, select **NOT**. **Note**: To define a service as a specific IP protocol, select **IP** and then select **Protocol**. Then, if you know: • The protocol name; select a protocol from the drop-down list. • The protocol number; type it—when you click **OK**, Skybox verifies that this is a valid protocol number and substitutes the protocol name
Applications	• (Palo Alto Networks firewalls) A list of the applications that are permitted for the rule. • (FortiGate firewalls) A list of the applications that are *not* permitted for the rule. The firewall uses traffic identification to determine the applications that exist for the rule in addition to the regular HTTP (port 80) communication.
Objects	(Except Check Point firewalls) The original representation of the applications in firewall objects.
Name	(Check Point firewalls only)
NAT	These fields are enabled only if **Action Type** = **Translate**.
Source	A comma-separated list of NAT source addresses for which to match the rule (the permitted NAT source addresses for a packet). • Separate the values of a range with a hyphen.
Destination	A comma-separated list of NAT destination addresses for which to match the rule (the permitted NAT destination addresses for a packet). • Separate the values of a range with a hyphen.

Property	Description
Service	The NAT service (protocol and port). Each service is one of: • `protocol/port` • `protocol/(range-of-ports)`
VPN	
VPN Usage	Specifies whether data is sent over a VPN: • **None**: Data is not sent over a VPN; the rule is a regular access rule. • **Any**: A packet matches the rule only if it arrives or is sent out over a VPN of this firewall. • **Specific**: A packet matches the rule only if it comes in or leaves the firewall over the VPN specified in **Specific**. • **Remote Access**: The access rule applies only to packets coming from a Remote Access VPN. **Note**: If you select **Remote Access**, you must set **Action Type** to **Authenticate**.
Specific	This field is enabled only if **VPN Usage** = **Specific**. The VPN over which to send data.
IPS	The IPS area is displayed (instead of the VPN area) only if **Action Type** = **IPS**.
Rule Group	Specifies whether to use only the selected IPS rule group.
Rule Attributes	
Disabled	Specifies whether the access rule is disabled (has no effect). You can also change the value for this field in the Access Control List Editor, using the **Enable** / **Disable** button.
Unsupported	Specifies that this access rule is unsupported by Skybox. **Note**: Unsupported access rules cannot be modeled or represented in the model for some reason, and they are therefore disabled in the model.
Implied	(Read-only) Specifies whether the access rule is *implied* (that is, it was not defined explicitly by the user but is derived from other device settings).

ACCESS RULE PROPERTIES: RULE REVIEW

Use the Access Rule Properties dialog box with Rule Review section to review access rules. The dialog box displays:

- Basic information about the access rule, retrieved from the device
- Information about the access rule from Skybox processes, including compliance and usage trace information
- Attributes that are assigned to the rule for review purposes (for example, owner information and IDs of any related tickets)

The properties of the (extended) Access Rule Properties dialog box are described in the following tables.

Basic information

All the information in this area is read-only; you can modify access rules from the Access Control List Editor (see page 433).

Property	Description
Action Type	The action to take on a packet (traffic) that matches the rule's criteria (properties).
Direction Type	The direction of the packets for which to apply the access rule.
Chain	The chain in which the access rule is found.
Expiration Date	(Check Point firewalls only) The expiration date of the access rule. If a rule has passed its expiration date, Skybox does not use it in access analysis, Access Compliance, or attack simulation.
Original Text	The original command for the access rule found in the device configuration, if the command exists.
Original Rule ID	The original rule ID (name or number) found in the firewall configuration, if the ID exists.
Modification Time	The most recent time that the access rule was modified on the device.
Network Interfaces	The network interfaces on which to apply the rule (for any packet direction).
Source Network Interfaces	The network interfaces on which to apply the rule only if the packet arrived from the specified interface.
Routed Network Interface	(Cisco firewalls only) The egress interface configured in the NAT rule. **Note**: If you provide an egress interface, no route lookup is done.
Source	
Addresses	A comma-separated list of source IP addresses that match the rule (the permitted source addresses for a packet).
Users	(Palo Alto Networks, Check Point, and FortiGate firewalls only) A list of users that get permissions in the rule; this field is populated when importing a Palo Alto Networks firewall. A user applies to the firewall; the firewall identifies the user based on the IP address from LDAP (or the VPN login) and then permits the user to access the destination.
Objects	(Except Check Point firewalls) The original representation of the IP addresses in firewall objects.
Name	(Check Point firewalls only)
Destination	
Addresses	A comma-separated list of destination IP addresses that match the rule (the permitted destination addresses for a packet).

Property	**Description**
Objects	(Except Check Point firewalls) The original representation of the IP addresses in firewall objects.
Name	(Check Point firewalls only)
Services	
Services	The services that match the rule (the permitted services for a packet).
Rule Applications	• (Palo Alto Networks firewalls) A list of the applications that are permitted for the rule. • (FortiGate firewalls) A list of the applications that are *not* permitted for the rule. The firewall uses traffic identification to determine the applications that exist for the rule in addition to the regular HTTP (port 80) communication.
Objects	(Except Check Point firewalls) The original representation of the applications in firewall objects.
Name	(Check Point firewalls only)
Description	A description of the access rule (provided within the device configuration).
User Comments	Comments about the access rule (provided within the device information).

Access rule information from Skybox processes

The **Compliance Category** table in the **Highlights** tab displays an overview of the information about the access rule taken from Skybox processes; all information in this table is read-only.

You can view detailed read-only information in the **Rule Details** tab.

Property	**Description**
Access Policy	The number of Access Policy violations caused by the rule. The violations are listed in the **Policy Compliance** tab.
Rule Policy	The number of Rule Policy violations caused by the rule. The violations are listed in the **Policy Compliance** tab.
Usage Trace	Rule trace summary (when available). The **Usage Trace** tab includes: • Detailed information about the rule trace for each object in the access rule (when available) • The usage type and hit count for the rule
Shadowed & Redundant	The number of rules that shadow the rule and rules that cause the rule to be redundant. The **Shadow** tab includes detailed information about the shadowing; the **Redundant** tab includes detailed information about the redundancy.
Change Tracking	The number of changes to the access rule. The **Change Tracking** tab lists the actual changes.

Business attributes

The Business Attributes area of the **Highlights** tab displays user-defined business information of the access rule that can be used for review and recertification; you can edit the value of these attributes.

Property	Description
Owner	The owners of the access rule.
Ticket ID	The IDs of any tickets related to the access rule. You can enter these values manually for external ticketing systems. When a request for recertifying the rule is opened, Skybox enters the ID of the requesting ticket in this field (and it then becomes read-only).
Next Review Date	The next date set for reviewing the access rule.
Email	The email addresses of the access rule owners.
Business Function	The business function of the access rule.
Comment	Comments about the access rule.

If your organization uses custom business attributes, they are listed here also.

Chapter 24

Working with routing rules

Routing rules are resolved from routing tables and from configuration files of routers and other gateways. During data collection, Skybox reads and models routing rules, and normalizes them into the routing rule data format used by Skybox.

Skybox supports standard routing rules and policy-based routing (PBR) rules.

This chapter describes how to view routing rules and how to manage them when necessary (usually in the What If model) by adding, modifying, deleting, and replicating routing rules manually.

In this chapter

MANAGING ROUTING RULES

You can view routing rules in the Details pane (**Routing Rules** tab) when you select a router (or other asset with routing rules) in the Table pane. You can view and edit the rules in the Routing Rules Editor.

To open the Routing Rules Editor

1 Open the Model workspace.

2 In the tree, select an entity node that displays, in the Table pane, the desired asset.

3 In the Table pane, right-click the asset and select **Routing Rules.**

The Routing Rules Editor has 2 tabs: **Routing Rules** and **PBR**. The properties of routing rules are described in Routing rule properties (on page 441) and Access Policy-based routing rule properties (on page 442).

To add a new routing rule

1 In the Routing Rules Editor, click **New**.

2 In the New Routing Rule Properties dialog box, fill in the fields of the new rule (see Routing rule properties (on page 441)) and click **OK**.

To modify a routing rule

1 In the Routing Rules Editor, select a routing rule to modify.

(To search for a rule, click **Find**; see Finding routing rules (on page 441).)

2 Click **Modify**.

3 In the Routing Rule Properties dialog box, modify values of properties (see Routing rule properties (on page 441)) and click **OK**.

To add a new PBR

1 In the Routing Rules Editor, click the **PBR** tab.

2 Click **New**.

3 In the New Access Policy Based Routing Rule dialog box, fill in the fields of the new rule (see Access Policy-based routing rule properties (on page 442)) and click **OK**.

To modify a PBR

1 In the Routing Rules Editor, click the **PBR** tab.

2 Select the PBR to modify.

3 Click **Modify**.

4 In the Access Policy Based Routing Rule Properties dialog box, modify the fields (see Access Policy-based routing rule properties (on page 442)) and click **OK**.

Finding routing rules

Use the Find in Table (Routing Rules) dialog box to find a routing rule in the current tab of the Routing Rules Editor.

The properties in this dialog box are described in the following table.

Property	Description
Find what	The string for which to search. Use the characters **?** and ***** for standard pattern matching (see the **Match Criteria** field later in this table).
Look in Field	The fields (columns) to search for the string specified in the **Find what** field.
Search	The search direction.
Case Sensitive	Specifies whether the search for the string specified in the **Find what** field is case-sensitive.
Match Criteria	The required match between the routing rule properties and the string listed in the **Find what** field. Select **Pattern match (? and *)** if the **Find what** field uses the characters **?** and ***** for standard pattern matching.

Routing rule properties

Use the Routing Rule Properties dialog box to modify and create routing rules.

The properties in this dialog box are described in the following table.

Property	Description
Destination IP Address	The destination IP address for the rule.

Property	Description
Destination Mask	This field is displayed only for IPv4 rules. The netmask of **Destination IP Address**.
CIDR	This field is displayed only for IPv6 rules. The CIDR of **Destination IP Address**.
Gateway IP Address	The gateway IP address for the rule. If the computer (host) is directly connected to the gateway, use a value of 0.0.0.0.
Network Interface	The network interface for the rule.
Metric	The best (most appropriate) rule for the network destination (the smaller the metric, the better it is for this purpose). This value should depend on the value of the **Dynamic** property.
Dynamic	Specifies whether the rule was created by a dynamic routing protocol. • Select this option if the rule is *dynamic*—the rule is created by a dynamic routing protocol (for example, OSPF or BGP). This choice is good for large networks. Use a high **Metric**. • Clear this option if the rule is *static*—the rule is created explicitly. This choice is good for small networks and as a fallback for large networks. Use a low **Metric**.

Access Policy-based routing rule properties

Use the Access Policy Based Routing Rule Properties dialog box to modify and create policy-based routing rules.

The properties of policy-based routing rules are described in the following table.

Property	Description
Action Type	The action to take when a packet matches the rule. • **Undefined**: Same as **Deny**. • **Allow**: If the packet matches the rule, permit the packet to continue. • **Deny**: If the packet matches the rule, drop the packet. • **IPS**: If the packet matches the rule, run the IPS checks as defined by the rule and permit the packet to continue if nothing malicious found.
Applied Network Interfaces	The network interfaces for which to apply the rule for an inbound packet.
Default	Specifies whether to use the usual (non-PBR) routing rule if it exists (if it does not exist, route the packet using the PBR rule). Clear this option to skip the usual routing rules for this packet. • If the PBR rule uses a default definition for the next hop or interface, Skybox uses this rule only if no other relevant regular (non-PBR) routing rule exists. • If the PBR rule does not use the default definition for

Property	Description
	the next hop or interface, Skybox uses the PBR rule instead of the regular (non-PBR) routing rule.
Outgoing Network Interfaces	The network interfaces for which to apply the rule for an outbound packet.
Next Hop	The next IP address to which the computer (host) connects.
Original Text	The text of the command found in the router configuration. This information is retrieved by the Skybox task that reads the configuration. **Note**: This field contains text only for devices with command syntax.
Source	A comma-separated list of permitted source IP addresses for a packet. • Separate the values of a range with a hyphen. • To permit all source IP addresses *except* those selected, select **NOT**.
Destination	A comma-separated list of permitted destination IP addresses for a packet. • Separate the values of a range with a hyphen. • To permit all destination IP addresses *except* those selected, select **NOT**.
Services	A comma-separated list of permitted services (protocol and port). Each service is one of: • `protocol/port` • `protocol/(range-of-ports)` To permit all services *except* those selected, select **NOT**.
User Comments	A statement to display in the **User Comments** column in the **PBR** tab of the Routing Rules Editor.

REPLICATING ROUTING RULES

Skybox supports the replication of a set of routing rules to all the assets in a network, asset group, or Business Asset Group.

To replicate routing rules

1. In the **Model** workspace, locate the desired asset in the Table pane.
2. Right-click the asset and select **Advanced** > **Replicate Routing Rules to**.
3. In the Replicate Routing Rules dialog box, select the destination type for the routing rules: **Network**, **Asset Group**, or **Business Asset Group**.
4. Select the destination for the replication of the routing rules.
5. Click **OK**.

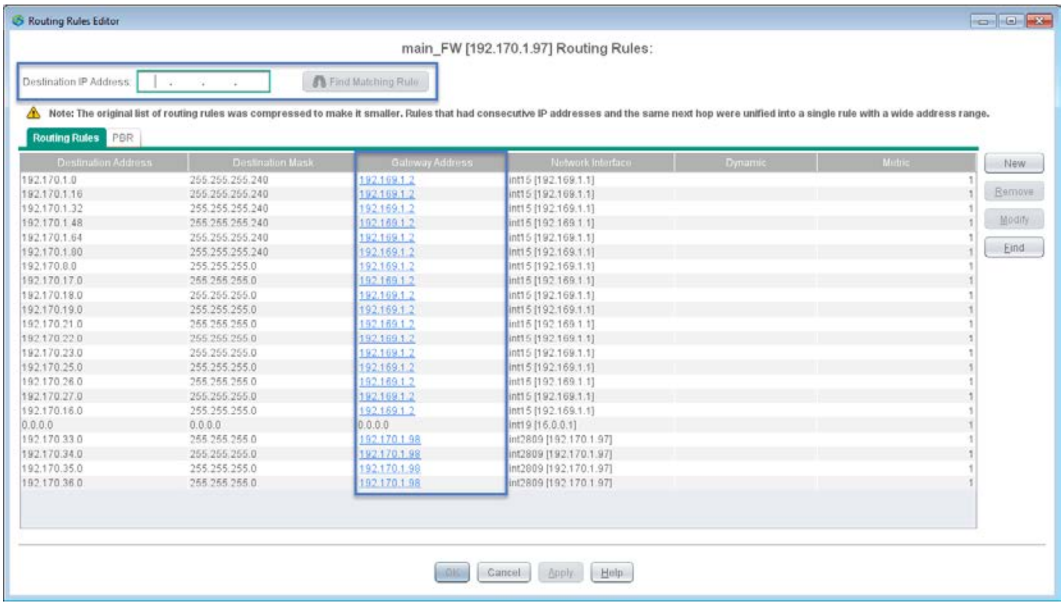
TROUBLESHOOTING MISSING DEVICES (ADVANCED)

Use the Routing Rules Editor to investigate and troubleshoot scenarios by manually tracing routing rules between devices to find missing or disconnected devices.

- The **Destination IP Address** search box in the editor enables you to search any destination address to find the routing rule it matches.

  The search checks the routing rule destination addresses of the device and displays the rule that matches the searched address. This is the calculation performed by routers.

- You can click the gateway address of the matching rule (that is, the next hop address) to open the routing rules for that gateway and continue the investigation.



main_FW [192.170.1.97] Routing Rules:

Destination IP Address: . . .

Note: The original list of routing rules was compressed to make it smaller. Rules that had consecutive IP addresses and the same next hop were unified into a single rule with a wide address range.

Destination Address	Destination Mask	Gateway Address	Network Interface	Dynamic	Metric
192.170.1.0	255.255.255.240	192.169.1.2	int15 [192.169.1.1]		1
192.170.1.16	255.255.255.240	192.169.1.2	int15 [192.169.1.1]		1
192.170.1.32	255.255.255.240	192.169.1.2	int15 [192.169.1.1]		1
192.170.1.48	255.255.255.240	192.169.1.2	int15 [192.169.1.1]		1
192.170.1.64	255.255.255.240	192.169.1.2	int15 [192.169.1.1]		1
192.170.1.80	255.255.255.240	192.169.1.2	int15 [192.169.1.1]		1
192.170.8.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.17.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.18.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.19.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.21.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.22.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.23.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.25.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.26.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.27.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
192.170.16.0	255.255.255.0	192.169.1.2	int15 [192.169.1.1]		1
0.0.0.0	0.0.0.0	0.0.0.0	int19 [16.0.0.1]		1
192.170.33.0	255.255.255.0	192.170.1.98	int2809 [192.170.1.97]		1
192.170.34.0	255.255.255.0	192.170.1.98	int2809 [192.170.1.97]		1
192.170.35.0	255.255.255.0	192.170.1.98	int2809 [192.170.1.97]		1
192.170.36.0	255.255.255.0	192.170.1.98	int2809 [192.170.1.97]		1

Chapter 25

Access Analyzer

This chapter describes how to set the properties of queries in Access Analyzer.

In this chapter

ACCESS ANALYZER QUERY FIELDS: VULNERABILITY CONTROL

The query fields for Access Analyzer when working with Skybox Vulnerability Control are described in the following table.

Field	Description
Source	
Scope	The source points for access analysis. Click the **Browse** button to define the source scope or IP address range. • For information about source and destination fields, see the Defining the source and the destination section in the Skybox Vulnerability Control User Guide.
Services	The services to use on the source assets to analyze access. • **NOT**: Analyze access on all services except those selected. **Note**: Use this field in special cases only—by default, TCP and UDP communication source ports are chosen at random.
Destination	
Sending To For information about using **Sending To** fields, see the Additional destination options topic in the Skybox Vulnerability Control User Guide.	
IP Ranges	The IP address ranges to use when sending packets. Use this field to limit the query to a set of IP addresses, even though the destination (or source) field might be a network or a location.
Services & Applications	The services and applications to use when sending packets to IP address ranges. • **NOT**: Analyze access on all service-application combinations except those selected. Use this field when packets are sent through a proxy server and only the proxy port is known.

Field	Description
Arriving At	
For information about using **Arriving At** fields, see the Additional destination options topic in the Skybox Vulnerability Control User Guide.	
Scope	The destination points for access analysis. Click the **Browse** button to define the destination scope or IP address range.
Services	The services to use to access the destination. • **NOT**: Analyze access on all services except those selected.
Filter By	
NAT	Specifies the NAT for the request: • **Source Nat**: Show only access results that involve source NAT (that is, the source of the query was translated) • **Destination Nat**: Show only access results that involve destination NAT (that is, the destination of the query was translated) • **No Source Nat**: Show only access results that do not involve source NAT (that is, the source of the query was not translated) • **No Destination Nat**: Show only access results that do not involve destination NAT (that is, the destination of the query was not translated) • **None**: Show all results (do not filter by NAT)
Advanced	
Access Rules	• **Use All**: Use all access rules encountered in the model. • **Ignore All Rules**: Ignore access and address translation rules. This option is useful for connectivity testing and model verification. • **Use Only NAT Rules**: Ignore access rules; use only address translation rules.
Routing Rules	• **Use All**: All routing rules. • **Ignore All Rules**: Ignore routing rules—route each packet through all available interfaces. This option is useful for connectivity testing and model verification. • **Ignore Dynamic Rules Only**: Use only static routing rules; route packets that do not match the static routing rules through all available interfaces. **Note**: This option has no effect on assets and gateways without routing rules. For such assets, packets are routed through all available interfaces.
Routes Per Service	The number of routes to analyze for each service. If the displayed route is incomplete—for example, it covers access from only some sources—increase this value to provide a more complete result. **Note**: Increasing the value of this property increases the analysis time for this query. **Note**: The default value is controlled by the `AccessAnalyzer_max_routes_for_service` property in `<Skybox_Home>\server\conf\sb_server.properties`

Field	Description
Simulate IP Spoofing During Analysis	Specifies whether to analyze access from any IP address (to simulate IP address spoofing).
Ignore Rules on Source	Specifies whether to analyze access as if the source assets permit *any* outbound traffic, regardless of the access and routing rules.
Show Source network in Destination	Specifies whether to include the **Source** networks in the Analysis Result pane.

Note: If you change the values of any query fields after analyzing a rule, reanalyze the rule for the changes to take effect.

For information about working with Access Analyzer, see the Access Analyzer chapter in the Skybox Vulnerability Control User Guide.

ACCESS ANALYZER QUERY FIELDS: FIREWALL ASSURANCE AND NETWORK ASSURANCE

The query fields for Access Analyzer when working with Skybox Firewall Assurance or Skybox Network Assurance are described in the following table.

Field	Description
Firewall	(Displayed if **Firewall Mode** is selected on the toolbar) The firewall on which to analyze access.
Source	
Scope	The source points for access analysis. Click the **Browse** button to define the source scope or IP address range. For information about source and destination fields: • If you are working with Skybox Firewall Assurance, see the Defining the source and the destination topic in the Skybox Firewall Assurance User Guide. • If you are working with Skybox Network Assurance, see the Defining the source and the destination topic in the Skybox Network Assurance User Guide.
Services	The services to use on the source assets to analyze access. • **NOT**: Analyze access on all services except those selected. **Note**: Use this field in special cases only—by default, TCP and UDP communication source ports are chosen at random.
Destination	
Sending To For information about using **Sending To** fields, see the Additional destination options topic in the Skybox Network Assurance User Guide.	
IP Ranges	The IP address ranges to use when sending packets. Use this field to limit the query to a set of IP addresses, even though the destination (or source) field might be: • (Skybox Network Assurance) A network or location

Field	Description
	• (Skybox Firewall Assurance) All the IP addresses behind a network interface
Services & Applications	The services and applications to use when sending packets to IP address ranges. • **NOT**: Analyze access on all service-application combinations except those selected. Use this field when packets are sent through a proxy server and only the proxy port is known.
Arriving At	
For information about using **Arriving At** fields, see the Additional destination options topic in the Skybox Network Assurance User Guide.	
Scope	The destination points for access analysis. Click the **Browse** button to define the destination scope or IP address range.
Services	The services to use to access the destination. • **NOT**: Analyze access on all services except those selected.
Filter By	
NAT	Specifies the NAT for the request: • **Source Nat**: Show only access results that involve source NAT (that is, the source of the query was translated) • **Destination Nat**: Show only access results that involve destination NAT (that is, the destination of the query was translated) • **No Source Nat**: Show only access results that do not involve source NAT (that is, the source of the query was not translated) • **No Destination Nat**: Show only access results that do not involve destination NAT (that is, the destination of the query was not translated) • **None**: Show all results (do not filter by NAT)
Advanced	
Access Rules	• **Use All**: Use all access rules in the model. • **Ignore All Rules**: Ignore access and address translation rules. This option is useful for connectivity testing and model verification. • **Use Only NAT Rules**: Ignore access rules; use only address translation rules.
Routing Rules	• **Use All**: Use all routing rules. • **Ignore All Rules**: Ignore routing rules—route each packet through all available interfaces. This option is useful for connectivity testing and model verification. • **Ignore Dynamic Rules Only**: Use only static routing rules; route packets that do not match the static routing rules through all available interfaces. **Note**: This option has no effect on assets and gateways without routing rules. For such assets, packets are routed through all available interfaces.

Field	Description
Routes Per Service	The number of routes to analyze for each service. If the displayed route is incomplete—for example, it covers access from only some sources—increase this value to provide a more complete result. **Note**: Increasing the value of this property increases the analysis time for this query. **Note**: The default value is controlled by the `AccessAnalyzer_max_routes_for_service` property in `<Skybox_Home>\server\conf\sb_server.properties`
Simulate IP Spoofing During Analysis	Specifies whether to analyze access from any IP address (to simulate IP address spoofing).
Ignore Rules on Source	Specifies whether to analyze access as if the source assets permit *any* outbound traffic, regardless of the access and routing rules.
Show Source network in Destination	Specifies whether to include the **Source** networks in the Analysis Result pane.

Note: If you change the values of any query fields after analyzing a rule, reanalyze the rule for the changes to take effect.

For information about working with Access Analyzer, see the Access Analyzer chapter in the Skybox Network Assurance User Guide.

Chapter 26

Network Map

This chapter describes how to set the properties of the Network Map.

For information about the Network Map:

- (Skybox Vulnerability Control) See the Network visualization (maps) section in the Skybox Vulnerability Control User Guide
- (Skybox Network Assurance) See the Network Map visualization topic in the Skybox Network Assurance User Guide

In this chapter

NETWORK MAP CONTROL PANEL

The options available in the control panel of the Network Map are described in the following table.

Button / Field	**Description**
(Basic)	These buttons and fields are always displayed.
Map	Specifies the map to display in the Map pane. If you made changes to the map, you can save the changes before the selected map is displayed.
Reload the maps	Prompts to save all unsaved maps, refreshes the map definitions from the Skybox Server, and reloads the selected map to the Map pane.
Help	Opens help for the Network Map.
Save current map	Saves the map (including any changes) with its original name. **Note**: This option is disabled for the default map.
Save current map as a new one	Saves the map (including any changes) with a new name.
Relayout	Redraws the map (excluding nodes that are hidden). When the map is redrawn, the optimized layout is recalculated, which might result in a better view of the map, especially if you have made changes to the model or map properties.

Button / Field	Description
Zoom to Fit	Fits all nodes of the map into the Map pane (excluding nodes that are hidden).
Display Filter Pane	Displays a small pane above the map that you use to filter the nodes that are displayed in the map. Note: Use **Ctrl-F** to display the filter pane, and the **Esc** key (in the **Show** field or in the white space of the Map pane) to close it.
Select Neighbor Nodes	If you select specific nodes in the map, adds the immediate neighbor nodes of the selected nodes to the selection.
Clear Current Selection	Clears the map so that no nodes are selected.
Highlight Neighbors	If you select a node in the map, all neighbors within the specified number of hops are highlighted in lighter colors. For example, a value of 1 means that immediate neighbors (only) are highlighted.
File	
Save current map	Saves the map (including any changes) with its original name.
Save current map as a new one	Saves the map (including any changes) with a new name. • For information about map properties, see Properties of single maps (on page 454).
Properties	Opens the Network Map Properties dialog box for editing the scope of the map.
Export	• Export image: Saves the visible portion of the map as a graphic file to the directory that you select in the Export dialog box. **Note**: You can change the resolution of the saved image in the Export dialog box for easier viewing outside Skybox. • Export to Visio: Exports the visible portion of the map as a Microsoft Visio VDX file.
New	Creates a map from the nodes that are visible in the Map pane.
Delete Map	Deletes the map from the Map pane and the Skybox database, and opens the default map.
View	
Zoom In	Increases the magnification of the map.
Zoom Out	Decreases the magnification of the map.
Zoom to Area	When selected, moving the mouse up and down controls the size of the display rather than moving the display up and down.
Display Locations	Specifies the location labels (if any) that are displayed in the map. Locations labels are not part of the map; you can drag them around the map.

Button/Field	Description
Display Map Groups	Specifies the Map Group labels (if any) that are displayed in the map. Map Group labels are not part of the map, you can drag them around the map.
Layout	
Relayout	Redraws the map (excluding nodes that are hidden). When the map is redrawn, the optimized layout is recalculated, which might result in a better view of the map, especially if you have made changes to the model or map properties.
Layout Properties...	Opens an advanced dialog box that for fine-tuning the display in the map window (see Layout properties (on page 456)).
Map Groups	
New...	Creates a Map Group from the nodes selected in the map.
Attach...	Attaches the nodes selected in the map to a Map Group.
Detach	Detaches the nodes selected in the map from a Map Group.
? Help	Opens help for Map Groups.
Highlight	The map groups to highlight.
Collapse All	Collapses all Map Groups. If there are any nested Map Groups, only the outermost group is displayed.
Expand All	Expands all Map Groups so that all the groups at all levels are displayed.
Auto Grouping...	Opens the Auto Grouping dialog box for this map.
Highlight	
Network Type	Highlights in tan all networks of the specified type (Perimeter Cloud, regular network, or secure VPN) in the map.
Location	Highlights in turquoise all nodes related to the selected location.
Zone	Highlights in tan all networks and devices that belong to the selected zone type. **Note**: Zones are defined and used in Skybox Network Assurance.
Validation	• Has Missing Hops: Highlights in gray each device that has a missing next hop according to its routing table. • Empty Networks: Highlights in gray all networks that contain no non-gateway assets.
Scope	Highlights in peach all nodes within the selected scope.

Button / Field	Description
Show only highlighted	Hides most nodes in the map, so that only the highlighted nodes and their neighbors to the selected degree are displayed.
Select Highlighted	Selects all the highlighted nodes in the map and their neighbors to the selected degree.
Clear	Resets all the *Highlight* fields to **None** and clears all highlights in the map.

NETWORK MAP FILTER TOOLBAR

The options available in the filter pane are described in the following table.

To open the pane, click ▽ in the control panel or press **Ctrl-F**; to close the pane click ✕ in the pane or press the **Esc** key.

Button / Field	Description
Visible	(Read-only) Specifies how many nodes to display in the map and the total number of nodes in the map. **Note**: When a Map Group is collapsed, it is counted as a single node. For nested Map Groups, only the outermost group is counted.
Show	Enables you to select entities in the map by typing in the (full or partial) name or IP address of the desired nodes. Wildcards and regular expression syntaxes are permitted. For additional information, see: • The Navigating the Network Map (Network Assurance) topic in the Skybox Network Assurance User Guide • The Navigating the Network Map (Vulnerability Control) topic in the Skybox Vulnerability Control User Guide
Show Only Highlighted	Hides most nodes in the map, so that only the highlighted nodes and their neighbors to the selected degree are displayed.
Regular Mouse Mode	Specifies whether, when you select nodes in the map, the selected nodes and their neighbors are highlighted.
Focus	Specifies whether, when you select nodes in the map, only the selected nodes and their neighbors (within a radius of **Neighbors Distance**) are displayed. All other nodes in the map are hidden.
Extend	Specifies whether, when you select nodes in the map, the map expands (if parts of it are hidden) by adding all neighbors of the selected node up to a radius of **Neighbors Distance**.
Neighbors Distance	The radius of the neighborhood to use for Focus and Expand modes.
Display All Nodes	Restores all hidden nodes to the map but keeps the magnification (so some nodes might not be displayed).

Button/Field	Description
✘ Close Filter Pane	Hides the filter pane.

PROPERTIES OF SINGLE MAPS

With the Network Map open, click (in the File pane) to open the Network Map Properties dialog box.

Note: The properties in this dialog box refer to the map that is displayed in the Map pane.

The map properties are described in the following table.

Property	Description
General	
Name	A name for the map.
Properties	
Scope	The assets and container entities to include in the Network Map. See Map scope (on page 454).
Expand scope's neighborhood	Specifies whether to include the closest neighborhood of the selected scope in the map.
Auto group nodes with the same neighbors	
Networks	Specifies whether to group all networks that have the same neighbors. These are usually either clusters or networks at the perimeter of the model that are connected to the same device. If selected, the networks are displayed as a single entity with a grouping symbol around them.
Gateways	Specifies whether to group all gateway entities of the same type that have the same neighbors. These are usually clusters of firewalls or routers used for redundancy. If selected, the gateways are displayed as a single entity with a grouping symbol around them.
Auto group mesh	
VPN Mesh	A topology in which all participant gateways in a group are directly interconnected via a point to point VPN.
Tunnel Mesh	A topology in which all participant gateways in a group are directly interconnected via a point to point tunnel.

Map scope

Property	Description
Basic tab	
Scope	
Asset Name	A string for filtering asset names.
Network Scope	The assets and container entities to include in the Business Asset Group.

Property	Description
Automatically add networks	If locations are chosen in the Network Scope, automatically add networks that are assigned or created under the locations to the Network Map scope.
Exclude Network Scope	Assets and container entities that match the **Network Scope** but are not to be included in the Business Asset Group.
Asset Attributes	
Asset Type	Only include assets of these types.
Operating Systems	Only include assets with these operating systems.
Has Patches	The assets to include: • **All**: Do not filter based on whether the asset has patches • **Yes**: Only assets that have patches • **No**: Only assets that have no patches
Has Packages	The assets to include: • **All**: Do not filter based on whether the asset has packages • **Yes**: Only assets that have packages • **No**: Only assets that have no packages
Service	Only include assets with these services.
Service Created Since	Only include assets with services created since this date.
Products	Only include assets with these products.
Advanced tab	
Business Attributes	
Owner	Only include assets with these owners.
Email	Only include assets with these email addresses.
Business Function	Only include assets with these business functions.
Site	Only include assets from these sites.
Tag	Only include assets with this tag.
Comment	Only include assets that include this string in their comments.
Custom Attributes	Only include asset with these custom attributes.
Scan Time	
Filtering Mode	Specifies whether to include scanned or unscanned assets.
Scan Time	Depending on the value of **Filtering Mode**: • When the assets were most recently scanned • How long since the assets were scanned Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time

Property	Description
Creation & Modification	
Created Since	Only include assets created in the specified time frame. Select **Custom** to define a date range by: • Specifying the earliest creation date • Specifying the earliest creation time relative to the current time
Created By	Only include assets created by a user whose name contains the specified string.
Modified Since	Only assets modified in the specified time frame are included. Select **Custom** to define a date range by: • Specifying the earliest modification date for • Specifying the earliest modification time relative to the current time
Modified By	Only include assets modified by a user whose name contains the specified string.
Model Validation tab	
Model Validation	
Model Validation Attributes	Only include assets that include the specified model validation attributes.
Validation Severity	Only include assets that have the selected validation severity.
Model Maintenance	
Locked By User	Specifies whether only assets that have a field locked by the user are included. (A lockable field is automatically locked if the user modifies its value.)
About to be deleted	Only include assets that are about to be deleted.
Dynamic Routing	Only include assets that use dynamic routing.
VPN Attributes	
Participate in VPN	Only include assets that participate in a VPN group.
VPN Original Text	The original text of any comment found in the VPN configuration. Use the characters **?** and ***** for standard pattern matching.

LAYOUT PROPERTIES

The layout of the Network Map is based on a simulation of interacting forces. Nodes in the Network Map represent networks and gateways, with networks represented by blue dots and gateways represented by icons. Edges in the Network Map represent the connection between the gateways and the networks in which they are included; each edge represents a network interface of a gateway.

The default layout values are optimum for most medium to large models. In some cases, tuning the layout properties can achieve a better layout.

Tuning the layout

If tuning is required, a change to 1 or 2 of the properties is usually sufficient to produce a better layout. The process is mainly trial and error; here are some tips:

- If the model is relatively small or has low complexity (for example, the demo model or when presenting a single location), a smaller **DragCoefficient** (for example, 0.003) or a smaller **DefaultSpringLength** (for example, 60) might create a better layout.
- Decreasing the **DefaultSpringLength** can improve distinction between areas of nodes in the layout.
- Decreasing the **GravitationalConstant** (a stronger repelling force) usually leads to a more spread-out model; you might need to increase the **SpringCoefficient** to balance the antigravity forces.

How the simulation works

Three types of forces are simulated in the Network Map:

- N-body force: A force between nodes, similar to gravity or electrostatic force. By default, each node repels the other nodes according to its distance from them.
- Spring force: Each edge acts as a spring. It applies force on the nodes it connects if the length of the edge is greater or smaller than the default (resting) spring length.
- Drag force: Resistance to change in the node positions due to other forces, similar to air resistance or fluid viscosity.

Each force type has properties that control its behavior, as described in the following table.

Property	**Description**
NBodyForce	
GravitationalConstant	The magnitude of the gravity or antigravity. Nodes attract each other if this value is positive and repel each other if it is negative.
Distance	The distance within which 2 nodes interact. If -1, the value is modeled as infinite.
BarnesHutTheta	Specifies when gravity (or antigravity) is computed between a node and a group of relatively distant nodes, rather than between the node and each of the group members. This property determines that when all the group members fit into a viewing angle from the node that is smaller than theta, the ‘mass’ of the group is aggregated, and the gravity force is computed between the node and the group. A small theta leads to somewhat more accurate gravity computation, but a longer calculation time.
DragForce	

Property	**Description**
DragCoefficient	Specifies the magnitude of the drag force.
SpringForce	
SpringCoefficient	The spring tension coefficient (*k* in Hooke’s law).
DefaultSpringLength	The spring resting length (length at equilibrium position).
Layout invisible nodes	Specifies whether the layout operation considers all nodes (including hidden nodes).

Part IV: Entities

This part describes the entities used in the model.

Chapter 27

Model entities

You can access all model entities from:

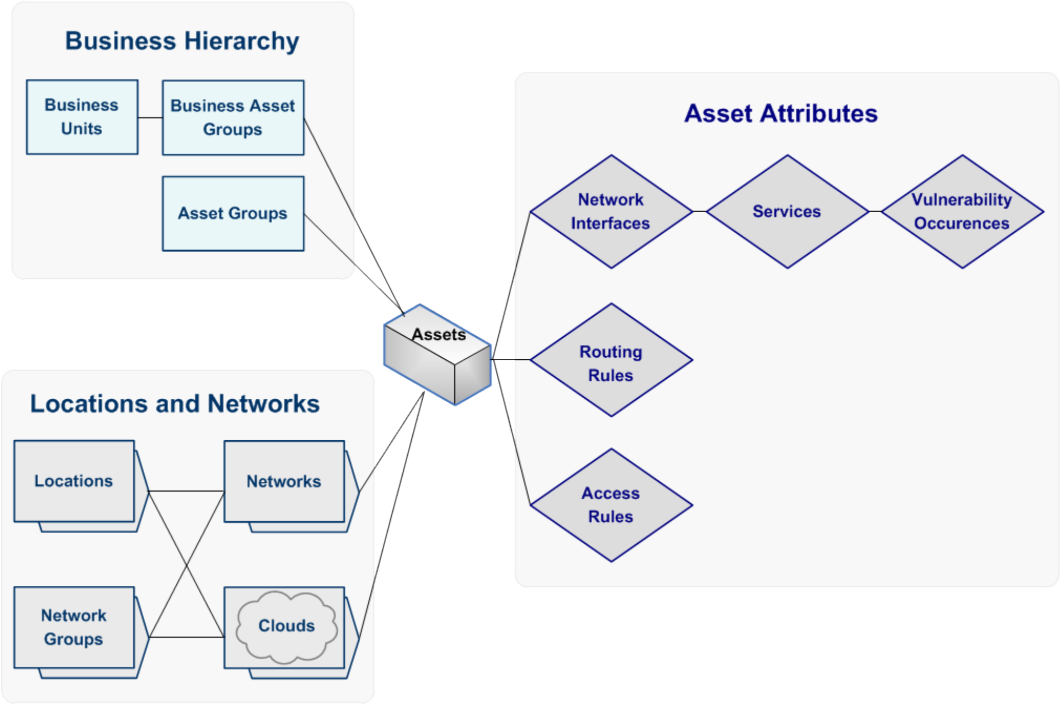
- The Model tree
- The Network Map

You can access specific types of model entities from other locations in Skybox. For example, you can access network devices from the Network Assurance workspace.

In this chapter

ENTITY RELATIONSHIPS

The main entity types in the model are assets and networks.



- You can group assets into Business Asset Groups and asset groups (logical groupings).
- Assets can be part of networks or clouds (topological groupings).
- Networks and clouds can be parts of locations.
- You can group networks into Network Groups for zoning purposes when working with Skybox Network Assurance.

LOCKING ENTITY PROPERTIES

Some fields (properties) of model entities are lockable:

- 🔒 (**Locked**): The data in the field was entered or changed by a user; it is not updated by the system.
- 🔓 (**Unlocked**): The data in the field is the system-collected (or default) value.

Click 🔒 to set the field data back to the system-collected (or default) value. The icon toggles to 🔓.

The main reason for changing the value of a field of a model entity is because scans or online collections return an incorrect value for the field; locked fields are not updated by the system.

ASSETS

An asset is a device or system in your organization’s network. Skybox supports the following asset types:

: Asset (used for non-network-device assets that do not belong to another category)

: Server

: Printer

: Firewall

: Load Balancer

: Wireless Device

: Mobile Device

: Workstation

: Router

: IPS

: Proxy

: Switch

: Network Device (used for network-device assets that do not belong to another category)

Note: You can use the Find dialog box to help you to find an asset.

The properties of assets are described in the following table.

Property	**Description**
Asset Name	The name of the asset.
Other Names	(Read-only) A name that Skybox generates internally.
Type	The asset type. The list of asset types precedes this table.
Network Interfaces	A list of network interfaces associated with the asset. The network interface properties are described in Network interfaces (on page 476).
Status	The status of the asset. • **Up**: Only an asset that is **Up** can be attacked. • **Down**: An asset that is **Down** cannot be attacked but is visible for analyses. This overrides the interface status (that is, if the status of the asset is **Down**, interfaces with status **Up** are considered down). • **Not Found** • **Unknown**
General tab	
Firewall Type	This field is enabled only if **ACL Enabled** = **Yes**. The type selected sets the access rule order. For **Custom** types only, you can specify the rule chains and their order; click the **Browse** button to open the ACL Management dialog box (see page 464).
Forwarding	Specifies whether forwarding is enabled (that is, whether the asset can forward packets from one interface to another). **Note**: **Unknown** is equivalent to **No**. • For information about specifying routing rules, see Managing routing rules (on page 440).
ACL Enabled	Specifies whether access rules are enabled on the asset. **Note**: **Unknown** is equivalent to **No**. • For information about enabling access rules, see Using

Property	**Description**
	the Access Control List Editor (on page 433).
Proxy ARP	IP address ranges for which the asset is to act as a proxy for ARP requests.
IPS Enabled	This field is enabled only if **ACL Enabled** = **Yes**. Specifies whether the asset is IPS enabled. **Note**: **Unknown** is equivalent to **No**.
Patches	A list of applicable patches for the asset.
Dynamic Routing	Specifies whether the asset supports dynamic routing (see Routing rule properties (on page 441)).
Layer 2	Specifies whether the asset is an L2 asset.
Virtual Routing Enabled	Specifies whether virtual routing is enabled on the asset.
Do Not Outdate	Specifies whether the asset (including its network interfaces, services, and vulnerability occurrences) is ignored by **Model – Outdated Removal** tasks. These tasks mark entities that were not updated for a specific period as **Down** and later delete them from the model. **Note**: Manually created assets (and assets created by iXML import) are usually not updated on a regular basis so should not be outdated.
Platform & OS tab	
OS	The operating system of the asset. The available operating systems depend on the value of **OS Vendor**.
OS Vendor	The operating system vendor of the asset.
OS Version	The version of the operating system.
Platform	The platform used for the asset. The available platforms depend on the value of **Platform Vendor**.
Platform Version	The version of the platform.
Platform Vendor	The platform vendor of the asset.
Business Attributes tab	
Owner	The owner of the asset.
Business Function	The business function of the asset.
Email	The email address of the asset owner.
Site	The site where the asset is located.
Tag	A unique ID for the asset (for example, a serial number from an inventory management system), which can help you to identify assets when adding or updating assets.
User Comments	A statement describing the asset.

ACL Management dialog box

The ACL Management dialog box displays the order in which the access chains of a firewall are applied. (To add access rules to a rule chain or to change the order of the access rules in the chain, see Using the Access Control List Editor (on page 433).)

You can access the ACL Management dialog box from the Properties dialog box of any asset or network device that is access-rule-enabled; click the **Browse** button next to the **Firewall Type** field.

The dialog box has several variations, depending on the device for which you are specifying the order of access rules.

For all devices except Custom firewalls, the ACL Management dialog box displays:

- The Available Rule Chains pane: The available rule chains for the device, in alphabetic order.
- The Inbound Order pane: The order in which the rule chains are applied for inbound traffic.
- The Outbound Order pane: The order in which the rule chains are applied for outbound traffic. For load balancers, the Outbound Order pane is empty because load balancers have no outbound traffic.
- (Check Point FireWall-1 only) VPN Mode: **Simplified** or **Traditional**.

The available rule chains for non-custom devices and the order in which the chains are applied cannot be changed. If you work with custom firewalls, you can create additional rule chains and change the order of the chains.

ACL Management dialog box: Custom firewall

Skybox supports 3 custom firewall types with different rule chains. Each custom firewall can define a firewall type that is not directly supported by Skybox.

The Available Rule Chains pane lists, in alphabetic order, the rule chains that are available for use by the Inbound and Outbound panes.

Note: Adding a rule chain to the Available Rule Chains pane of the ACL Management dialog box makes the rule chain available for use by the Inbound and Outbound panes, but it is not added to the list of rule chains used for the firewall.

The Inbound and Outbound panes list the rule chains that are used for the selected firewall and specify their order.

To add a rule chain to the ACL Management dialog box

1. In the Available Rule Chains pane of the ACL Management dialog box, click **New**.
2. In the New Rule Chain dialog box, in the **Rule Chain Label** field, type the name of a rule chain.

   The rule chain name can contain any ASCII characters, including spaces.

   Note: Rule chain names are case-sensitive.
3. Click **OK**.

ASSET GROUPS

An asset group (▦) is a logical container that you can use to group and filter assets.

The properties of asset groups are described in the following table.

Property	Description
Name	The name of the asset group.
Group Type	The type of the asset group.
Assets	The assets that belong to the asset group.
Member Dependency	• **Default**: Security loss of any type (confidentiality, integrity, or availability) on a group member implies the same security loss on the asset group; integrity loss on a group member also implies an availability and confidentiality security loss on the asset group. • **Simple**: Security loss of any type (confidentiality, integrity, or availability) on a group member implies the same security loss on the asset group. • **None**: Used (if the **Default** and **Simple** options of describing dependency are not sufficient) to state explicitly how a security loss on every asset group member affects the asset group (see the Adding dependency rules and Explicit dependency rules topics in the Skybox Vulnerability Control User Guide).
Owner	The owner of the asset group.
User Comments	A statement describing the asset group.

BUSINESS ASSET GROUPS

A Business Asset Group (▦) is a group of assets that serve a common business purpose. Each Business Asset Group has an associated set of damage (Business Impact) and dependency rules that define the impact of security loss on that Business Asset Group.

Business Asset Groups are relevant only to Skybox Vulnerability Control for attack simulation.

The Business Asset Group dialog box has 3 tabs:

- Properties (on page 465)
- Business Impacts (on page 468)
- Regulations (on page 469)

General Business Asset Group properties

The main properties of Business Asset Groups are described in the following table.

Property	Description
Name	The name of the Business Asset Group.
Members	The members of the Business Asset Group. See Business Asset Group members (on page 466).
Member	Specifies how the security of a Business Asset Group

Property	Description
Dependency	depends on the security of its member assets: • **Default**: Security loss of any type (confidentiality, integrity, or availability) on a Business Asset Group member implies the same type of security loss on the Business Asset Group; integrity loss on a Business Asset Group member implies an availability and confidentiality security loss on the Business Asset Group. • **Simple**: Security loss of any type (confidentiality, integrity, or availability) on a Business Asset Group member implies the same type of security loss on the Business Asset Group. • **None**: Used if the **Default** and **Simple** options of describing dependency are not sufficient and you want to state explicitly how a security loss on each of the Business Asset Group members affects the Business Asset Group (see the Adding dependency rules and Explicit dependency rules topics in the Skybox Vulnerability Control User Guide).
Threat Origins	Specifies whether to consider the listed Threat Origins when examining attacks on the Business Asset Group. • Ignore pane: Threat Origins to ignore when examining attacks on the Business Asset Group. • Analyze for Risk pane: Threat Origins that are not Detached (that is, Threat Origins to consider when examining attacks on the Business Asset Group). Use < and > to move selected Threat Origins from one pane to the other. Alternatively, in the Threat Origin Properties dialog box, you can define the Business Asset Groups to be considered by the Threat Origin (see the Adding Threat Origins section in the Skybox Vulnerability Control User Guide). A Threat Origin with a grayed-out icon next to its name is disabled.
Owner	The owner of the Business Asset Group.
User Comments	A statement describing the Business Asset Group.

Business Asset Group members

The properties that Skybox uses to determine the assets in the model to include in a Business Asset Group are described in the following table.

Property	Description
Basic tab	
Scope	
Asset Name	A string for filtering asset names.
Network Scope	The assets and container entities to include in the Business Asset Group.
Automatically add networks	If locations are chosen in the Network Scope, automatically add networks that are assigned or created

Property	Description
	under the locations to the Network Map scope.
Exclude Network Scope	Assets and container entities that match the **Network Scope** but are not to be included in the Business Asset Group.
Asset Attributes	
Asset Type	Only include assets of these types.
Operating Systems	Only include assets with these operating systems.
Features	
Has Patches	The assets to include: • **All**: Do not filter based on whether the asset has patches • **Yes**: Only assets that have patches • **No**: Only assets that have no patches
Has Packages	The assets to include: • **All**: Do not filter based on whether the asset has packages • **Yes**: Only assets that have packages • **No**: Only assets that have no packages
Service	Only include assets with these services.
Service Created Since	Only include assets with services created since this date.
Products	Only include assets with these products.
Advanced tab	
Business Attributes	
Owner	Only include assets with these owners.
Email	Only include assets with these email addresses.
Business Function	Only include assets with these business functions.
Site	Only include assets from these sites.
Tag	Only include assets with this tag.
Comment	Only include assets that include this string in their comments.
Custom Attributes	Only include asset with these custom attributes.
Scan Time	
Filtering Mode	Specifies whether to include scanned or unscanned assets.
Scan Time	Depending on the value of **Filtering Mode**: • When the assets were most recently scanned • How long since the assets were scanned Select **Custom** to define a date range by: • Specifying starting and ending dates • Specifying starting and ending times relative to the current time

Property	Description
Creation & Modification	
Created Since	Only include assets created in the specified time frame. Select **Custom** to define a date range by: • Specifying the earliest creation date • Specifying the earliest creation time relative to the current time
Created By	Only include assets created by a user whose name contains the specified string.
Modified Since	Only assets modified in the specified time frame are included. Select **Custom** to define a date range by: • Specifying the earliest modification date for • Specifying the earliest modification time relative to the current time
Modified By	Only include assets modified by a user whose name contains the specified string.
Model Validation tab	
Model Validation	
Model Validation Attributes	Only include assets that include the specified model validation attributes.
Validation Severity	Only include assets that have the selected validation severity.
Model Maintenance	
Locked By User	Specifies whether only assets that have a field locked by the user are included. (A lockable field is automatically locked if the user modifies its value.)
About to be deleted	Only include assets that are about to be deleted.
Dynamic Routing	Only include assets that use dynamic routing.
VPN Attributes	
Participate in VPN	Only include assets that participate in a VPN group.
VPN Original Text	The original text of any comment found in the VPN configuration. Use the characters **?** and ***** for standard pattern matching.

Business Asset Groups: Business Impact properties

A Business Impact is a rule that specifies the damage to your organization as a result of an attack (that is, security loss) on a Business Asset Group. Business Impacts are defined in the Skybox Admin window. For information about Business Impacts, see the Business Impacts and Regulations topic in the Skybox Vulnerability Control User Guide.

In the **Business Impacts** tab of the Business Asset Groups dialog box, you specify the Business Impacts to associate with the selected Business Asset Group (expressing the effects of a security loss).

The **Business Impacts** properties of Business Asset Groups are described in the following table.

Property	**Description**
(Attach / Detach check box)	Specifies whether the selected Business Impact is attached to the Business Asset Group.
Name	(Read-only) The name of the Business Impact.
Damage	Damage associated with the Business Impact. **Note**: You can specify **Damage** as either a monetary value or a level between Very High and Very Low.
Loss Type	(Read-only) Loss type associated with the Business Impact: C (confidentiality), I (integrity), A (availability)

Business Asset Groups: Regulation properties

A Regulation is a Business Impact that specifies the impact to a Business Asset Group (that is, the damage to your organization) that results if your organization is not in compliance with a security-related regulation. For information about Regulations, see the Business Impacts and Regulations topic in the Skybox Vulnerability Control User Guide.

The **Regulations** properties of Business Asset Groups are described in the following table.

Property	**Description**
(Attach / Detach check box)	Specifies whether the selected Regulation is attached to the Business Asset Group.
Name	(Read-only) The name of the Regulation.
Damage	Damage associated with the Regulation. **Note**: You can specify **Damage** as either a monetary value or a level between Very High and Very Low.
Loss Type	(Read-only) Loss type associated with the Regulation: C (confidentiality), I (integrity), A (availability)

BUSINESS UNITS

Business Units () enable you to group Business Asset Groups for management purposes.

The properties of Business Units are described in the following table.

Property	**Description**
Name	The name of the Business Unit.
Members	The members of the Business Unit: • Business Units under the direct responsibility of the Business Unit (for creating a hierarchy of Business Units) • Business Asset Groups under the direct responsibility of the Business Unit • Locations that include the assets that support the

Property	Description
	operation of the Business Unit Specify locations only if you need vulnerability occurrence counts for the Business Units.
Owner	The owner of the Business Unit.
User Comments	A statement describing the Business Unit.

Business Units are relevant only to Skybox Vulnerability Control. For additional information, see the Business Units section in the Skybox Vulnerability Control User Guide.

CLOUDS

Clouds are networks (or groups of networks) that are not completely modeled. For example, the internet, partner organizations, or sensitive areas in your own organization that cannot be fully modeled.

Skybox supports the following cloud types:

- ☁: Perimeter Cloud: Represents missing networks at the edges of the model
- ☁: Connecting Cloud: Represents missing networks between 2 entities in the model

For additional information about clouds:

- (Skybox Vulnerability Control) See the Clouds section in the Skybox Vulnerability Control User Guide.
- (Skybox Network Assurance) See the Clouds section in the Skybox Network Assurance User Guide.

Perimeter Clouds

Perimeter Clouds (☁) are networks or groups of networks at the edges of the model that are not completely modeled (for example, the internet or a partner organization).

The properties of Perimeter Clouds are described in the following table.

Property	Description
Name	The name of the cloud.
Associate Assets Dynamically	Specifies whether Skybox attempts to match assets to the cloud when new assets are imported that do not belong to any network, and when Model Completion and Validation tasks (see page 318) are run.
Location Path	(Read-only) The hierarchical path of the cloud in the Model tree.
Do Not Outdate	Specifies whether the cloud (including its assets and their network interfaces, services, and vulnerability occurrences) is ignored by **Model – Outdated Removal** tasks. These tasks mark entities that were not updated for a specific period as **Down** and later delete them from the model. **Note**: Manually created clouds (and clouds created by iXML import) are usually not updated on a regular basis

Property	Description
	so should not be outdated.
Owner	The owner of the cloud.
Zone Type	This field is displayed only for Skybox Network Assurance. The zone type to which the cloud belongs. A *zone type* is a way of classifying entities into different zones for use in the Access Policy.
Network Address	
IP Address	The IP address of the cloud.
Mask	This field is displayed only for IPv4 clouds. The netmask of the cloud.
CIDR	This field is displayed only for IPv6 clouds. The CIDR of the cloud.
Discovery Method	Specifies how the cloud was discovered.
Cloud Addresses	
Include	A list of IP address ranges to include in the scope of the cloud. There are 3 ways to define the IP addresses to include: • **Automatic (routing based)**: Skybox calculates the IP addresses to include based on the addresses behind the network interfaces (see page 478) that are connected to the cloud. You can configure Model – Completion and Validation (see page 318) tasks to recalculate these addresses. • **User Defined**: Lists the **Automatic** addresses, enabling you to edit them. These addresses are not recalculated automatically. • **Any**: All IP addresses.
Exclude	A list of IP address ranges to be excluded from the scope of the cloud. Click **Private** to exclude IANA reserved addresses: • 10.0.0.0-10.255.255.255 • 172.16.0.0-172.31.255.255 • 192.168.0.0-192.168.255.255 If you are configuring an internet cloud, exclude reserved addresses. If you are configuring a public cloud, exclude public IP addresses that your organization uses.
Routable from Cloud	
Include	A list of IP address ranges to use as destination addresses from the cloud. Skybox uses these destination IP address ranges for all queries starting at the cloud in attack simulation and in Access Analyzer. There are 2 ways to define the IP addresses to include: • **User Defined**: Lists the **Automatic** IP addresses, enabling you to edit them. These addresses are not recalculated automatically.

Property	Description
	- **Any**: All IP addresses.
Exclude	A list of IP address ranges to be excluded from the destination address ranges of the cloud. Click **Private** to exclude IANA reserved addresses: - 10.0.0.0-10.255.255.255 - 172.16.0.0-172.31.255.255 - 192.168.0.0-192.168.255.255 If you are configuring an internet cloud, exclude reserved addresses. If you are configuring a public cloud, exclude public IP addresses that your organization uses.
Comments	Additional information about the cloud.

Connecting Clouds

Connecting Clouds (☁) represent networks or groups of networks that are missing in the model (for example, sensitive areas in your organization that cannot be fully modeled); Connecting Clouds connect entities that are not at the edges of your organization's network.

The properties of Connecting Clouds are described in the following table.

Property	Description
Name	The name of the cloud.
Associate Assets Dynamically	Specifies whether Skybox attempts to match assets to the cloud when new assets are imported that do not belong to any network in the model, and when Model Completion and Validation tasks (see page 318) are run.
Location Path	(Read-only) The hierarchical path of the cloud in the Model tree.
Owner	The owner of the cloud.
Zone Type	This field is displayed only for Skybox Network Assurance. The zone type to which the cloud belongs. A *zone type* is a way of classifying entities into different zones for use in the Access Policy.
Connections	
Connection	A connection is an entity to which the cloud is connected. Each connection consists of a network, gateway, and network interface to which the cloud is connected. To add another connection to a cloud, click **Add**.
Cloud Addresses	
Include	A list of IP address ranges to include in the scope of the cloud. There are 3 ways to define the IP addresses to include: - **Automatic (routing based)**: Skybox calculates the IP addresses to include based on the addresses behind the network interfaces (see page 478) that are connected to the cloud. These addresses can be recalculated when you run a Model – Completion and Validation (see page 318) task.

Property	Description
	- **User Defined**: Lists the **Automatic (routing based)** addresses, enabling you to edit them. These addresses are not recalculated automatically. - **Any**: All IP addresses.
Exclude	A list of IP address ranges to be excluded from the scope of the cloud. Click **Private** to exclude IANA reserved addresses: - 10.0.0.0-10.255.255.255 - 172.16.0.0-172.31.255.255 - 192.168.0.0-192.168.255.255 If you are configuring an internet cloud, exclude reserved addresses. If you are configuring a public cloud, exclude public IP addresses used by your organization.
Routable from Cloud	
Include	A list of IP address ranges to use as destination addresses from the cloud. Skybox uses these address ranges for all queries starting at the cloud for attack simulation and in Access Analyzer. There are 2 ways to define the IP addresses to include: - **User Defined**: Lists the IP addresses, enabling you to edit them. These addresses are not recalculated automatically. - **Any**: All IP addresses.
Exclude	A list of IP address ranges to be excluded from the destination address ranges of the cloud. Click **Private** to exclude IANA reserved addresses: - 10.0.0.0-10.255.255.255 - 172.16.0.0-172.31.255.255 - 192.168.0.0-192.168.255.255 If you are configuring an internet cloud, exclude reserved addresses. If you are configuring a public cloud, exclude public IP addresses used by your organization.
Advanced	
Forwarding Cloud	Specifies whether forwarding is enabled (that is, whether the cloud can forward packets from one interface to another).
ACL Enabled	Specifies whether access rules are enabled on the cloud.
Firewall Type	(For ACL-enabled clouds only) The type selected sets the access rule order. For **Custom** types only, you can specify the rule chains and their order; click the **Browse** button to open the ACL Management dialog box (see page 464).
Comments	Additional information about the cloud.

LOCATIONS

Locations () reflect the physical or geographical organization of your network (for example, a site, a building, or a lab inside a building). Locations contain other locations and networks.

The properties of locations are described in the following table.

Property	Description
Location Name	The name of the location.
Members	The members of the location (other locations and networks).
Location Path	(Read-only) The hierarchical path of the location in the model tree.
Owner	The owner of the location.
User Comments	A statement describing the location.

For additional information about locations:

- (Skybox Vulnerability Control) See the Locations topic in the Skybox Vulnerability Control User Guide
- (Skybox Network Assurance) See the Locations topic in the Skybox Network Assurance User Guide

NETWORKS

A network has an IP address and netmask. Skybox supports the following network types:

: Regular

: Tunnel

: Link

: Secure VPN

: Serial Link

Note: In the Network Map, tunnels and VPN tunnels are represented as colored lines linking their 2 endpoints.

For information about modeling networks in Skybox, see the Building the network layer section in the Skybox Vulnerability Control User Guide.

The properties of networks are described in the following tables. The properties common to all network types are described in the 1st table.

Property	Description
General	
Name	The name of the network.
Type	The type of the network.
IP Address	The IP address of the network.
Mask	This field is displayed only for IPv4 networks. The netmask of the network.

Property	**Description**
CIDR	This field is displayed only for IPv6 networks. The CIDR of the network.
Location Path	(Read-only) The hierarchical path of the network in the Model tree.
Owner	The owner of the network.
Zone Type	This field is displayed only for Skybox Network Assurance. The zone type to which the network belongs. A *zone type* is a way of classifying networks into different zones for use in the Access Policy.
Do Not Outdate	Specifies whether the network (including its assets and their network interfaces, services, and vulnerability occurrences) is ignored by **Model – Outdated Removal** tasks. These tasks mark entities that were not updated for a specific period as **Down** and later delete them from the model. **Note**: Manually created networks (and networks created by iXML import) are usually not updated on a regular basis so should not be outdated.
Comments	Additional information about the network.
Description	(Read-only) A description of the network.

The additional properties that are displayed in the Tunnel Properties pane for **Tunnel**, **Secure VPN**, and **Serial Link** networks are described in the following table.

Property	**Description**
Type	This field is disabled for **Serial Link** networks. The network type. • For **Tunnel** networks, select **OTHER** or **GRE** • For **Secure VPN**s, select **Tunnel** or **Transport**
Endpoint 1	An endpoint of the tunnel network or secure VPN.
Endpoint 2	The other endpoint of the tunnel network or secure VPN.
Display as Cloud in Network Map	**Secure VPN**s can be displayed as clouds in the Network Map.

NETWORK GROUPS

A network group (🖧) is a logical container that you can use to group and filter networks. Network groups are especially useful when working with Skybox Network Assurance. By marking network groups (instead of individual networks) as zones to check for Access Compliance, you can understand the model better and improve performance.

The properties of network groups are described in the following table.

Property	**Description**
Group Name	The name of the network group.
Members	The networks that belong to the network group.

Property	Description
Owner	The owner of the network group.
Zone Type	This field is displayed only for Skybox Network Assurance. The zone type to which the network group belongs. A *zone type* is a way of classifying network groups or individual networks into different zones for use in the Access Policy.
User Comments	A statement describing the network group.

For information about how Skybox uses network groups to build the model, see the Network groups topic in the Skybox Network Assurance User Guide.

NETWORK INTERFACES

Network interfaces () enable an asset to communicate with other assets and networks. To view the network interfaces of an asset, select the asset and then click the **Network Interfaces** tab in the Details pane.

Note: If necessary, click ⊞ to view the **Network Interfaces** tab.

The properties of network interfaces are described in the following table.

Property	Description
General	
Name	The name of the network interface.
Type	The type of the network interface.
Proxy ARP Behavior	The ARP state of the interface: • **Static**: The interface acts as a proxy for ARP requests for IP address ranges. • **Any Address** • **Disabled**: Proxy ARP is disabled on the interface. • **Unknown**: The ARP state of the interface is unknown. In Skybox, proxy ARP is not simulated on the interface.
IP Address	The IP address of the network interface.
Subnet Mask	This field is displayed only for IPv4 interfaces. The subnet mask of the network interface.
CIDR	This field is displayed only for IPv6 interfaces. The CIDR of the network interface.
MAC Address	The MAC address of the network interface. (For **Ethernet** networks only.)
Status	The status of the network interface.
Network	The network or cloud to which the network interface is attached. **Note**: In some cases, the automatic attachment does not work correctly, and the network interface is not attached to the correct network (for example, if there is an error in the netmask of the network interface in the configuration file). You can select a different network in this field and then

Property	Description
	click the **Lock** icon to lock the interface to the network. Additional offline file imports or online collections of firewall data do not change the association.
Primary IP Address	Specifies whether the value in the **IP Address** field is the primary IP address for the network interface. For information about how Skybox selects the primary IP address when collecting or importing device configuration data, see Primary IP address (on page 478).
Layer 2	Specifies whether the interface is an L2 network interface.
Default Gateway	Specifies whether the network interface is the default gateway for its asset.
Addresses Behind Interface	Each network interface on a gateway device communicates with a set of networks. The IP addresses of these networks are the interface's *ABI* (addresses behind interface). **Note**: By default, the fields related to ABI are updated when Skybox imports the device routing table. If you changed the value of the ABI fields manually for a network interface, these fields are **Locked** (🔒) and their values are not updated by the import. - For information about ABIs, see Addresses behind network interfaces (on page 478).
Default Gateway / Unknown Addresses	Specifies whether the network interface is the default interface or the interface leading to the internet. Data that is not routed through any other network interface on the asset is routed through this network interface.
Specific Addresses	The IP addresses behind the interface (that is, the ABI for the interface). These are the IP addresses of the networks with which the network interface communicates. - **Addresses**: IP address ranges behind the network interface - **Exclude**: IP addresses to be excluded from the address ranges in the **Addresses** field
Zone tab	Skybox Firewall Assurance and Skybox Network Assurance only. Information about the zone to which the network interface is attached. (Zones are used with Access Policies.)
Zone Type	The type of the zone to which the network interface is attached.
Zone Name	The name of the zone to which the network interface is attached.
Comments tab	Additional information about the network interface.
Description tab	(Read-only) A description of the network interface. This field is filled for network interfaces found during collection of the asset configuration. Usually, this field contains the interface comment or description specified in the original asset configuration.

Addresses behind network interfaces

Each network interface on a gateway device communicates with a set of networks. The IP addresses of these networks are the interface's *addresses behind interface* (ABI).

These IP addresses are assumed to be distinct on each interface—an IP address that is behind one network interface of a firewall is not also behind another network interface on the same firewall.

When firewalls are imported into the model, Skybox ascertains the ABI for each network interface in the firewall based on the routing table and other information in the imported firewall configuration. Skybox uses ABIs for:

- Skybox Firewall Assurance: Analyzing access between network interfaces of the firewall
- Skybox Network Assurance and Skybox Vulnerability Control: Calculating (routing-based) IP address ranges for clouds:
  - For Perimeter Clouds, the cloud IP addresses are based on the ABI of the network interface that connects the cloud to the model.
  - For Connecting Clouds, the cloud IP addresses are calculated by taking the intersection of the ABIs for all the network interfaces connected to the cloud minus all the addresses of all networks to which the cloud is connected.

For information about using ABIs in Skybox Firewall Assurance, see the Addresses behind network interfaces topic in the Skybox Firewall Assurance User Guide.

Primary IP address

This section lists the criteria for setting the primary IP address of a collected or imported device.

Collection tasks

The collection IP address is set as the primary IP address.

Import tasks

The management IP address is set as the primary IP address.

If there are multiple management IP addresses, the lowest IP address is set.

Cisco PIX firewalls

The primary IP address is set according to the interface with the highest security level.

SERVICES

Services (⚙) on assets are found by vulnerability scanners or by network scans, or added from an iXML file built from an asset repository.

The properties of services are described in the following table.

Property	Description
Vendor	The vendor of the service.

Property	Description
Service Type	(Read-only) The service type of the service, taken from the Skybox database.
Product	The product used for the service. The available products depend on the value of **Vendor**.
Protocol	The protocol used by the service.
Version	The version of the product. The available products depend on the value of **Product**.
Port #	The port number of the service if **Protocol** = **TCP** or **Protocol** = **UDP**.
Protocol #	The protocol number of the service if **Protocol** = **IP**.
Program #	The program number of the service if **Protocol** = **RPC**.
CPE	The CPE definition of the service.
Status	The status of the service.
Network Interfaces	The network interfaces for the service.
Description	(Read-only) A description of the service, taken from the Skybox database.
Banner	A free text field containing data that helps Skybox to identify details of the product running the service. The text is usually the initial service output that is displayed when connecting to the service.
User Comments	A statement describing the service.

THREAT ORIGINS

A Threat Origin (🎩) is a location inside or outside your network that constitutes a threat (that is, a location where an attacker might be found). All Threat Origins are user-defined.

You can create Threat Origin in the Model workspace; use the **Threat Origin Categories** > **All Threat Origins** node, see the Adding Threat Origins chapter in the Skybox Vulnerability Control User Guide.

The properties of Threat Origins are described in the following table.

Property	Description
General tab	
Name	The name of the Threat Origin
Threat Location	The locations from which the Threat Origin can attack the network.
Categories	Categories of the Threat Origin to use for grouping purposes. **Note**: Although assigning categories is not mandatory, we recommend that you assign categories to each Threat Origin. This enables presentation of a more complete picture when viewing risk analyses and reports. In particular, it enables viewing the risk and exposure of

Property	Description
	vulnerability occurrences according to each of the specified categories.
Attacker Skill	The presumed skill level of the attacker launching the attack. The skill level is a factor when analyzing risk from the Threat Origin.
Likelihood to Attack	The presumed likelihood that the Threat Origin will launch an attack on the network.
Advanced tab	
Attacker Privilege	The presumed privilege of the attacker on the device from which the attack is initiated. Many vulnerability occurrences cannot be exploited without a specific privilege level.
Cloud Source Addresses	The range of source IP addresses to use in cloud attacks: • **All**: Use all cloud addresses as sources for attacks. • **Wide source addresses**: Use only attacks that are possible from wide address ranges of the cloud. • **Specific addresses**: Use only attacks that are possible from specific addresses of the cloud. For additional information, see the Using clouds as Threat Origins topic in the Skybox Vulnerability Control User Guide.
Lower Likelihood for Attacks from Specific Addresses	Specifies whether to assign a lower risk value from attacks that originate from specific IP addresses inside clouds.
Business Asset Groups	
Ignore	Business Asset Groups for which you are not interested in the effects of attacks from the Threat Origin.
Analyze for Risk	Business Asset Groups for which you want to view the effect of attacks from the Threat Origin.

For additional information about Threat Origins, see the Defining Threat Origins topic in the Skybox Vulnerability Control User Guide.

VULNERABILITY OCCURRENCES

Vulnerability occurrences () on assets are found by vulnerability scanners.

The properties of vulnerability occurrences are described in the following table.

Property	Description
ID / Title	The Vulnerability Definition of the vulnerability occurrence.
Service	(Read-only) The service that the vulnerability occurrence affects.
Commonality	(Read-only) States how frequently attackers exploit the Vulnerability Definition of the vulnerability occurrence.
CVE	(Read-only) The identity of the Vulnerability Definition of the vulnerability occurrence in the CVE dictionary.

Property	Description
Severity	The severity of the Vulnerability Definition of the vulnerability occurrence.
Detection Reliability	The level of detection reliability of the vulnerability occurrence. The detection reliability value is imported from the scanner that reported the vulnerability occurrence and specifies the certainty with which the scanner determines that the vulnerability occurrence exists. • **Low**: The scanner is not sure that the vulnerability occurrence exists • **Medium**: The scanner is fairly sure that the vulnerability occurrence exists
Status	The status of the vulnerability occurrence.
Exposure	(Read-only) States how exposed the vulnerability occurrence is to attacks from the Threat Origins. For example, a *directly* exposed vulnerability occurrence can be reached in a single step from the attacking Threat Origin.
Status Explanation	(Read-only) The cause of the **Status**.
Description	(Read-only) A description of the vulnerability occurrence, taken from the Skybox model.
User Comments	A statement describing the vulnerability occurrence.

The additional properties of vulnerability occurrences that are accessible from the Details pane are described in the following table. Many properties are taken from the Vulnerability Definition.

Tab	Description
General	General information about the vulnerability occurrence.
CVSS	The CVSS base score and temporal score of the Vulnerability Definition, and metrics on which the scores are based.
Asset	Information about the asset on which the vulnerability occurrence is located.
Service	Information about the service on which the vulnerability occurrence is found.
Risk Profile	Information about the risk of the vulnerability occurrence.
External Catalogs	A list of the names and IDs of the Vulnerability Definition as they appear in the external vulnerability databases that are supported by Skybox. **Note**: Not every Vulnerability Definition in the Skybox Vulnerability Dictionary is listed in all external databases supported by Skybox.
External URLs	A list of links to URLs containing information about the Vulnerability Definition.
Affected Platforms	The platforms affected by the vulnerability occurrence.
Tickets	A list of Skybox tickets opened on the vulnerability

Tab	Description
	occurrence.
Solutions	A list of known solutions that close the vulnerability occurrence.
Scanner Info	If the vulnerability occurrence was imported by a scanner, this tab contains additional information from the scanner.
Comments	User comments about the vulnerability occurrence.
History	History of the vulnerability occurrence, including creation time and most recent modification time.