Skybox Installation and Administration Guide

Additional Servers .................................................................................. 35

Multi-tiered servers for Change Manager ................................................... 36

Autonomous collection units .................................................................... 37

Skybox connectivity requirements ............................................................ 40

Updating Skybox..................................................................................... 41
  Updating Skybox ............................................................................... 41
  Skybox update file ............................................................................. 42
  Downloading the update file ............................................................... 42
  Preparing to update .......................................................................... 42
  Updating the Server and local components ........................................... 43
  Updating remote components ............................................................. 44
  Updating multi-tiered servers ............................................................. 44

Migrating the Collector infrastructure ....................................................... 46

Skybox licenses ..................................................................................... 48
  Invalid licenses.................................................................................. 48
  Node-count violations........................................................................ 49

Uninstalling Skybox ................................................................................ 50

Product security..................................................................................... 51
  Communication and certificates ........................................................ 51
  Encryption ........................................................................................ 54
  Using FIPS mode ............................................................................. 55
  Limiting login attempts ................................................................... 55
  Security check: Last login message .................................................. 55
  Customizable login warning messages .............................................. 55
  User session timeout ........................................................................ 56

Part II: Administration ............................................................................ 57

User management .................................................................................. 58
  User roles ......................................................................................... 58
  Managing users and user groups ....................................................... 65
  Working with external authentication systems .................................... 72
  Managing users externally using LDAP ............................................. 74
  Changing the password for database clients ...................................... 76

Backup and restore ................................................................................ 78
  Backup and restore scenarios ........................................................... 78
  About the model .............................................................................. 78
  Backing up the model ..................................................................... 79
  Fast backup ..................................................................................... 81
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skybox Web Client</td>
<td>131</td>
</tr>
<tr>
<td>Working with IPv6</td>
<td>132</td>
</tr>
<tr>
<td>Configuring Skybox using the properties files</td>
<td>134</td>
</tr>
<tr>
<td>Server properties file</td>
<td>134</td>
</tr>
<tr>
<td>Collector properties file</td>
<td>134</td>
</tr>
<tr>
<td>Manager properties file</td>
<td>134</td>
</tr>
<tr>
<td>Common properties file</td>
<td>134</td>
</tr>
<tr>
<td>Port properties file</td>
<td>135</td>
</tr>
<tr>
<td>Managing multiple Appliances</td>
<td>136</td>
</tr>
<tr>
<td>Viewing Appliance information</td>
<td>136</td>
</tr>
<tr>
<td>Disabling tasks on the secondary Appliance Server</td>
<td>136</td>
</tr>
<tr>
<td>Dictionary updates</td>
<td>138</td>
</tr>
<tr>
<td>About Vulnerability Dictionary updates</td>
<td>138</td>
</tr>
<tr>
<td>Updating the Skybox Vulnerability Dictionary</td>
<td>139</td>
</tr>
<tr>
<td>Skybox logs</td>
<td>140</td>
</tr>
<tr>
<td>Activity log</td>
<td>140</td>
</tr>
<tr>
<td>Audit log</td>
<td>140</td>
</tr>
<tr>
<td>Event logging</td>
<td>140</td>
</tr>
<tr>
<td>Log files</td>
<td>141</td>
</tr>
<tr>
<td>Activity and audit log messages</td>
<td>147</td>
</tr>
</tbody>
</table>
Preface

Intended audience

The Skybox Installation and Administration Guide includes:

› Comprehensive instructions for installation and migration, including general system and installation information and detailed procedures
› Topics of interest to system administrators, including user management, product security, and ticket setup and configuration

The intended audience of the Installation and Administration Guide is:

› Personnel responsible for installing and configuring Skybox components
› All Skybox system administrators

Related documentation

The following documentation is available for Skybox:

› Skybox Reference Guide
› Skybox Developer Guide
› Skybox Release Notes

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

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 (on page 145)).
Chapter 1

Introduction

This chapter explains the Skybox platform and its basic architecture.

In this chapter

Skybox platform ................................................................. 8
Skybox architecture ............................................................ 10
Platform technology ............................................................. 11

Skybox platform

Skybox® Security arms security professionals with the broadest platform of solutions for security operations, analytics, and reporting. By integrating with more than 100 networking and security technologies organizations, the Skybox Security Suite merges data silos into a dynamic network model of your organization’s attack surface, giving comprehensive visibility of public, private, and hybrid IT environments. Skybox provides the context needed for informed action, combining attack vector analytics and threat-centric vulnerability intelligence to continuously assess vulnerabilities in your environment and correlate them with exploits in the wild. This makes the accurate prioritization and mitigation of imminent threats a systematic process, decreasing the attack surface and enabling swift response to exposures that truly put your organization at risk.
Skybox arms security leaders with a comprehensive cybersecurity management platform to address the security challenges of large, complex networks. The Skybox Security Suite breaks down data silos to build a dynamic network model that gives complete visibility of an organization’s attack surface and the context needed for informed action across physical, multi-cloud, and industrial networks. We leverage data by integrating with 120 security technologies, using analytics, automation, and advanced threat intelligence from the Skybox Research Lab to continuously analyze vulnerabilities in your environment and correlate them with exploits in the wild. This makes the prioritization and mitigation of imminent threats an efficient and systematic process, decreasing the attack surface and enabling swift response to exposures that truly put your organization at risk. Our award-winning solutions automate as much as 90 percent of manual processes and are used by the world’s most security-conscious enterprises and government agencies, including Forbes Global 2000 companies. For additional information visit the Skybox website

visit the Skybox website
The Skybox Security Suite includes:

- **Skybox Vulnerability Control**: Powers threat-centric vulnerability management by correlating intelligence on vulnerabilities in your environment, the surrounding network and security controls and exploits in the wild focusing remediation on your most critical threats.

- **Skybox Threat Manager**: Consolidates threat intelligence sources and prioritizes advisories in the context of your attack surface, automatically analyzing the potential impact of a threat and providing remediation guidance.

- **Skybox Firewall Assurance**: Brings multi-vendor firewall environments into a single view and continuously monitors policy compliance, optimizes firewall rule sets and finds attack vectors that others miss.

- **Skybox Network Assurance**: Analyzes hybrid environments end to end across physical, virtual and cloud – even operational technology – networks, illuminating complex security zones, access paths and policy compliance violations.

- **Skybox Change Manager**: Ends risky changes with network-aware planning and risk assessments, making firewall changes a secure, consistent process with customizable workflows and automation.

- **Skybox Horizon**: Visualizes an organization’s unique attack surface and indicators of exposure (IOEs), giving threat-centric insight to critical risks, visibility across an entire organization or down to a single access rule and metrics to track risk reduction over time.

The products share common services, including modeling, simulation, analytics, reporting, and automated workflow management.

### Skybox architecture

The Skybox platform includes all Skybox products, so there is a single installer for all products. Your license controls the products that are available.

The platform uses a 3-tiered architecture with data collectors, a centralized server, and a user interface (the Manager). Skybox can be easily scaled to suit the complexity and the size of any infrastructure.

Skybox includes:

- **Skybox Server**: Running on a dedicated server, the Skybox Server merges all collected data, builds the Skybox model, and maintains an up-to-date snapshot of the network environment. The Skybox Server is the central coordination point for all data elements in the model, the analytic engine, and the report generator.

- **Skybox Collector**: Deployed in various network segments, Skybox Collectors discover network topology and collect configuration data from network devices, vulnerability scanners, and network management frameworks.

- **Skybox Manager**: A Java client application, Skybox Manager is the management interface to the Skybox Server. There is a Manager for Skybox Firewall Assurance and Skybox Network Assurance, and a separate Manager for Skybox Vulnerability Control and Skybox Threat Manager. Multiple instances of Skybox Manager can run concurrently across the network.
Note: Skybox Web UI, Skybox Horizon, and Skybox Change Manager are web-based; they do not require installation of the Manager.

Skybox Vulnerability Dictionary: A central repository of definitions and profiles for Vulnerability Definitions, threats, worms, and network security policies. With a dedicated team of security professionals, Skybox continually monitors a wide array of security bulletins, alerts, and publications to provide clients with timely updates to the dictionaries.

The following figure shows the basic architecture of Skybox.

Platform technology

The following figure shows the relationships between the software components in Skybox.
Part I: Installation

This part provides comprehensive instructions for installation and migration, including general system and installation information and detailed procedures.
Installing Skybox

This chapter provides an overview of Skybox installation.

In this chapter

Installation overview ........................................................... 13
Installation environment comparison ..................................... 13
Downloading installation files ............................................. 14

INSTALLATION OVERVIEW

There are different types of Skybox platform installation, depending on:

- The component or components that you need to install
- Where you are installing—on a Skybox Appliance, in a virtual environment, or on a standard computer

Various installation scenarios are described in the following table, with links to instructions or additional information.

<table>
<thead>
<tr>
<th>Component</th>
<th>Where / why you want to install it</th>
<th>Instructions or additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager (UI) only</td>
<td>Your organization is already working with Skybox and you need to work with it also</td>
<td>Manager installation (on page 16)</td>
</tr>
<tr>
<td>Server</td>
<td>For organization or enterprise deployment</td>
<td>Server installation (on page 18)</td>
</tr>
<tr>
<td>All components</td>
<td>In trial situations, or as an auditor who must run Skybox on a laptop</td>
<td>Installing the Server on Windows (on page 20)</td>
</tr>
<tr>
<td>Collector only</td>
<td>After the Server is set up and you need another Collector for off-loading or for a segmented network</td>
<td>Collector installation (on page 31)</td>
</tr>
</tbody>
</table>

Installation environment comparison (on page 13) shows the benefits of each installation environment.

INSTALLATION ENVIRONMENT COMPARISON

The benefits of each installation environment are listed in the following table.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Physical Appliance</th>
<th>Virtual Appliance</th>
<th>Windows Installer</th>
<th>Linux Installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skybox High Availability (active/passive)</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Syslog facility for Rule Usage Analysis and log-based change tracking</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>SNMP monitoring of physical machine components</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>SNMP monitoring of Skybox processes and OS components</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Secured (hardened) via iptables</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Webadmin utility for managing system configuration including network interfaces, DNS, NTP, date/time, system mode, LDAP, RADIUS, SSH, Skybox services, and syslog</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Built-in Python and Perl (including packages) for Skybox plug-in connector architecture</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Collectors that must reside on a Windows platform:</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>• Microsoft WSUS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Active Directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Retina 4.9 (higher versions are OK for Linux also)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux libraries</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>x</td>
</tr>
<tr>
<td>Collectors that must reside on a Linux platform:</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>• Blue Coat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• McAfee Enterprise</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• A10 Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco ACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco CSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Citrix NetScaler</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• F5 BIG-IP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Radware Alteon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Radware AppDirector</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HP ProCurve</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skybox facilities for OS update</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**DOWNLOADING INSTALLATION FILES**

Access to the installation files is always available at http://downloads.skyboxsecurity.com/files/Installers/Skybox_View/<major version>/<minor version>/
For example,

A text file containing the MD5 checksum is in the same folder.

To verify that the installation file has not been corrupted or tampered with
1 Run `md5sum` from the directory to which you downloaded the installation file.
2 Check that the value you receive matches the value in the checksum file in the downloads folder.

Note: The checksum file contains checksums for both Linux and Windows downloads.
Chapter 3

Manager installation

This chapter explains how to install Skybox Manager by itself.

In this chapter

Installing Skybox Manager ........................................................... 16
Manager system requirements...................................................... 16

INSTALLING SKYBOX MANAGER

Note: Skybox Manager runs on most Microsoft Windows operating systems. For details, see Manager system requirements (on page 16).

Installing Skybox Manager requires administrator privileges.

To install Skybox Manager

1 Run the installation file (SkyboxManager-<version#>-<build>.exe).
2 Follow the directions in the wizard.

Note: Installation under <Drive>:\Program Files (or any other path containing a space) is not supported.

Post installation notes

▷ The Manager is configured to communicates with the server over 8443/TCP. If there is a firewall between the Manager and the Server, access on this port must be explicitly permitted.
▷ The user running the Manager must have Modify permissions for the directory where the Manager is installed.

MANAGER SYSTEM REQUIREMENTS

Skybox Manager is a Java client application that connects to the Skybox Server (through port 8443).

You can install multiple Managers on a single computer; this is useful when connecting to Servers of different versions.

Operating system

The following operating systems are supported for the Manager:

▷ Windows 7
▷ Windows 10 (64bit only)
▷ Windows Server 2012
**Browser**
The following browsers are supported for the Manager:

- Microsoft Internet Explorer 9 and higher
  
  Note: Microsoft Edge is not supported.

- Google Chrome
- Mozilla Firefox
- Safari (for Skybox Horizon)

**Hardware**
The hardware requirements for the Manager are listed in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel i3 or</td>
<td>Intel i5 or</td>
</tr>
<tr>
<td></td>
<td>equivalent</td>
<td>equivalent</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Available disk</td>
<td>1 GB</td>
<td>2 GB</td>
</tr>
<tr>
<td>space</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4

Server installation

There are several possible Server installation scenarios; each scenario requires a different installation process.

In this chapter

Installation instructions for different environments .................. 18
Installation workflow ........................................................... 18
Server system requirements ................................................ 19
Installing the Server on Windows .......................................... 20
Silent installation .............................................................. 20
Installing the Server on Linux ............................................... 24
Starting and stopping components via the Windows system tray 25
Post-installation steps ......................................................... 25
Elasticsearch and Skybox..................................................... 29

INSTALLATION INSTRUCTIONS FOR DIFFERENT ENVIRONMENTS

<table>
<thead>
<tr>
<th>If you are installing in this environment...</th>
<th>Refer to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skybox Appliance</td>
<td>Skybox 5500/6000/7000/8000 Appliance Quick Start Guide</td>
</tr>
<tr>
<td>Skybox Virtual Appliance (ISO installed in a VMware environment)</td>
<td>Skybox Virtual Appliance Quick Start Guide</td>
</tr>
</tbody>
</table>
| Windows for corporate environment           | • Installing the Server on Windows (on page 20) (via a wizard)  
  • Silent installation (on page 20) (via a script; full installation or only Collector) |
| Windows all-in-1: For a trial or as an auditor using a laptop | Installing the Server on Windows (on page 20) |
| Linux                                       | Installing the Server on Linux (on page 24) |
| FIPS                                        | Silent installation (on page 20) and Using FIPS mode (on page 55) |

INSTALLATION WORKFLOW

The general workflow for installing the Server is:
1 Check that the machine on which you are installing meets the system requirements (see page 19).

2 Follow the installation instructions that are described in:
   • (Windows) Installing the Server on Windows (on page 20)
   • (Linux) Installing the Server on Linux (on page 24)
   • Silent installation (on page 20) (without user intervention)

3 Perform any necessary post-installation steps (see page 25).

Note: If Skybox is already installed, you can download an update package from the Skybox update management server and install it (see Updating Skybox (on page 41)).

SERVER SYSTEM REQUIREMENTS

Install the Skybox Server on a server-class machine. The size and complexity of your network might require a powerful server with a multiprocessor and a large amount of memory. For very large deployments, you might need multiple Skybox Servers (each running on a separate server). The Manager and Collector are usually installed with the Server, but additional Managers and Collectors might be required.

The Skybox Server communicates through ports 8443 (between Server and Manager) and 9443 (between Server and Collector). We recommend that you permit communication through these ports only.

Installing multiple Servers

Install each Skybox Server on a separate machine. If you do install 2 Servers on the same machine, change the ports used by 1 of them to prevent port collision (see Installing multiple components on a single host (on page 26)).

Operating system

The operating systems supported for the Skybox Server are listed in the following table.

Note: The Server must run on a 64bit operating system.

<table>
<thead>
<tr>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
</tr>
<tr>
<td>Windows 10</td>
</tr>
<tr>
<td>Windows Server 2012</td>
</tr>
<tr>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6 (for existing installations only)</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7</td>
</tr>
<tr>
<td>CentOS 6 (for existing installations only)</td>
</tr>
<tr>
<td>CentOS 7</td>
</tr>
</tbody>
</table>

Hardware

Server hardware requirements are listed in the following table. If you need help, contact Skybox technical support.
<table>
<thead>
<tr>
<th>Item</th>
<th>Standard Deployment</th>
<th>Large Deployment (Over 250 Firewalls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>8 cores</td>
<td>16 cores</td>
</tr>
<tr>
<td>RAM</td>
<td>32 GB</td>
<td>128 GB</td>
</tr>
<tr>
<td>Available disk space</td>
<td>500 GB</td>
<td>1 TB</td>
</tr>
</tbody>
</table>

**INSTALLING THE SERVER ON WINDOWS**

Installing and running the Skybox Server on Windows requires administrator privileges. When you install the Server, the Manager and Collector are installed on the same machine by default.

Before installing the Server, check that the machine on which you are installing meets the **system requirements** (see page 19).

*To install Skybox*

1. Run the installation file (`SkyboxInstaller-<version#>-<build>.exe`).
2. Follow the directions in the wizard.
   - Mandatory options are listed in the following table. In all other places, either use the default option or make the necessary change.
   - At the end of the installation, Skybox is launched. To log in requires a valid Skybox license file.
3. Navigate to the location where you stored the Skybox license file.

   *Note: If you have a licensing problem, you cannot log in until it is resolved. Contact [Skybox Support](#) for assistance.*

<table>
<thead>
<tr>
<th>Page Action</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Install Folder</td>
<td>Specify the installation directory.</td>
</tr>
<tr>
<td><strong>Note:</strong> Installation under <code>&lt;Drive&gt;:\Program Files (or any other path containing a space)</code> is not supported.</td>
<td></td>
</tr>
<tr>
<td>If another (previous) version of Skybox is installed, do not install to the same directory.</td>
<td></td>
</tr>
<tr>
<td>Preferences</td>
<td>By default, the Server and Collector run as services. If the target platform is used for running Skybox only occasionally, you can choose to run them as batch processes.</td>
</tr>
</tbody>
</table>

**SILENT INSTALLATION**

Use silent installation to:

- Install Skybox on Linux machines
- Install Skybox on Windows without user intervention
- Install Skybox on either Linux or Windows in FIPS mode
Note: Only install Skybox in FIPS mode if required to do so (see Using FIPS mode (on page 55)).

Before running a silent installation, ensure that:

› You have administrator privileges
› If you previously installed Skybox (any version), you specify a different directory for this installation

To prepare for silent installation

1 Download the installation file (on page 14) or locate it on the file system if it was already downloaded:
   • (Windows) SkyboxInstaller-<version#>-<build>.exe
   • (Linux) SkyboxInstaller-<version#>-<build>.bin
2 Copy the file to your computer.
3 Select a properties file from the file system or from an email if it was sent to you:
   • installer.properties: For full installation (all 3 components)
   • installer-collector.properties: For Collector installation; contains properties required for Collector installation only
   If no such file exists, create a properties file (see page 21).
4 Copy the properties file to the directory on your computer that contains the installation program (see step 1).
5 (Collector-only installation) Rename the copied installer properties file (installer-collector.properties) to installer.properties
6 If necessary, customize the properties file (see page 21) for your installation.

To run a silent installation

› Run the installation program:
   • (Windows) Execute the command: SkyboxInstaller-<version#>-<build>.exe -f installer.properties
   • (Linux) Execute the command: ./SkyboxInstaller-<version#>-<build>.bin -f installer.properties

Note: During silent installation, the file that is required for silent uninstallation is created.

Properties file for silent installation

The properties in installer.properties that are used for a full installation are described in the following table. For silent installation of the Collector, the file contains a subset of these properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLER_UI</td>
<td>Use the default value (silent)</td>
</tr>
<tr>
<td>SB_SERVER_HOST</td>
<td>Server host IP address</td>
</tr>
<tr>
<td></td>
<td>If the Server and Manager are on the same machine, use</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USER_INSTALL_DIR</td>
<td>The directory into which to install Skybox. The default is c:\Skybox. <strong>Note:</strong> For Windows installations, change the value to C:\Program Files\Skybox</td>
</tr>
</tbody>
</table>
| CHOSEN_INSTALL_SET   | The set of Skybox components to install  
• (Default) **Server** *(Full)*: Install all components: Server, Manager, and Collector  
• Collector: **Install only the Collector** |
| SB_LICENSE_FILE       | The Skybox license file name. The default name is license.xml. **This property is used only if you are installing the Server.**  
**Note:** Do not change the value of this property (the file name) or the Server cannot start. |
| SB_PATH_OF_LICENSE_FILE | The directory-level path to the license file. There is no default value.  
**Note:** If you do not provide a license file now, add the license file manually (after the installation) to <Skybox_Home>\server\conf |
| SB_FIPS140_MODE       | Specifies whether to install in approved (FIPS) mode:  
• 1: Yes  
• 0: No (default) |
| SB_SERVER_SERVICE     | If you are installing the Server, specifies whether to install it as a service:  
• 1: Yes (default)  
• 0: No |
| SB_COLLECTOR_SERVICE  | If you are installing the Collector, specifies whether to install it as a service:  
• 1: Yes (default)  
• 0: No |
| SB_SERVER_SERVICE_START | If you are installing the Server as a service, specifies whether to start it after installation:  
• 1: Yes  
• 0: No (default) |
| SB_COLLECTOR_SERVICE_START | If you are installing the Collector as a service, specifies whether to start it after installation:  
• 1: Yes  
• 0: No (default) |
| SB_SERVER_MAIL        | Mail server name or IP address for sending reports and alerts.  
There is no default value.  
**Note:** This property is used only if you are installing the Server. |
| SB_MAILADDRESS        | Mail server name or IP address for sending **Admin** email  
The default address is skybox_admin@skyboxsecurity.com |
### Property Description

This property is used only if you are installing the Server.

**Note:** This information can be added later using the Manager.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB_MANAGER_ACROBAT</td>
<td>Specifies whether to install Adobe Reader on the Manager machine:</td>
</tr>
<tr>
<td></td>
<td>- 1: Yes</td>
</tr>
<tr>
<td></td>
<td>- 0: No (default)</td>
</tr>
<tr>
<td></td>
<td>This property is used only if you are installing the Manager.</td>
</tr>
<tr>
<td>USER_SHORTCUTS</td>
<td>(Windows only) Location of the user shortcut</td>
</tr>
<tr>
<td></td>
<td>The default location is:</td>
</tr>
<tr>
<td></td>
<td>C:\Documents and Settings\All Users\Start Menu\Programs\Skybox</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> By default, this property is commented out—there is no user shortcut.</td>
</tr>
<tr>
<td>SHORTCUT_NAME</td>
<td>(Windows only) The name of the user shortcut</td>
</tr>
<tr>
<td></td>
<td>The default name is <code>skyboxview</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> By default, this property is commented out—there is no user shortcut.</td>
</tr>
<tr>
<td>SB_INSTALL_NEW</td>
<td>Specifies whether to perform a new installation:</td>
</tr>
<tr>
<td></td>
<td>- 1: Yes (default)</td>
</tr>
<tr>
<td></td>
<td>- 0: No</td>
</tr>
<tr>
<td></td>
<td>Do not change this value.</td>
</tr>
<tr>
<td>SB_INSTALL_UPGRADE</td>
<td>Do not change this value.</td>
</tr>
<tr>
<td>SB_PREV_HOME_DIR</td>
<td>Do not change this value.</td>
</tr>
</tbody>
</table>

### Example of installer.properties

```
INSTALLER_UI=silent
SB_SERVER_HOST=localhost
USER_INSTALL_DIR=c:\Skybox
# -- Manager, Collector, Server(Full)
CHOSEN_INSTALL_SET=Server(Full)
# -- License file name and location
SB_LICENSE_FILE=license.xml
SB_FIPS140_MODE=0
SB_SERVER_SERVICE=1
SB_COLLECTOR_SERVICE=1
SB_SERVER_SERVICE_START=0
SB_COLLECTORSERVICE_START=0
SB_SERVER_MAIL=
SB_MAIL_ADDRESS=skybox_admin@skyboxsecurity.com
SB_MANAGER_ACROBAT=0
SB_INSTALL_NEW=1
SB_INSTALL_UPGRADE=0
SB_PREV_HOME_DIR=/opt/Skybox
```
INSTALLING THE SERVER ON LINUX

Before installing Skybox

Before installing the Skybox Server, you must:

1. Be the root user
2. Install CentOS 7 (see page 24)
3. Install required packages (see page 25)
4. Harden platforms according to your hardening policy
5. Know the location of the Skybox license file

Note: If you do not have a license file, you can complete the installation without it; the 1st time that you log in to Skybox Manager, you are asked for the location of the license. (If you have a licensing problem, you cannot complete the login until it is resolved. Contact Skybox Support for assistance.)

Installation

You install Skybox on Linux silently (see page 20).

Users

The following users are set up during the installation of Linux and Skybox:

- root: Created by Linux installation
- %user_name%: During installation, you must give a non-root user access to the Server
- skyboxview: Created by Skybox installation

Linux (CentOS 7) installation

The topics in this section explain how to install CentOS 7 to work with Skybox Appliance.

Initial setup

To download and install CentOS 7

1. Download the operating system:
   a. Go to [http://isoredirect.centos.org/centos/7/isos/x86_64/](http://isoredirect.centos.org/centos/7/isos/x86_64/)
   b. Select the nearest mirror site for downloading the CentOS ISO file.
   c. Download the most recent full version of the ISO file
      - The file is approximately 4 GB and has DVD in its name.

2. Install CentOS with the following parameters:
   - Language + Keyboard: US English
   - Software selection:
     - Base Environment: Server with GUI
     - Add-Ons for selected Environment: Java platform, KDE
   - Installation destination (Partitions):
Installing packages

After installing Linux and before installing Skybox, you must install additional software packages. These packages can be installed from the EPEL repository.

To enable the EPEL repository

› Enable the EPEL repository by running:
  1. `yum install epel-release`
  2. `yum repolist`

Packages to install

› Add the following packages using `yum`.

<table>
<thead>
<tr>
<th>Package</th>
<th>For</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>glibc 64bit</td>
<td>Skybox</td>
<td><code>yum install glibc</code></td>
</tr>
<tr>
<td>glibc.i686 glibc-devel.i686</td>
<td>Skybox</td>
<td><code>yum install glibc.i686</code></td>
</tr>
<tr>
<td>pam.i686</td>
<td>Skybox</td>
<td><code>yum install pam.i686</code></td>
</tr>
<tr>
<td>numa</td>
<td>MySQL</td>
<td><code>yum install numactl-libs</code></td>
</tr>
<tr>
<td>wget</td>
<td>HTTP file retrieval</td>
<td><code>yum install wget</code></td>
</tr>
</tbody>
</table>

STARTING AND STOPPING COMPONENTS VIA THE WINDOWS SYSTEM TRAY

If you are working in Windows, you can start or stop the Server or Collector from the Skybox icon in the Windows system tray. You can launch the Manager in the same way.

To start or stop a Skybox component from the Windows system tray

› Right-click the Skybox icon (้าน) in the system tray and select the desired option.

Making the system tray icon visible after it was hidden

To make the system tray icon visible

› At the command line, run:

```
<Skybox_Home>\server\bin\startservertray.exe (or startservertray.bat if Skybox is installed as a program).
```

POST-INSTALLATION STEPS

After installing Skybox:
If you installed 2 Servers or 2 Collectors on the same machine (not recommended), check that you specified a unique set of ports for each installation (see Installing multiple components on a single host (on page 26)).

(Linux) Check that the machine’s resource limits are configured optimally for running Skybox (see Verifying resource limits in Linux (on page 27)).

Start the Server and the Collector if they did not start automatically.

The Server and the Collector start automatically:
- After installation completes (unless you cleared this option in the wizard)
- At system startup (unless you chose, in the wizard, to install either as a batch program)

If you changed these options, you must start the Server and Collector manually (see Starting and stopping the Server and Collector (on page 27)).

Set the time zone used by Skybox for logging and task scheduling. The default time zone is GMT (see Setting the time zone (on page 29)).

(The 1st time that you log in to Skybox) If the location of the license file was not provided during installation, specify its location during the login process.

Note: You cannot log in to Skybox until the license is added.

After logging in to Skybox, specify the SMTP server for Skybox to use and the Skybox administrator email address (see Email Configuration (on page 115)). Without this, Skybox cannot send alerts or receive emails.

Enable event logging (to syslog or Windows Event Viewer) for system events (see System Events (on page 116)).

Installing multiple components on a single host

You can install multiple Skybox components of a single type on a single machine. Required configuration changes are listed in this section.

Skybox Servers

We recommend that you install each Server on a separate machine. If you install multiple Servers on a single machine:

- Each installation must use a unique set of ports. These ports are set in the port properties file (see page 135).
- Only one Server per machine can run as a service; additional Servers must run as batch programs (see Starting and stopping the Server and Collector (on page 27)).

Skybox Managers

You can install and run multiple Managers on a single machine.

Skybox Collectors

We recommend that you install each Collector on a separate machine. If you install multiple Collectors on a single machine:
Each installation must use a unique set of ports. These ports are set in the port properties file (see page 135).

Only one Collector per machine can run as a service; additional Collectors must run as batch programs (see Starting and stopping the Server and Collector (on page 27)).

Verifying resource limits in Linux

After installing Skybox on a Linux machine, make sure that the resource limits of the main Skybox user match the recommended resource limits for Skybox.

To check resource limits

1. Switch from the root user to the skyboxview user (su - skyboxview).
2. Under /usr/bin, execute:
   ```bash
   ulimit -a
   ```
3. Compare the output results with the recommended values in the table that follows this procedure.
4. If the output results do not match the values in the table, edit /etc/security/limits.d/10-skybox.conf for the skyboxview user only.

   Each line in this file specifies a limit for the user, with the format:
   ```bash
   #<domain> <type> <item> <value>
   ```

   Note: Changing the values of resources in this file can cause changes to other values due to dependencies between the resources; after changing values, check that none of the other values are set higher than recommended.

Recommended resource limits are listed in the following table.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Recommended value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>core</td>
<td>0</td>
<td>Limits the core file size (kB)</td>
</tr>
<tr>
<td>data</td>
<td>unlimited</td>
<td>Maximum data size (kB)</td>
</tr>
<tr>
<td>size</td>
<td>unlimited</td>
<td>Maximum file size (kB)</td>
</tr>
<tr>
<td>memlock</td>
<td>unlimited</td>
<td>Maximum locked-in-memory address space (kB)</td>
</tr>
<tr>
<td>nofile</td>
<td>65536</td>
<td>Maximum number of open files</td>
</tr>
<tr>
<td>stack</td>
<td>unlimited</td>
<td>Maximum stack size (kB)</td>
</tr>
<tr>
<td>cpu</td>
<td>unlimited</td>
<td>Maximum CPU time (minutes)</td>
</tr>
<tr>
<td>nproc</td>
<td>unlimited</td>
<td>Maximum number of processes</td>
</tr>
</tbody>
</table>

Starting and stopping the Server and Collector

You can install the Server and the Collector as services or they can run as regular programs. If you install them as services, they usually start automatically.

If a component does not start automatically, you can start it manually.
Starting the Server and Collector on Windows

To start the Server or Collector

› Right-click the Skybox icon ( ) in the system tray and select Start <Component>.

To start the Server or Collector program from the command-line interface

› Server: <Skybox_Home>/server/bin/startserver.bat
› Collector: <Skybox_Home>/collector/bin/startcollector.bat

Stopping the Server and Collector on Windows

To stop the Server or Collector

› Right-click the Skybox icon ( ) in the system tray and select Stop <Component>.

To stop the Server or Collector program from the command-line interface

› Server: <Skybox_Home>/server/bin/stopserver.bat
› Collector: <Skybox_Home>/collector/bin/stopcollector.bat

Starting the Server and Collector on Linux

To start the Server as a service

› Execute one of:
  • service sbvserver start
  • /etc/init.d/ sbvserver start

Note: Additional keywords available when executing these commands are stop, status, and restart.

To start the Collector as a service

› Execute one of:
  • service sbvcollector start
  • /etc/init.d/ sbvcollector start

Note: Additional keywords available when executing these commands are stop, status, and restart.

To start the Server as a program on Linux

1 Log in to the Linux machine as user skyboxview and open a terminal window.
2 From the <Skybox_Home>/server/bin directory, execute:
   ./startserver.sh&
To start the Collector as a program on Linux

1. Log in to the Linux machine as user **skyboxview** and open a terminal window.
2. From the `<Skybox_Home>/collector/bin` directory, execute:
   ```bash
   ./startcollector.sh&
   ```

Stopping the Server and Collector on Linux

**To stop the Server**

- From the `<Skybox_Home>/server/bin` directory, execute:
  ```bash
  ./stopserver.sh&
  ```

**To stop the Collector**

- From the `<Skybox_Home>/collector/bin` directory, execute:
  ```bash
  ./stopcollector.sh&
  ```

Setting the time zone

By default, Skybox uses GMT for logging and task schedules.

**To change Skybox time to local time**

1. Add a property, `user.timezone`, to `<Skybox_Home>/server/conf/system.properties`
2. Set the property to:
   - A GMT offset
     For example, `user.timezone=GMT-8`
     
   - A location
     For example, `user.timezone=America/Los_Angeles`

   Note: Reset the GMT offset when switching to or from daylight saving time (summer time).

Storing your files

Skybox installation creates an empty directory under `<Skybox_Home>` named `integration`. Use this directory to store all external files that you want to keep in the installation (for example, those required for model building or updating), including configuration files from data sources that you imported into the model.

ELASTICSEARCH AND SKYBOX

Skybox Server now supports the export of data into an external instance of Elasticsearch.
Prerequisites for working with Elasticsearch

- You must configure Skybox to work with Elasticsearch
- The hosted Elasticsearch version must be any 6.x.y version from 6.4.2 and up. We recommend that you use version 6.4.2.

Configuring Skybox to work with Elasticsearch

Set up Skybox to work with Elasticsearch at Tools > Options > Server Options > Elasticsearch Export Settings (on page 111).

Elastic Cloud

Skybox can export data to a hosted Elastic Cloud running on AWS or GCP. For further information, see https://www.elastic.co/guide/en/cloud/current/getting-started.html

Skybox can export data to Elastic Cloud Enterprise running on-premises. For further information, see https://www.elastic.co/guide/en/cloud-enterprise/current/ece-overview.html

Using Elasticsearch with Skybox

Indexing Skybox data into Elasticsearch

Skybox data can be indexed into Elasticsearch in any of 3 ways:

- Invoking a Skybox task of type Elasticsearch – Index Export
  For more information about this task, see Elasticsearch index export tasks, in the Skybox Reference Guide.

- Invoking any CSV export task in Skybox with Export to Elasticsearch selected

- Invoking es documents Skybox REST API calls at
  https://<host>:8443/skybox/webservice/swagger-ui/index.html, where
  <host> is the IP address or name of the Skybox Server

IP address search

Fields of the IP address type can be searched as follows:

- In the query search bar, fieldName:10.125.0.0/8
- In Add filter, fieldName is one of 10.125.0.0/8

Region Map visualization can be used the field hostLocationCountry.

Kibana

Kibana is no longer distributed with Skybox installations.

To install Kibana

1 Follow the directions in

2 Replace the contents of the Kibana configuration with the files from
   <Skybox_Home>/server/conf/kibana
This chapter explains how to install the Skybox Collector by itself. There are several possible Collector installation scenarios; each scenario requires a different installation process.

Before you start, check Collector system requirements (on page 32).

After you install a Collector, you must connect it to the Server. See Connecting Skybox Connectors (on page 33).

In this chapter

Installation environment ...................................................... 31
Installing the Collector on Windows ....................................... 31
Installing the Collector on Linux ............................................ 32
Collector system requirements ............................................. 32
Connecting Skybox Collectors ............................................. 33

INSTALLATION ENVIRONMENT

<table>
<thead>
<tr>
<th>If you are installing in this environment...</th>
<th>Refer to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skybox Appliance</td>
<td>Skybox 5500/6000/7000/8000 Appliance Quick Start Guide</td>
</tr>
<tr>
<td>Skybox Virtual Appliance (ISO installed in a VMware environment)</td>
<td>Skybox Virtual Appliance Installation Guide</td>
</tr>
<tr>
<td>Windows</td>
<td>Installing the Collector on Windows (on page 31)</td>
</tr>
<tr>
<td>Linux</td>
<td>Installing the Collector on Linux (on page 32)</td>
</tr>
</tbody>
</table>

INSTALLING THE COLLECTOR ON WINDOWS

To install the Skybox Collector on Windows:

› Turn off previously installed versions of Skybox to prevent port collision
› Have administrator privileges

To install the Skybox Collector on Windows

Note: To install the Collector on Windows without user interaction, use the procedure in Silent installation (on page 20).
1 Run the installation file (SkyboxInstaller-<version#>-<build>.exe).

2 Follow the directions in the wizard.
   Mandatory options are listed in the following table. In all other places, either use the default option or make any necessary changes.

<table>
<thead>
<tr>
<th>Page Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Install Set</td>
</tr>
<tr>
<td>Choose Install Folder</td>
</tr>
<tr>
<td>Preferences</td>
</tr>
</tbody>
</table>

For instructions about starting the Collector, see Starting and stopping the Server and Collector (on page 27).

### INSTALLING THE COLLECTOR ON LINUX

**Before installing the Collector**

Before installing the Collector on Linux:

- Turn off previously installed versions of Skybox to prevent port collision
- Be the root user
- Install all required packages (see Installing packages (on page 25))

**To install the Skybox Collector on Linux**

- Use the installation procedure provided in Silent installation (on page 20).

For instructions about starting the Collector, see Starting and stopping the Server and Collector (on page 27).

### COLLECTOR SYSTEM REQUIREMENTS

The Skybox Collector does not need a powerful machine because there is no heavy processing or data storage on the Collector side; the collected data is moved to the Skybox Server machine for processing.

We recommend that you permit communication through ports 22 and 9443 only.

**Note:** Install each Skybox Collector on a separate machine (to prevent port collision). If you do install 2 Collectors on the same machine, you must change the ports used by 1 of them (see Installing multiple components on a single host (on page 26)).

**Operating system**

The operating systems supported for the Collector are listed in the following table.

**Note:** The Collector must run on a 64bit operating system.
Chapter 5  Collector installation

### Operating system
- Windows 7
- Windows 10
- Windows Server 2012
- Red Hat Enterprise Linux 6 (for existing installations only)
- Red Hat Enterprise Linux 7
- CentOS 6 (for existing installations only)
- CentOS 7

### Hardware
The hardware requirements for a Collector machine are listed in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>4 cores</td>
<td>8 cores</td>
</tr>
<tr>
<td>RAM</td>
<td>16 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Available disk space</td>
<td>100 GB</td>
<td>500 GB</td>
</tr>
</tbody>
</table>

Note: Syslog collection requires the resources specified in the **Recommended** column. For additional information, contact [Skybox Support](#).

### CONNECTING SKYBOX COLLECTORS
After installing a Skybox Collector:

- Add it to Skybox so that the Server can connect to it to collect data
- Connect it to the networks from which it is to collect data

Note: The current SSH client used by the Skybox Collector for remote collection can only use a Diffie-Hellman key of up to 2048 bits. Collection from remote devices that use a larger key will fail.

### Adding a new Collector to Skybox
Only **Admins** can add Collectors to Skybox.

**To add a Collector to Skybox**

1. In the Operational Console, right-click **Collectors** and select **New Collector**.
2. In the New Collector dialog box, define the Collector.
   
   Note: If you change the port value, change the Collector’s listening port on the Collector machine.
3. Click **OK**.

After you add Collectors to Skybox (or at any other time), you can verify connectivity between the Server and the Collectors.
To verify connectivity from the Server to Collectors

1 In the Operational Console:
   • To check all Collectors: In the tree, right-click Collectors and select Update All Statuses.
   • To check a single Collector: In the Table pane, right-click the Collector and select Check Status.

2 Check the Status column in the Table pane; if the status is Up, the Server is connected to the Collector and you can use it to retrieve data.
Chapter 6

Additional Servers

In some cases, it is neither possible nor desirable to manage your whole enterprise network as a single model on a single Skybox Server. Possible reasons for this include:

› Skybox is managing unrelated networks or enterprises.
› Different business units require autonomy in managing their security risks and you have decided to deploy a separate Skybox Server for each business unit.
› Security reasons dictate full separation between different parts of your enterprise network, even within the model.
› The full enterprise network cannot be conveniently handled as a single model in Skybox.

If any of these reasons apply, as required:

› Include multiple models on a single Skybox Server.
  Only one model can be active at any time, but you can switch between the different models at any time.

› Deploy multiple Skybox Servers within your enterprise network.
  You can either manage all the Servers from the same Skybox Manager or use a separate Skybox Manager for each Server.

The following figure shows an example of a multiple-server deployment.
In some scenarios, organizations want Skybox Change Manager to run on separate web servers, not on the main Skybox Server.

To add servers for Skybox Change Manager
1 Install an additional Skybox Server (on page 35) on each machine that you want to use as a web server for Change Manager.

2 On each web server machine, in \<Skybox_Home>\server\conf\sb_server.properties, set the value of web_remote.skybox_server to be the IP address or full path name of the main Skybox Server.

3 On the main Skybox Server, add each web server as a Skybox Collector: In the Operational Console, right-click Collectors and select New Collector; add the web server IP address and a name for this Collector.

Users running Skybox Change Manager must log in to a web server rather than the Skybox Server.

Note: The following scenarios are not supported: Skybox Server running on Linux and web servers running on Windows, and vice versa.
Autonomous collection units

In some scenarios, organizations need to install autonomous Skybox collection units on separate servers. Autonomous collection units include collection capabilities, tasks, and user administration. The collected data is not sent to a Skybox Server, but rather saved locally and then downloaded to a device (such as a disk on key) for later upload to a Skybox Server at a different location.

Hardware requirements

Hardware requirements for autonomous collection units are listed in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>8 cores</td>
</tr>
<tr>
<td>RAM</td>
<td>32 GB</td>
</tr>
<tr>
<td>Available disk space</td>
<td>1 TB</td>
</tr>
</tbody>
</table>

*Note:* If the collection unit is running on Linux, at least one Manager (Java client) must be installed on a Windows machine to operate the Collector (for example, to run the tasks and manage users).

To install a collection unit

1. **Download the installation file** (on page 14) or locate it on the file system if it was already downloaded:
   - (Windows) SkyboxInstaller-<version#>-<build>.exe
   - (Linux) SkyboxInstaller-<version#>-<build>.bin
2. Copy the file to your computer.

3. Create a file called installer.properties in the directory on your computer that contains the installation program. Use the sample text following these instructions as the basis for the file.

4. Install Skybox as explained in Silent installation (on page 20).

Sample installer.properties for a collection unit

```
SB_OEM=AUTONOMOUS_COLLECTION
INSTALLER_UI=silent
#SB_INSTALL_USER=skybox
SB_SERVER_HOST=localhost
# (for windows installation change USER_INSTALL_DIR to C:\\Program Files\\Skybox)
USER_INSTALL_DIR=/opt/skyboxview
# -- Manager ,Collector ,Server(Full)
CHOSEN_INSTALL_SET=Server(Full)
# -- License file name and location
SB_LICENSE_FILE=license.xml
SB_PATH_OF_LICENSE_FILE=
# -- Install as services and start after the installation options (1=yes, 0=no)
SB_SERVER_SERVICE=1
SB_COLLECTOR_SERVICE=1
SB_SERVER_SERVICE_START=0
SB_COLLECTOR_SERVICE_START=0
# -- Mail server IP/name address for sending reports/alerts, and admin email
SB_SERVER_MAIL=
SB_MAIL_ADDRESS=skybox_admin@skyboxsecurity.com
# -- Option to install Acrobat Reader on the Manager (1=yes, 0=no)
SB_MANAGER_ACROBAT=0
# (Win only)
#USER_SHORTCUTS=C:\\Documents and Settings\\All Users\\Start Menu\\Programs\\Skybox
#SHORTCUT_NAME=skyboxview
SB_PS_VISTA=0

#Upgrade Settings
SB_INSTALL_NEW=1
SB_INSTALL_UPGRADE=0

#Skybox Previous Home Directory
# * It's recommended that USER_INSTALL_DIR and SB_PREV_HOME_DIR won't be the same
SB_PREV_HOME_DIR=/opt/Skybox
# (for Win the default is: C:\\Program Files\\Skybox)
```

### Installing the Manager

- To install the Manager, follow the same instructions as for the collection unit, but use the following sample file as the basis for the installer.properties file.
  - Make sure to change the value of SB_SERVER_HOST to the IP address of the collection unit.
Sample installer.properties for the Manager

```
SB_OEM=AUTONOMOUS_COLLECTION
INSTALLER_UI=silent
#SB_INSTALL_USER=skyboxview
SB_SERVER_HOST=localhost
USER_INSTALL_DIR=/opt/skyboxview
CHOOSEN_INSTALL_SET=Manager
SB_MANAGER_ACRÔBAT=0
#USER_SHORTCUTS=C:\\Documents and Settings\\All Users\\Start
Menu\\Programs\\Skybox
#SHORTCUT_NAME=skyboxview
SB_PS_VISTA=0

#Upgrade Settings
SB_INSTALL_NEW=1
SB_INSTALL_UPGRADE=0

#Skybox Previous Home Directory
# * It's recommended that USER_INSTALL_DIR and SB_PREV_HOME_DIR won't be
# the same
SB_PREV_HOME_DIR=/opt/Skybox
# (for win the default is: C:\\Program Files\\Skybox)
```
## Skybox connectivity requirements

The connectivity requirements for Skybox installations are described in the following table.

<table>
<thead>
<tr>
<th>From...</th>
<th>To...</th>
<th>Port / service</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skybox administrator workstation</td>
<td>Skybox Appliance</td>
<td>22/TCP and 444/TCP</td>
<td></td>
</tr>
<tr>
<td>Skybox Manager</td>
<td>Skybox Servers</td>
<td>8443/TCP</td>
<td></td>
</tr>
<tr>
<td>Skybox Servers</td>
<td>Skybox Collectors</td>
<td>9443/TCP</td>
<td></td>
</tr>
<tr>
<td>Skybox Appliance</td>
<td>NTP server</td>
<td>123/UDP</td>
<td></td>
</tr>
<tr>
<td>Skybox Servers</td>
<td>Internal syslog server</td>
<td>514/UDP</td>
<td></td>
</tr>
<tr>
<td>Skybox Servers</td>
<td>LDAP</td>
<td>389/TCP or 636/TCP (for LDAPS)</td>
<td>Used for Skybox application authentication</td>
</tr>
<tr>
<td>Skybox Servers</td>
<td>RADIUS server</td>
<td>1812/TCP and 1813/TCP</td>
<td>Used for Skybox application authentication</td>
</tr>
<tr>
<td>Skybox Appliance</td>
<td>LDAP</td>
<td>389/TCP</td>
<td>Used for authenticating the underlying OS to LDAP</td>
</tr>
<tr>
<td>Skybox Appliance</td>
<td>RADIUS server</td>
<td>1812/TCP and 1813/TCP</td>
<td>Used for authenticating the underlying OS to RADIUS</td>
</tr>
<tr>
<td>Skybox Server</td>
<td>SMTP server</td>
<td>25/TCP</td>
<td></td>
</tr>
<tr>
<td>SNMP monitoring platform</td>
<td>Skybox Appliance</td>
<td>161/UDP</td>
<td></td>
</tr>
<tr>
<td>Skybox Appliance</td>
<td>DNS server</td>
<td>53/UDP</td>
<td></td>
</tr>
<tr>
<td>Skybox Server or Collector on which the <strong>Dictionary Update</strong> task is configured</td>
<td>Skybox Internet update services (dictionary and update URLs)</td>
<td>443/TCP</td>
<td>Configure the proxy with https://*.skyboxsecurity.com / to collect data from all hosts in the skyboxsecurity.com domain</td>
</tr>
<tr>
<td>Firewalls / Syslog server</td>
<td>Skybox Collectors</td>
<td>514/UDP</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 10

Updating Skybox

You can update Skybox without uninstalling the current version; software updates for Skybox are issued periodically.

To update the Skybox Vulnerability Dictionary, see Dictionary updates (on page 138).

In this chapter

Updating Skybox ................................................................. 41
Skybox update file ............................................................. 42
Downloading the update file ............................................. 42
Preparing to update ......................................................... 42
Updating the Server and local components ..................... 43
Updating remote components ......................................... 44
Updating multi-tiered servers ......................................... 44

UPDATING SKYBOX

To update Skybox:

1. Download a software update file (see page 42) from the Skybox update management server.

2. Make any necessary preparations (see page 42).

3. Run the update tool (see page 43) (included in the Skybox installation) to apply the update file to Skybox.

   The Server and other local components are updated, and then the remote Managers and Collectors are updated.

Note: If you need to roll back to a previous version for any reason, contact Skybox Support

Important: In Skybox version 9.0.700 and higher, the infrastructure of the Collector was migrated from a JBoss application server deployment to a new infrastructure, based on Spring Boot version 1.5.17 with an embedded Tomcat servlet container, version 8.5.34. If you have done any customization of the old JBoss Tomcat server.xml file or the TLS setting in <Skybox_Home>/collector/conf/jvmargs.properties for any existing Collectors, you must customize the new infrastructure as well. For additional information, see Migrating the Collector infrastructure (on page 46)
SKYBOX UPDATE FILE

A Skybox update can be a patch to the current version or an upgrade to a newer version. Each downloaded update file is a compressed file that contains updates for all supported operating systems.

Update files are *cumulative*; each file contains all published updates for the current version.

Each update file has an accompanying file, Readme.txt, that contains information about the update.

DOWNLOADING THE UPDATE FILE

You can query the Skybox update management server to see whether an update to the installed version of Skybox is available and then download the update file.

Note: If the Manager machine is configured to connect to the internet via a proxy, configure the proxy settings before you download an update file (go to Tools > Options > Manager Options > Proxy Settings (Manager)).

To download an update file

Note: You can download the latest update file in the background by running (or scheduling) a Tools – Server Software Update task. For information about Tools – Server Software Update tasks, see the Server software update tasks topic in the Reference Guide.

1 Select Help > Check for updates.

In the About Skybox dialog box, Version Information is selected in the tree.

Skybox connects to the Skybox update management server; a Check for update progress bar is displayed in the dialog box.

When the check is complete, the version number of the update file is displayed in the Available version field.

Note: If the installed version of Skybox is current, no new version available is displayed in the Available version field.

2 Click Download.

The update file starts to download; a progress bar is displayed in the dialog box.

When the download completes, the progress bar closes and the version number is displayed in the Ready for installation field.

To apply the update file to the Server, see:

- Preparing to update (on page 42)
- Updating the Server and local components (on page 43)

PREPARING TO UPDATE

Before updating the Server:
1. Read the Readme.txt file that comes with the update file; it might specify additional steps required during the update that are not included in the standard update instructions.

   The readme file also includes the MD5 checksum for the update file (at the start of the Fix installation section).

   Note: If you received the update via Help > Check for updates, you can view the readme file from Skybox by clicking Help > Check for updates and then clicking View release notes.

   The readme file is available online at the same location as the update files: https://update-us1.skyboxsecurity.com/updates/releases/oem1/10.0.0/

   Take the file whose name exactly matches that of your update file. For example, Readme-10.0.106-74.txt matches upgrade-10.0.106-74.sbu.

2. Verify the security of the downloaded update file:
   a. Run md5sum on the file from the directory to which you downloaded the update file: `md5sum <filename>`.
   b. Check that the value you receive matches the checksum value specified in the readme file.

3. If you work with the What If and Forensic models, back up a copy of each of them (File > Models > Save) as a precautionary measure before applying an update (see Backing up the model (on page 79)).

   Note: If the Skybox Server is running, Skybox backs up the Live model as part of the update; Skybox does not back up the What If and Forensics models.

**UPDATING THE SERVER AND LOCAL COMPONENTS**

The Update tool updates the Server and any other components on the Server machine in the same installation directory as the Server.

**To update the Server**

1. (Recommended) Make sure that the Server is running so that Skybox can back up the model as part of the update process.

2. If the Manager is running on the Server machine, shut down the Manager before running the Update tool.

3. Copy the update file to `<Skybox_Home>\utility\bin`

4. Run the Update tool:
   - (Windows) `<Skybox_Home>\utility\bin\updatetool.bat`
   - (Linux) `<Skybox_Home>/utility/bin/updatetool.sh`

   Any Skybox user can execute the update; there is no need to log in as root.
Before applying the update, the Skybox Server backs up the Live model to 
<Skybox_Home>\data\xml_models\update_backup<MMddyyyyHHmm>.xml

Note: If the Server is not running, the Live model is not backed up and your data might be lost in the event of a system failure during the update. In some cases, the Update tool does not continue until the Server backs up the Live model. Restart the Server and run the Update tool again.

Most Server updates take between 5 and 8 minutes. During this time, the Update tool stops the Server (and, if present, the local Collector), applies the update, and restarts the Server (and Collector).

As part of the update, the following occur:
- The files in the update package (1 for each operating system that has separate update instructions) are copied to the <Skybox_Home>\data\fixes directory, where they are used to update remote Managers and Collectors.
- The files necessary to restore the previous version are saved in the <Skybox_Home>\updates\<update directory name>\backup directory, where <update directory name> includes the version and operating system.

UPDATING REMOTE COMPONENTS

When the Server machine is updated, remote Managers and Collectors cannot work with the Server until they are updated to the same version as the Server.

Updating remote Managers
Remote Managers are updated as part of the login procedure.

Updating remote Collectors
The Server checks the version of all running Collectors on an hourly basis to see whether they need updating. If the Server detects that a Collector needs updating, it sends the appropriate update file for the Collector operating system and updates the Collector.

You can update a Collector by running a Tools – Collector Software Update task. This is useful if you do not want to wait until the next update check or if a Collector was down during the scheduled update.

UPDATING MULTI-TIERED SERVERS

If you work with multi-tiered servers, the remote web servers are not updated as remote Collectors. You must update them separately.

To update a remote web server
1. Copy the update file to <Skybox_Home>\utility\bin on the remote server machine.
2. Run the Update tool:
   (Windows) <Skybox_Home>\utility\bin\updatetool.bat
   (Linux) <Skybox_Home>/utility/bin/updatetool.sh
Any Skybox user can execute the update; there is no need to log in as root.

3 Verify that the server restarted.
Chapter 11

Migrating the Collector infrastructure

As of version 9.0.700, the Collector infrastructure was migrated from a JBoss application server deployment to one based on Spring Boot version 1.5.17 with an embedded Tomcat servlet container version 8.5.34.

General changes

- The configuration for Tomcat and Spring Boot is in the spring boot section in <Skybox_Home>/collector/conf/sb_collector.properties
- The default port is set to 9443; the shutdown port is set to 9099 and is bound to localhost.
- Logging configuration is now set in <Skybox_Home>/collector/conf/log4j-collector.xml, which gets sampled every minute.
- Java garbage collection logs have changed location to <Skybox_Home>/collector/log/debug/gc
- On Windows, when the Collector is running as an operating system service, the service is reinstalled on every update.
  For this reason, if you changed the service logon options to use a service user for collection, you must specify the service user again after every update.
- Any messages in the Collector logs that are marked as "(mock msg)" are intended for backward compatibility and can be safely ignored.

Changes for customized Collectors

The following information is relevant for any Collectors in which the old JBoss Tomcat server.xml file or the TLS settings in <Skybox_Home>/collector/conf/jvmargs.properties were customized:

- Copy any customization of the old JBoss Tomcat server.xml file or the TLS settings in <Skybox_Home>/collector/conf/jvmargs.properties to the spring boot section in <Skybox_Home>/collector/conf/sb_collector.properties.
- Future updates will overwrite conf/jvmargs.properties for the Collector, and recalculate the memory settings. Therefore, add any customization to conf/jvmargs.user.properties, which is not modified by the update.

Main Spring Boot parameters

The following is a list of the main parameters in the spring boot section of <Skybox_Home>/collector/conf/sb_collector.properties:
springboot.server.port=9443
springboot.server.session.timeout=3600
springboot.server.ssl.key-store=classpath:server.keystore
springboot.server.ssl.keyStoreType=JKS
springboot.server.ssl.protocol=TLS
springboot.server.ssl.enabled-protocols=TLSv1.2
springboot.server.ssl.enabled-protocols=TLSv1.2,TLSv1.1,TLSv1
springboot.server.session.cookie.http-only=true
springboot.server.session.cookie.secure=true

A full list of Spring Boot settings is available at:

> [https://docs.spring.io/spring-boot/docs/1.5.17.RELEASE/reference/htmlsingle/#common-application-properties](https://docs.spring.io/spring-boot/docs/1.5.17.RELEASE/reference/htmlsingle/#common-application-properties)
Chapter 12

Skybox licenses

You install a Skybox license file by uploading it to the Server. The license controls the Skybox products that are available, the license expiration date, and the maximum size of the network model.

Viewing license information

To view license information
1 Select Help > About Skybox.
2 In the tree, select License Information.

Updating the license

If you receive a new license from Skybox, save it on your file system and upload it to the Server.

To upload a new license
1 Select Help > About Skybox > License Information.
2 Click Update License.
3 In the dialog box, navigate to the file location and click Open.

In this chapter

Invalid licenses .......................................................... 48
Node-count violations .................................................. 49

INVALID LICENSES

If you try to launch Skybox with an invalid license, the Skybox Server does not start.

A license is invalid if:

› It has expired
› It does not match the Skybox product being launched
› The license hardware ID does not match the server that is trying to run Skybox
› The grace period has expired for an old license version

Sometimes, when a new version of Skybox is released, it has a new license scheme. In this case, you have a grace period (usually 30 days) to install a new license. If you launch Skybox during the grace period, Skybox displays a warning message.
The grace days have expired for a license node-count violation
License node-count violations are described in the following section.

**NODE-COUNT VIOLATIONS**

Each Skybox license limits the number of nodes that you can include in the model of your network. When you launch a Skybox product, Skybox checks the number of nodes in the model. If the number of nodes exceeds the license limit, Skybox displays a warning message.

Skybox provides a 30-day grace period for violations in the number of licensed nodes in Skybox products. Each day that there is a violation in any product uses up a day of the grace period. The purpose of the grace period is to enable you to continue working with Skybox while you either fix the violation by deleting unnecessary nodes or upgrade your license to include additional nodes. After the grace period expires, the Server is locked; you must get a new license to continue working with Skybox.

The entities that are limited per Skybox product are listed in the following table.

<table>
<thead>
<tr>
<th>Product</th>
<th>Limited entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Assurance</td>
<td>Physical and virtual devices in the Firewall Assurance workspace</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The Add Firewalls Wizard does not permit you to exceed the licensed number of firewall nodes</td>
</tr>
<tr>
<td>Network Assurance</td>
<td>Network devices in the model Virtual assets in clouds and virtualized environments</td>
</tr>
<tr>
<td>Vulnerability Control</td>
<td>Number of assets in the model</td>
</tr>
</tbody>
</table>

**Note**: These limits apply to the Live model only.
Chapter 13

Uninstalling Skybox

To uninstall Skybox from a Linux machine
The commands in this procedure require root permissions.

1 Uninstall the server service and the collector service:
   • `<Skybox_Home>/server/bin/uninstall_service_server.sh`
   • `<Skybox_Home>/collector/bin/uninstall_service_collector.sh`

2 Delete the entire Skybox directory:
   • `rm -rf <Skybox_Home>/`

3 Delete the Skybox user and the Skybox home directory:
   • `userdel -r skyboxview`

4 Delete the Skybox group:
   • `groupdel skyboxview`

To uninstall Skybox from a Windows machine
The commands in this procedure require administrator permissions.

1 Uninstall the server service and the collector service:
   • `<Skybox_Home>\server\bin\ uninstall-server-service.bat`
   • `<Skybox_Home>\collector\bin\ uninstall-collector-service.bat`

2 Delete the entire Skybox directory `<Skybox_Home>`
Chapter 14

Product security

This chapter explains steps that Skybox takes to ensure that the Skybox platform and its data are kept secure.

In this chapter

- Communication and certificates ............................................ 51
- Encryption ......................................................................... 54
- Using FIPS mode ............................................................ 55
- Limiting login attempts ..................................................... 55
- Security check: Last login message ...................................... 55
- Customizable login warning messages ................................. 55
- User session timeout ....................................................... 56

COMMUNICATION AND CERTIFICATES

Communication between Skybox Managers and the Skybox Server, and between the Server and Skybox Collectors is via an SSL service. The SSL service requires a certificate store protected by a password.

Skybox, as installed, has a default certificate store. The values in this store are the same for all Skybox products. However, you can use your own certificates; the following sections explain how to do this.

For information about viewing certificates, see Viewing certificates (on page 53).

For information about changing the default keystore password, see Changing the default password of the keystore (on page 53).

Generating a self-signed certificate for Skybox

To generate a self-signed certificate for Skybox

1. Connect to the server as the skyboxview user.
2. Navigate to <Skybox_Home>/server/conf

   Important: Work in this directory only; all commands use relative paths.

3. Back up the following files:
   - server.keystore
   - cacerts_customer.keystore
4 Create a new certificate request by running the following command.
   - Replace each instance of the term `<string>` in the command with the relevant text.
   - In this step and all subsequent steps, replace `<version#>` with the JDK version (for example, `1.8.0_152d`).
   - Google Chrome versions 65 and higher require an additional attribute in this command. See the subsection following this procedure for information.
   - The keysize value and algorithm number (`-sigalg`) may vary.

   ```
   ..\..\thirdparty\jdk<version#>\bin\keytool -genkey -keyalg rsa -keysize 2048 -sigalg SHA256withRSA -dname "CN=<string>, OU=<string>, O=<string>, L=<string>, S=<string>, C=<string>" -alias <mykey> -keypass skyboxview -keystore server.keystore -storepass skyboxview -validity 90
   ```

5 Review the `server.keystore` file to confirm that the certificate request was successfully added:

   ```
   ..\..\thirdparty\jdk<version#>\bin\keytool -list -v -keystore server.keystore -storepass skyboxview
   ```

   The relevant information appears under the alias `<mykey>`.

6 Generate the certificate request file, and make sure that the alias is the same as in step 4:

   ```
   ..\..\thirdparty\jdk<version#>\bin\keytool -certreq -file <file name> -alias <mykey> -keystore server.keystore -storepass skyboxview
   ```

7 Using the generated request file, follow the internal certificate request procedure to sign and receive the certificate. Make sure that the certificate format is PEM, Base64 encoded.

8 Add the CA root certificate to the keystore:

   ```
   ..\..\thirdparty\jdk<version#>\bin\keytool -import -alias root -file <CA root certificate file> -keystore server.keystore -storepass skyboxview
   ```

9 Add the intermediate certificate to `server.keystore`:

   ```
   ..\..\thirdparty\jdk<version#>\bin\keytool -import -alias inter -file <intermediate certificate file> -keystore server.keystore -storepass skyboxview
   ```

10 Replace the self-signed certificate with the CA signed certificate in the keystore. Make sure that the alias is the same as in step 4:

   ```
   ..\..\thirdparty\jdk<version#>\bin\keytool -import -alias <mykey> -file <certificate file> -keystore server.keystore -storepass skyboxview
   ```

11 Delete the predefined key:

   ```
   ..\..\thirdparty\jdk<version#>\bin\keytool -delete -alias <skyboxkey> -keystore server.keystore -storepass skyboxview
   ```

12 Add the CA root certificate to your cacerts keystore:

   ```
   ..\..\thirdparty\jdk<version#>\bin\keytool -import -alias root -file <CA root certificate file> -keystore cacerts_customer.keystore -storepass skyboxview
   ```
Add the intermediate certificate to your cacerts keystore:
```
..\..\thirdparty\jdk<version#>\bin\keytool -import -alias inter -file <intermediate certificate file> -keystore cacerts_customer.keystore -storepass skyboxview
```

Restart all Skybox Servers, Collectors, and Managers.

Working with Google Chrome version 65 and higher

From version 65, Google Chrome enforces the existence of the SAN (Subject Alternative Name) attribute in server certificates. By default, Skybox certificates do not include this attribute. For Skybox users to connect via Google Chrome, you must regenerate your certificates to include the attribute (or include it when generating a new certificate).

In the preceding workflow for generating a certificate, use the following command in place of the command at step 4.
```
..\..\thirdparty\jdk<version#>\bin\keytool -genkey -keyalg rsa -keysize 2048 -sigalg SHA256withRSA -dname "CN=<string>, OU=<string>, O=<string>, L=<string>, S=<string>, C=<string>" -alias <mykey> -keypass skyboxview -keystore server.keystore -storepass skyboxview -validity 90 -ext san=dns:<website>
```

If your organization has separate web servers for Change Manager

If your organization has separate web servers for Change Manager (not the main server running the database), you must import the root CA certificate to cacerts_customer.keystore on each web server.

You can check whether there are separate web servers for Change Manager by checking the `web_remote_skybox_server` property in `<Skybox_Home>\server\conf\sb_server.properties`

A value of anything other than 127.0.0.1 (localhost) means that separate web servers are used for Change Manager.

Viewing certificates

To view the content of a certificate

1. Go to `<Skybox_Home>\thirdparty\jdk<version#>\bin`, where `<version#>` is the version number of the JDK.
2. Run the command: `keytool.exe -v -list -keystore ..\..\server\conf\client.keystore -keypass skyboxview`

Changing the default password of the keystore

This section explains how to change the default password of the keystore. This must be done after installation, before starting the Server.

To change the default keystore password after installation

Note: Throughout this procedure, replace `<version#>` with the JDK version (for example, 1.8.0_152d).

1. Move to the directory containing the files:
   ```
   cd /opt/skyboxview/server/conf/
   ```
2 Execute the command:
   
   ```bash
   ../../thirdparty/<version#>/bin/keytool -keypasswd -keystore server.keystore -alias <skyboxkey>
   ```

   **Note:** If the Change certificate procedure was done before this procedure, change the alias to `<mykey>`.

3 Enter the keystore password: `(skyboxview)`.

4 Enter a new key password for `<skyboxkey>`.

5 Execute the command:
   
   ```bash
   ../../thirdparty/<version#>/bin/keytool -storepasswd -keystore server.keystore
   ```

6 Enter the keystore password: `(skyboxview)`.

7 Enter a new key password for `<skyboxkey>`.

8 Modify `secret.keyStorePassword` in
   `<Skybox_Home>/server/conf/sb_common.properties`

9 Start the Server.

### Replacing basic authentication for Web UI users

For users of Skybox Web UI, you can replace the basic authentication with client-side authentication.

**To replace basic authentication with client-side authentication**

1 Generate a client-side certificate according to your organization’s guidelines.

2 Install the certificate in each web browser that will be used for the Skybox Web UI.

3 Set the value of `client_cert` in
   `<Skybox_Home>/server/conf/sb_server.properties` to **true**.

Once this is done, each user who connects to the Web UI must select the certificate to use each time that they log in.

### ENCRYPTION

XML files and secret properties are encrypted for security reasons.

#### XML encryption

By default, when you back up a model to an XML file, the XML file is encrypted as an XMLX file as a security precaution. (To back up the model, select **File > Models > Save**. For additional information, see **Backing up the model** (on page 79).)

**To enable or disable file encryption when backing up a model to an XML file**

- Set the value of `encrypt_xml_files` in
  `<Skybox_Home>/server/conf/sb_server.properties` to **true** (recommended) or **false**.
USING FIPS MODE

In specific circumstances (for example, if you are a US government employee) you might be required to work in FIPS (Federal Information Processing Standards) mode.

Using FIPS mode has the following limitations:

- Old models saved in Skybox running in non-FIPS mode cannot be imported into Skybox running in FIPS mode (because they were encrypted using non-approved cryptographic ciphers).
  
  This means that there is no way to migrate directly from a non-FIPS mode installation.

- After Skybox is installed in a certain mode (FIPS or not FIPS), there is no way to switch between them, even during upgrades.

- If your organization uses self-signed certificates (cacerts), add the CA to thirdparty/jdk*/jre/lib/security/cacerts again after each major upgrade.

- Elasticsearch is automatically disabled.

LIMITING LOGIN ATTEMPTS

By default, after 3 failed login attempts by a Skybox user, their account is locked for 30 seconds. This limits the possibility of a non-user hacking into an account.

You can change the number of failed attempts and the time for which the account is locked by modifying the values of elapsed_lock_milliseconds and retry_allowed in <Skybox_Home>/server/conf/sb_server.properties.

SECURITY CHECK: LAST LOGIN MESSAGE

During the login process, Skybox Manager displays the date and time of the most recent successful login using your user name. For security reasons, check the date and time of this login to verify that the most recent use of your user name is legitimate.

Note: The same message ("Welcome <user name>, your last login was at <date> <time>") is displayed in the status bar at the bottom of the Manager window.

CUSTOMIZABLE LOGIN WARNING MESSAGES

You can add a customized warning message to the login screen. All users who log in to Skybox see the message.

To add a warning message to the login page

- Set login_warning_banner in <Skybox_Home>/server/conf/sb_server.properties to the desired text.

  Skybox adds <html> and </html> tags to this text; you can add other HTML tags.
USER SESSION TIMEOUT

User sessions (in the Manager and the web UI) automatically time out after a period of inactivity.

By default, user sessions time out after 30 minutes. You can change the timeout by changing the value of `client_session_timeout` in `<Skybox_Home>\server\conf\sb_server.properties`

- A value of -1 disables the timeout feature.

Note: After logging in again, the user’s previous point of reference in Skybox is restored.
Part II: Administration

This part includes topics of interest to system administrators, including user management, product security, and ticket setup and configuration.
Chapter 15

User management

Skybox is a multi-user system. There is a predefined Admin (skyboxview). After installation, this user can add additional users with different roles.

This chapter explains the different user roles, how to manage users in Skybox and externally, and how to work with external authentication systems.

Note: Only Admins can manage Skybox users. However, every user who has access to Skybox and who authenticates using the Skybox login mechanism can change their own password by selecting File > Change My Password.

In this chapter

User roles ................................................................. 58
Managing users and user groups ................................. 65
Working with external authentication systems ............... 72
Managing users externally using LDAP ........................ 74
Changing the password for database clients .................. 76

USER ROLES

The predefined user roles in Skybox are described in the following table.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Admins have permissions for all actions, including those that regular users do not.</td>
</tr>
<tr>
<td>Admin – Users</td>
<td>Same as Admin but functionality is limited to user administration only.</td>
</tr>
<tr>
<td>Admin – Operational</td>
<td>Same as Admin but functionality is limited to everything except user administration.</td>
</tr>
<tr>
<td>Admin – Vulnerability Control</td>
<td>Same as Admin but Skybox access is limited to Vulnerability Control and Threat Manager.</td>
</tr>
<tr>
<td>Admin – Assurance</td>
<td>Same as Admin but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.</td>
</tr>
<tr>
<td>User</td>
<td>Users have permissions for all actions except administrative tasks (for example, user management and model building). Users can access all Skybox products.</td>
</tr>
<tr>
<td>User – Vulnerability Control</td>
<td>Same as User but Skybox access is limited to Vulnerability Control and Threat Manager.</td>
</tr>
</tbody>
</table>
Chapter 15    User management

Role Description

User – Assurance Same as User but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.

Read-only User Read-only Users can view the model, but they cannot make changes to model entities. They have permissions for all activities required for managing tickets, including using and creating private analyses for displaying tickets. Read-only Users can be given access to any combination of Skybox products.

Read-only User – Vulnerability Control Same as Read-only User but Skybox access is limited to Vulnerability Control and Threat Manager.

Read-only User – Assurance Same as Read-only User but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.

Ticket User Ticket Users can manage tickets and view (but not generate) reports. This role is for Vulnerability Control and Threat Manager; it cannot be used for Change Manager.

Web Ticket User Web Ticket Users can log in to Change Manager, where they can manage tickets. They cannot log in to the Manager. This role is for Change Manager.

Web Ticket Requestor Web Ticket Requestors can create tickets (that is, submit change requests) in Change Manager and close tickets that they created. This role is for Change Manager.

Recipient Recipients can receive tickets, alerts, and reports. They cannot log in to Skybox or access any other Skybox features.

For information about user roles in Change Manager, see the User roles in the Skybox Change Manager User Guide.

Administrative users

The features and entities that each type of Admin can manage (create, modify, delete, and read) are listed in the following table. Additional clarification is provided after the table.

<table>
<thead>
<tr>
<th>User role / Feature or Entity</th>
<th>Admin – Users</th>
<th>Admin – Operations</th>
<th>Admin – Vul Control</th>
<th>Admin – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users, user groups, and user roles</td>
<td>✔</td>
<td></td>
<td>✔ (See note)</td>
<td>✔ (See note)</td>
</tr>
<tr>
<td>Triggers</td>
<td>✔</td>
<td>No</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>System logs (read-only)</td>
<td>✔</td>
<td>No</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Tools &gt; Options &gt; Server Options</td>
<td>✔</td>
<td>No</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
### User role / Feature or Entity

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Model instances (Live, What If, Forensics)</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

#### Vulnerability Control and Threat Manager related entities

<table>
<thead>
<tr>
<th>Feature or Entity</th>
<th>Admin</th>
<th>Admin – Users</th>
<th>Admin – Operations</th>
<th>Admin – Vul Control</th>
<th>Admin – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact Types</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Regulations</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Threat Alert Ticket Policies</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Vulnerability Occurrence Ticket Policies</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
</tbody>
</table>

#### Firewall Assurance and Network Assurance related entities

<table>
<thead>
<tr>
<th>Feature or Entity</th>
<th>Admin</th>
<th>Admin – Users</th>
<th>Admin – Operations</th>
<th>Admin – Vul Control</th>
<th>Admin – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Review Policies</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
</tr>
<tr>
<td>Rule Recertification Policies</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
</tr>
</tbody>
</table>

#### Operational Console

<table>
<thead>
<tr>
<th>Feature or Entity</th>
<th>Admin</th>
<th>Admin – Users</th>
<th>Admin – Operations</th>
<th>Admin – Vul Control</th>
<th>Admin – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection tasks</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Other tasks</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Collectors</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

#### Reports and analyses

<table>
<thead>
<tr>
<th>Feature or Entity</th>
<th>Admin</th>
<th>Admin – Users</th>
<th>Admin – Operations</th>
<th>Admin – Vul Control</th>
<th>Admin – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports – public and private</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ticket analyses – public and private</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Vulnerability Control and Threat Manager analyses – public and private</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Firewall Assurance and Network Assurance analyses</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
</tr>
<tr>
<td>Model analyses</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

#### Other

<table>
<thead>
<tr>
<th>Feature or Entity</th>
<th>Admin</th>
<th>Admin – Users</th>
<th>Admin – Operations</th>
<th>Admin – Vul Control</th>
<th>Admin – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skybox Horizon</td>
<td>✓</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In addition to this list, **Admins** can also manage all entities that can be managed by the corresponding user-type role. For example, **Admin – Assure** users can manage all entities that can be managed by **User – Assure** users.

### Notes

- **Admin – Vulnerability Control** users can only create users with the following roles:
Chapter 15    User management

- Admin – Vulnerability Control
- User – Vulnerability Control
- Read-only User – Vulnerability Control
- Recipient

▸ Admin – Assure users can only create users with the following roles:
  - Admin – Assure
  - User – Assure
  - Read-only User – Assure
  - Recipient
  - Custom user roles

▸ System logs are created automatically and can be viewed by the specified Admins.

Users

The features and entities that are available to each type of User user role are listed in the following table. The table also specifies whether the user can manage (create, modify, delete, and read) them or only read them.

<table>
<thead>
<tr>
<th>User role/Feature or Entity</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Map</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firewall Map</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Access Analyzer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Attack Explorer</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Tools &gt; Options &gt; Manager Options</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Workspaces</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Control and Threat Manager</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Firewall Assurance and Network Assurance</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Model workspace</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reports, tickets, and analyses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public reports</td>
<td>Generate</td>
<td>Generate</td>
</tr>
<tr>
<td>Private reports</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tickets</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Public ticket analyses</td>
<td>Read only</td>
<td>Read only</td>
</tr>
<tr>
<td>Private ticket analyses</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Vulnerability Control and Threat Manager public</td>
<td>Read only</td>
<td>Read only</td>
</tr>
<tr>
<td>User role/Feature or Entity</td>
<td>User</td>
<td>User – Vul Control</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>analyses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Control and Threat Manager public analyses</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firewall Assurance and Network Assurance analyses</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Model analyses</td>
<td>Read only</td>
<td>Read only</td>
</tr>
</tbody>
</table>

**Operational Console**

<table>
<thead>
<tr>
<th>Collectors</th>
<th>Read only</th>
<th>Read only</th>
<th>Read only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection tasks</td>
<td>Read only</td>
<td>Read only</td>
<td>Read only</td>
</tr>
<tr>
<td>Analysis tasks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CSV export and report generation tasks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ticket generation tasks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>XML Vulnerability Occurrence export tasks</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
</tbody>
</table>

**Vulnerability Control and Threat Manager related entities**

<table>
<thead>
<tr>
<th>Deployed products</th>
<th>✓</th>
<th>✓</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business units and Business Asset Groups</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Threat Origins</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
</tbody>
</table>

**Firewall Assurance and Network Assurance related entities**

<table>
<thead>
<tr>
<th>Exceptions</th>
<th>✓</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy management (access, rule, and configuration policies)</td>
<td>Edit, export, import</td>
<td>Edit, export, import</td>
</tr>
<tr>
<td>Application &amp; Service repository</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Read-only users**

The features and entities that are available to each type of **Read-only User** user are listed in the following table. The table also specifies whether the user can manage (create, modify, delete, and read) them or only read them.

<table>
<thead>
<tr>
<th>User role/Feature or Entity</th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Map</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firewall Map</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access Analyzer</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Attack Explorer</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User role/Feature or Entity</td>
<td>User</td>
<td>User – Vul Control</td>
<td>User – Assurance</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------</td>
<td>-------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Tools &gt; Options &gt; Manager Options</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

### Workspaces

<table>
<thead>
<tr>
<th></th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Control and Threat Manager workspaces</td>
<td>✔️</td>
<td>✔️</td>
<td>No</td>
</tr>
<tr>
<td>Firewall Assurance and Network Assurance workspaces</td>
<td>✔️</td>
<td>No</td>
<td>✔️</td>
</tr>
<tr>
<td>Model workspace</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

### Reports, tickets, and analyses

<table>
<thead>
<tr>
<th></th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports – Public</td>
<td>Can see properties as read only</td>
<td>Can see properties as read only</td>
<td>Can see properties as read only</td>
</tr>
<tr>
<td>Reports – Private</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Tickets</td>
<td>Create manually (for Vulnerability Control only)</td>
<td>Create manually</td>
<td>Read only</td>
</tr>
<tr>
<td>Ticket analyses – Public</td>
<td>Read only</td>
<td>Read only</td>
<td>Read only</td>
</tr>
<tr>
<td>Ticket analyses – Private</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Vulnerability Control and Threat Manager Public analyses</td>
<td>Read only</td>
<td>Read only</td>
<td>No</td>
</tr>
<tr>
<td>Vulnerability Control and Threat Manager Private analyses</td>
<td>✔️</td>
<td>✔️</td>
<td>No</td>
</tr>
<tr>
<td>Firewall Assurance and Network Assurance analyses</td>
<td>✔️</td>
<td>No</td>
<td>✔️</td>
</tr>
<tr>
<td>Model analyses</td>
<td>Read only</td>
<td>Read only</td>
<td>Read only</td>
</tr>
</tbody>
</table>

### Other / Miscellaneous

<table>
<thead>
<tr>
<th></th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending packlogs</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

### Firewall Assurance and Network Assurance related entities

<table>
<thead>
<tr>
<th></th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exceptions</td>
<td>Read only</td>
<td>No</td>
<td>Read only</td>
</tr>
<tr>
<td>Access Policies, Rule Policies, Configuration Policies</td>
<td>Read only</td>
<td>No</td>
<td>Read only</td>
</tr>
<tr>
<td>Application &amp; Service repository</td>
<td>Read only</td>
<td>No</td>
<td>Read only</td>
</tr>
</tbody>
</table>

### Vulnerability Control and Threat Manager related entities
Custom user roles

Skybox provides the ability to create custom user roles based on existing user roles.

For Firewall Assurance and Network Assurance, you can adjust the permissions for the following features to suit the needs of your organization.

- Exceptions: Full access or view only
- Analyses: Full access or view only
- Rule Policies: Full access or view only
- Access Policies: Full access or view only
- Configuration Policies: Full access or view only
- Configuration files: View only or no access
- Operational Console: Full access, view only, or no access
  - Permitted tasks: For user roles with full or viewing access to the Operational Console, you can select the Skybox tasks that they are permitted to run
    - Users with full access can also edit these tasks
- Reports: Full access, view only, or no access

Note: Because there are permissions for other features that are not included in the customization, we recommend that you start with the existing user role that is closest to the role that you want to create.

For Vulnerability Control, you can create a role based on Read Only User – Vulnerability Control and adjust the permissions for reports (full access, view only, or no access).

For Change Manager, you can create a role based on Web Ticket User and specify the tickets that users of this role can view (tickets assigned to themselves, to their group, or to anyone).

To create a custom user role

1. From the Tools menu, select Administrative Tools > User Roles.
2. In the Admin window, click .
3. Provide a name and description for the role.
4. Select a template.
   - Select the existing user role that most closely describes the permissions that you want this new role to have.
5. Adjust the permissions.
MANAGING USERS AND USER GROUPS

You view and manage users and user groups in the **Users** folder in the Skybox Admin window.

*To open the Admin window*

› Select **Tools > Administrative Tools > Users**.

You can create users and user groups, and you can edit existing users. You can disable and enable users.

**Default user**

Skybox includes a predefined **Admin** named **skyboxview**. This user cannot be disabled or deleted, and its user name and role cannot be changed. However, you can change its password and other user information.

**External user management**

Usually, users must be explicitly registered in Skybox, but you can have LDAP users work with Skybox without registering them (see **Managing users externally using LDAP (on page 74)**).

**User groups**

Skybox supports groups for users, so that you can group users in any way that is convenient for your organization.

The user group **All Users** is a predefined group that includes all defined users; it cannot be modified or deleted.

*To create a user group*

› Right-click the **Users** node in the Admin tree and select **New Group**.

The properties of user groups are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Group Name</td>
<td>A name for this user group.</td>
</tr>
<tr>
<td>Assign to LDAP Group</td>
<td>The field is displayed only if <strong>LDAP authentication is enabled</strong> (see page 74).</td>
</tr>
<tr>
<td></td>
<td>If users are managed using LDAP, specifies the name of the LDAP group or groups to match to the Skybox user group.</td>
</tr>
<tr>
<td></td>
<td>Specify the LDAP group name or use a comma-separated list. You can use * as a wildcard in the group names.</td>
</tr>
<tr>
<td></td>
<td>Use <strong>Any</strong> rather than specifying a specific group name if the group is intended for all LDAP-managed users.</td>
</tr>
<tr>
<td></td>
<td>See also <strong>Setting up Skybox user groups for LDAP users (on page 75)</strong>.</td>
</tr>
</tbody>
</table>
Property | Description
---|---
Default Role | This field is displayed only if LDAP authentication is enabled (see page 74). If users are managed using LDAP, specifies the Skybox role for those users.
Note: If LDAP users belong to multiple Skybox groups, the highest default role is used.

Group Members | The users who are members of the group.

Default Member | If a ticket is promoted to the user group, Skybox assigns it to the selected user.

User Comments | Information to be listed next to the User Group name when the Users node is selected in the workspace.

VC Permissions | Note: This tab is displayed only if permissions are enabled in Tools > Options > User Settings > User Permissions.

Filter By | Specifies whether to provide permissions for Skybox Vulnerability Control based on Business Units or locations.

(Permission) Each permission consists of:
- Type: Business Unit or Location
- Entity Name: The name of the Business Unit or location
- Path: The path of the Business Unit or location in the tree

FA Permissions | Note: This tab is displayed only if permissions are enabled in Tools > Options > User Settings > User Permissions.

(Permission) Each permission consists of:
- Entity Name: The name of the firewall folder
- Path: The path of the firewall folder in the tree

NA Permissions | Note: This tab is displayed only if permissions are enabled in Tools > Options > User Settings > User Permissions.

(Permission) Each permission consists of:
- Entity Name: The name of the location, network, or asset
- Path: The path of the entity in the tree

CM Permissions | Used to set permissions for the user group for phases in workflows. Non-Admin users in user groups can only work with tickets in phases for which they have permissions.
Note: This tab is displayed only if permissions are enabled in Tools > Options > User Settings > User Permissions.

(Permission) Each permission consists of a workflow or a specific phase in a workflow.

To add a user to a user group

To add a user to a group, right-click the group in the tree and select New User.
To add existing users to a group, select the users, right-click, and then select **Add to User Group**.

To add an existing user to a group, right-click the group in the tree, select **Properties**, click the **Browse** button next to the **Group Members** field, and then select the desired user.

**To change the properties of a user group**

Right-click the group in the tree and select **Properties**.

You can rename the group, change the comment, or change the group’s permissions (see page 70) in Firewall Assurance, Vulnerability Control, and Change Manager if permissions are enabled.

**To delete a user group**

Right-click the group in the tree and select **Delete**.

Users who were members of the group can be accessed in the **All Users** group.

**Users**

All users are members of the **All Users** group, even if you create them as members of other groups. A user can belong to many user groups.

**To create a user**

In the Admin tree, right-click the user group in which to create the user and select **New User**.

The properties of users are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Externally Managed</td>
<td>This field is displayed only if <a href="#">LDAP authentication is enabled</a>. Specifies whether this user is managed using LDAP.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users who are managed in LDAP are added to the Skybox user table on their 1st login. Their properties are updated every time that they log in to Skybox.</td>
</tr>
<tr>
<td>User Name</td>
<td>The name this user must use when logging in to Skybox. This value identifies the user in Skybox and is used, for example, to assign ticket owners or to assign recipients of alerts or reports.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For users who are authenticated using SiteMinder or LDAP, type the user name for the external authentication system.</td>
</tr>
<tr>
<td>Role</td>
<td>Sets the user permissions in Skybox (see <a href="#">User roles</a> on page 58).</td>
</tr>
<tr>
<td>First Name</td>
<td>User first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>User last name.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>The method to use for authenticating this user (Skybox, LDAP, RADIUS, or SiteMinder).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is enabled only if an external authentication system is enabled.</td>
</tr>
</tbody>
</table>
### Property Description

Authentication system is enabled ([Tools > Options > Server Options > User Settings > Authentication](#)). For additional information, see [Working with external authentication systems](#) (on page 72).

### Password

The password this user must use when logging in to Skybox. The password must contain at least 8 characters, including:
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 digit
- At least 1 non-alphanumeric symbol

The password must not contain the user name and it must not contain 5 or more characters that match the previous password.

**Note:** This field is disabled for users with non-Skybox authentication and for **Recipients**.

### Confirm Password

Confirmation of the password.

### Password Never Expires

Specifies whether the user can always log in with the same password.

### Password Expiration Date (Read-only)

User passwords expire 60 days after the 1st login using that password. The next time the user logs in after password expiration, they must change the password.

Expiration dates are not displayed for users whose passwords are marked as **Password Never Expires** or for users who are externally authenticated.

### Email

An email address for the user.

**Note:** If you do not provide an email address for the user and Skybox tries to send the user a report or an alert, the report or alert is not sent, and a message is written to the debug and server logs.

### Department

The user’s department in your organization.

### Phone #

A phone number where the user can be reached.

### Last Login

The most recent time that the user logged in to Skybox.

### User Groups

The user groups of which this user is a member.

### User Comments

Additional information about the user.

### VC Permissions

**Note:** This tab is displayed only if user permissions are enabled.

### Filter By

Specifies whether to provide permissions for Skybox Vulnerability Control based on Business Units or locations.

<table>
<thead>
<tr>
<th>(Permission)</th>
<th>Each permission consists of:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type: Location or Business Unit</td>
</tr>
<tr>
<td></td>
<td>Entity Name: The name of the Business Unit or location</td>
</tr>
<tr>
<td></td>
<td>Path: The path of the location or Business Unit in the tree</td>
</tr>
<tr>
<td></td>
<td>Group Permissions: (Read-only) The name of the user groups from which the user gets this permission</td>
</tr>
</tbody>
</table>
Chapter 15  User management

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| **FA Permissions** | **Note**: This tab is displayed only if user permissions are enabled.  
(Permission) Each permission consists of:  
• Entity Name: The name of the firewall folder  
• Path: The path of the firewall folder in the tree  
• Group Permissions: (Read-only) The name of the user groups from which the user gets this permission |
| **NA Permissions** | **Note**: This tab is displayed only if user permissions are enabled.  
(Permission) Each permission consists of:  
• Entity Name: The name of the location, network, or asset  
• Path: The path of the entity in the tree  
• Group Permissions: (Read-only) The name of the user groups from which the user gets this permission |
| **CM Permissions** | Used to set permissions for the user for phases in workflows. Non-Admin users can only work with tickets in phases for which they have permissions.  
**Note**: This tab is displayed only if permissions for Change Manager are enabled in **Tools > Options > User Settings > User Permissions**.  
(Permission) Each permission consists of:  
• Phase: The phase of the workflow. For **Web Ticket Requestors**, no phases are selected; the permission is for the first and last phase of the selected workflow.  
• Workflow: The name of the workflow  
• Group Permissions: (Read-only) If the permission was assigned to a user group and not directly to the user, the name of the user group from which this permission was inherited |

To update the properties of a user

▷ Right-click the user in the Table pane and select **Properties**.  
You cannot rename existing users, but you can change all other user properties.

To add users to a user group

▷ Select the users, right-click, and select **Add to User Group**.

To disable or enable a user

▷ Right-click the user name and select **Disable** or **Enable**.  
A disabled user cannot log in to Skybox and does not receive any Skybox emails (alerts or reports). Disabling a user has no effect on their tickets or on policies that the user owns; these are not reassigned to different users.
To delete a user

- Right-click the user in the Table pane and select **Delete**.
  
  If the user owns tickets or policies, select a new owner.

To change a user password

- Right-click the user in the Table pane and select **Change Password**.
  
  The user can use their current password for the next login but is asked to change the password as part of the login process.

Note: You can only change passwords of users who are authenticated and managed internally.

Permissions

Note: Permissions are available for Firewall Assurance, Network Assurance, Vulnerability Control, and Change Manager; permissions for Firewall Assurance, Network Assurance, and Vulnerability Control are disabled by default.

After permissions are enabled (see page 126), **Admins** can specify permissions for each user group and for each user. It is preferable to specify group-wide permissions on user groups, and specific permissions only on users who require separate permissions or are not part of a group.

- Firewall Assurance users can view firewall folders (and their firewalls) in the Firewall Assurance tree according to their permissions and the permissions specified for the groups to which they belong.
- Network Assurance users can view locations, networks, and assets in the Network Assurance tree according to their permissions and the permissions specified for the groups to which they belong.
- Vulnerability Control users can view Business Units and locations (and their subentities) according to their permissions and the permissions specified for the groups to which they belong:
  - The Exposure tree is filtered to include only the attacks and exposed vulnerability occurrences related to the user’s permitted Business Units.
  - Analysis views are filtered to list only permitted entities.
  - In Access Analyzer queries, users can select the source and destination from their permitted locations and Business Units only. The query results are filtered to display only entities from their permitted locations and Business Units.
  - The security metrics tree is filtered to include only the user’s permitted Business Units.
- Change Manager users can edit tickets (change requests) in specific ticket workflows and phases according to their permissions and the permissions specified for the groups to which they belong.
- Change Manager **Ticket Requestor** users can edit their own tickets in the first and last phases only.
Enabling and disabling permissions

To enable or disable permissions

1. From the **Tools** menu, select **Options > Server Options > User Settings > User Permissions**.
2. Select the required permissions:
   - Permissions for Firewall Assurance, Network Assurance (Access Analyzer) & Vulnerability Control
   - Permissions for Change Manager

Managing permissions

After permissions are enabled, you must specify them for each user or user group.

If no permissions are specified for a user or any of that user’s groups, the user cannot:

- View any firewall folders (in Firewall Assurance)
- View any Business Units or locations (in Vulnerability Control)
- View or edit any Change Request tickets (in Change Manager)

Note: **Admins** have full permissions for all entities; no configuration is required.

To specify permissions for a user or user group

1. Right-click the user or group in the Admin tree and select **Permissions**.
2. Specify the permissions for the user or group:
   - In the **VC Permissions** tab, specify the Business Units and locations that this user or group can view.
   - In the **FA Permissions** tab, specify the firewall folders that this user or group can view.
   - In the **NA Permissions** tab, specify the locations, networks, and assets that this user or group can view.
   - In the **CM Permissions** tab, specify the workflow phases (of Access Change tickets) that this user or group can edit or view.

Unlocking a locked user

Local users who try unsuccessfully to log in get locked out after 3 attempts.

Locked users are shown as in the **Locked** column of the list of users.

An administrator can unlock a locked user before the defined lockout time is reached.

To unlock a user

- Right-click the user in the Table pane and select **Unlock**.
Disabling and deleting inactive user accounts

Skybox provides an option whereby users who are inactive for a specified period are automatically disabled and then deleted from Skybox after an additional period. The option is disabled by default.

To disable users automatically

1. From the Tools menu, select Options > Server Options > User Settings > Disabling Inactive Users.
2. Define the period after which inactive users are disabled, and the period after which users who have remained inactive are deleted from Skybox.
3. Specify the user to receive all tickets belonging to users who were disabled or deleted.

WORKING WITH EXTERNAL AUTHENTICATION SYSTEMS

By default, the Skybox internal authentication mechanism authenticates users, but you can set up Skybox to work with the following external authentication systems:

- LDAP, including Microsoft Active Directory
- RADIUS
- CA SiteMinder®
- SAML 2.0 (for Skybox web client SSO)

When Skybox is integrated with these systems, their users log in to Skybox using their SiteMinder, RADIUS, SSO, or LDAP user name and password, and the external system authenticates them. All other user management (for example, setting up user groups and permissions) is done either in Skybox or using an external user management system (which is separate from the external authentication system).

Note: You can use a mixed authentication mode, where some users authenticate against Skybox and others authenticate against an external system. The skyboxview user can only log in to Skybox using Skybox authentication.

To set up Skybox to use external authentication (other than SAML)

1. Go to Tools > Options > Server Options > User Settings > Authentication.
2. Select Support External Authentication and then select the external authentication to use.
3. Fill in the fields as described in Authentication (on page 120).

For information about setting up Skybox to use SAML authentication, see Enabling user management via SAML (SSO) authentication (on page 73).

Handling expired passwords

If a user who is authenticated in an external system tries to log in to the Skybox web interface with an expired password (or using a locked account), Skybox can display a message specifying what happened and a link to the appropriate URL.
To add a link, modify the following properties in
<Skybox_Home>\server\conf\sb_server.properties:

- `webapp_login_expired_message_link`
- `webapp_login_expired_message_label=Account Management`

If there is no value for the link, nothing is displayed when a user with an expired
password or locked account tries to log in. Otherwise, `webapp_login_expired_message_label` is displayed and points to
`webapp_login_expired_message_link`.

Enabling user management via SAML (SSO) authentication

Enabling Skybox web client users to log in via their organization's Single Sign On
(SSO) system, such as Okta, requires setup of the SSO and of Skybox.

Setting up the SSO

Configure the SSO as specified in the following example, replacing `<server>`
with the Skybox Server's DNS name or IP.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion
   xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
   Version="2.0">
   <saml2:Subject>
       <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userName</saml2:NameID>
       <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
       </saml2:SubjectConfirmation>
   </saml2:Subject>
       <saml2:AudienceRestriction>
       </saml2:AudienceRestriction>
   </saml2:Conditions>
       <saml2:AuthnContext>
       </saml2:AuthnContext>
       <saml2:AuthnStatement>
           <saml2:Attribute Name="email"
               NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
               <saml2:AttributeValue
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xsi:type="xs:string">user.email</saml2:AttributeValue>
           </saml2:Attribute>
           <saml2:Attribute Name="samaccountname"
               NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
               <saml2:AttributeValue
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xsi:type="xs:string">user.samaccountname</saml2:AttributeValue>
           </saml2:Attribute>
       </saml2:AuthnStatement>
   </saml2:AuthnStatement>
</saml2:Assertion>
```
Note: The line `<saml2:AttributeValue
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">"ADMIN"
</saml2:AttributeValue>
</saml2:Attribute>
</saml2:AttributeStatement>
</saml2:Assertion>` logs the users in to Skybox as admins. If it is empty, users will be given the default role defined in `sb_server.properties` (see below).

**Setting up Skybox**

1. Obtain the SSO’s URL and certificate (.CERT file).
2. Put the certificate in a temporary directory on the server.
3. Run the following keytool command, where `okta.cert` is the certificate from step 2:
   ```
   keytool -importcert -file okta.cert -keystore saml.jks -alias saml
   ```
4. When prompted, enter the keystore password.
5. Re-enter the keystore password.
7. Configure the following properties in `<Skybox_Home>/server/conf/sb_server.properties`:
   - `saml2_provider_name=`
     This is the SAML message to display on the Login page. For example: "Login via external SSO provider"
   - `saml2_provider_service_url=`
     Use the URL from step 1 above. This is the direct access URL to the SSO.
   - `saml2_default_user_role=READONLY`
     This is the default user role for all users logging in to Skybox via the SSO.
8. Restart the Skybox Server.

**MANAGING USERS EXTERNALLY USING LDAP**

You can enable LDAP users to log in to Skybox. Skybox supports Active Directory 2003 and higher, as well as generic LDAP servers. Multiple servers can be configured to support multiple domains.
To integrate an external user management system with Skybox

1. **Enable user management using LDAP** (see page 75).
2. **Set up Skybox user groups for the LDAP users** (see page 75).
   These user groups define the role of the LDAP users in Skybox.

**Enabling user management using LDAP**

**To enable user management using LDAP**

1. Go to **Tools > Options > Server Options > User Settings > Authentication**. Make sure that at least 1 LDAP server is defined.
2. Go to **Tools > Options > Server Options > User Settings > External User Management**.
3. Select **LDAP**.
4. Click **Configure**.
5. Type the **Global User** and **Global Password**.
6. If you want LDAP users to authenticate using RADIUS, set **Default authentication Method** to RADIUS.

**Setting up Skybox user groups for LDAP users**

Set up Skybox user groups for all LDAP users who log in to Skybox, so that when users log in, Skybox knows how to manage them and the permissions that they have.

If all LDAP users have the same Skybox user role, you can create a single Skybox user group to match all LDAP user groups.

**To set up a Skybox user group for LDAP users**

1. Create a new user group in Skybox.
2. In the **Assign to LDAP Groups** field, type the comma-separated names of the LDAP user groups to associate with this Skybox group.
   The following example demonstrates how to use * as a wildcard in this field to match multiple user groups.
3. In the **Default Role** field, select the role to which these users are assigned when they are working in Skybox.

If there are several groups of LDAP users and they require different roles (that is, different permissions) in Skybox, create a separate Skybox group for each Skybox role that is used.

**Default group**

There are 2 ways to enable all Active Directory users to log in to Skybox:

- Create a group in Skybox. Next to the **Assign to LDAP Group** field, select **Any**.
- Create a group in Skybox. In the **Assign to LDAP Group**, specify the default LDAP user group in your organization; in most cases, this is **Default Users**.

In `<Skybox_Home>\server\conf\sb_server.properties`, set the
You can then assign the necessary permissions to the Skybox group.

**LDAP users who are members of multiple LDAP user groups**

If an LDAP user is a member of several LDAP groups, each of which matches a separate Skybox group, the LDAP user becomes a member of all the matching Skybox groups.

**Example**

Skybox includes the user groups listed in the following table for LDAP users.

<table>
<thead>
<tr>
<th>Skybox group</th>
<th>Assigned to LDAP group whose name matches this pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupA</td>
<td>*</td>
</tr>
<tr>
<td>GroupB</td>
<td>Dev*</td>
</tr>
<tr>
<td>GroupC</td>
<td>IT*</td>
</tr>
<tr>
<td>GroupD</td>
<td>USA*_hr</td>
</tr>
<tr>
<td>GroupE</td>
<td>USA*admin or IT_World</td>
</tr>
</tbody>
</table>

In this organization, if an LDAP user is a member of the IT_Europe, IT_World, and Everybody LDAP user groups, then in Skybox, this user is a member of the GroupA, GroupC, and GroupE Skybox user groups.

**Authentication to a super domain**

If Active Directory includes multiple forests, you can represent the domain name in Skybox using an asterisk in the `LDAP_root_DN` property. The asterisk is replaced by the domain name. In such cases, the user must login with `<domain name>\<user name>`.

**CHANGING THE PASSWORD FOR DATABASE CLIENTS**

This section explains how to change the database password for database clients.

Default passwords after installation are:

- User: root       Password: manager
- User: skyboxview Password: skyboxview

To change the database password

1. Shut down the Skybox Server.
2. Make sure that MySQL is running.
3. In SQLyog or another SQL client, connect as root and run the following commands to set the new password:

   - For the root user:
     ```sql
     ALTER USER 'root'@'localhost' IDENTIFIED BY '<new root password>';
     ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY '<new root password>';  
     ```
ALTER USER 'root'@':1' IDENTIFIED BY '<new root password>';  
• For the skyboxview user:  
  ALTER USER 'skyboxview'@'localhost' IDENTIFIED BY '<new Skybox password>';  
  ALTER USER 'skyboxview'@'127.0.0.1' IDENTIFIED BY '<new Skybox password>';  
  ALTER USER 'skyboxview'@':1' IDENTIFIED BY '<new Skybox password>';  
  ALTER USER 'skyboxview'@'localhost.localdomain' IDENTIFIED BY '<new Skybox password>';  

4 In <Skybox_Home>\server\conf\sb_server.properties, update the values of the following properties with the new passwords (as clear text values):  
  • For the root user: secret.db_administrator_password  
  • For the skyboxview user: secret.db_client_password  

The values are encrypted in SHA2 and AES256 when the Server boots.
Chapter 16

Backup and restore

This chapter explains how Admins can back up and restore the model.

In this chapter

Backup and restore scenarios ............................................... 78
About the model .................................................................. 78
Backing up the model ......................................................... 79
Fast backup ....................................................................... 81
Backing up to an external location ........................................ 81
Loading a model ................................................................. 81
Restoring the model ........................................................... 82

BACKUP AND RESTORE SCENARIOS

This chapter explains how to prepare for and deal with:

› Restoring the model on a working Server
  You can load an old version of the model to see how the network looked some time ago (for example, to compare it to the current network or to view the properties of specific devices)
  To be able to restore the model, back it up on a regular basis as described in Backing up the model (on page 79).

› Restoring a Skybox Server following a hardware failure (disaster recovery)
  To be able to restore a Server, back up all relevant data (not the Skybox model only) to another location on a regular basis. This data includes:
  • Skybox Server configuration files
  • The Skybox model
  • Skybox property (configuration and settings) files
  • Attachments
  • Device certificates
  • Reports
  For additional information, see Backing up to an external location (on page 81) and Restoring the model (on page 82).

ABOUT THE MODEL

Skybox can maintain up to 3 model instances in the Skybox database:
The Live model represents the current state of your network. It is updated by automated data collection activities.

Use the What If model for validating changes virtually and checking possible scenarios. It is generated from the Live model.

Changes made to the What If model are not copied to the Live or Forensics models.

The Forensics model is a snapshot of an earlier model that you can load for comparison or review.

Back up and load each model separately. In general, changes made to one model are not copied to the other models; the only exception is that any changes in the structure of the Access Policy are made in all the models.

Using Skybox Manager, you can switch between models at any time. Different users can work with the same or different models simultaneously.

BACKING UP THE MODEL

You back up the model in XMLX (encrypted XML) format. If fast backup (see page 81) is enabled, you can back up in SQLX (encrypted SQL) format.

When you back up the model, you can choose any of 4 components: Model, Task and Report Definitions, Users, and Dictionary. Only the selected components are saved, and only these components can be loaded from the file.

Backing up the model using tasks

You can back up the Live model using a task of type Backup Model and Settings. The task saves the model itself and Skybox settings files.

The model is saved as
<br>\(<\text{Skybox}_\text{Home}\>\text{data}\text{xml\_models}\text{xml\_backup\_task\_<date>\--\<time>}\text{.xmlx}</br>

The settings files are saved as
<br>\(<\text{Skybox}_\text{Home}\>\text{data\settings\_backup\settings\_backup\_<date>\--\<time>\text{.zip</br>

Schedule a task (for example, the predefined Backup Data – Weekly task) to back up the Live model on a weekly basis. You can change the schedule so that the task runs daily rather than weekly.

You can add a custom list of additional files and directories to be backed up by the task. Specify these files and directories in <Skybox_Home>\server\conf\user_backup_list.txt. Instructions and format examples are included in the file.

Backing up the model manually

You can back up all models manually. When you back up a model manually, no settings files are saved.

To back up a model manually

1. Select File > Models > Save.
2. In the Save Model dialog box:
   a. Select the model to back up (Live, What If, or Forensics).
b. Type a name for the file.

c. Clear any types of data that you do not want to back up.

d. To back up an additional copy of the model to the Manager file system, select **Save copy to a local directory** and specify a directory.

e. To save the model for Skybox support, select **Save without credentials and passwords**.

   Note: This feature removes important information (user names and passwords in Skybox tasks) and should only be used if you need to send the model to Skybox support.

f. Click **OK**.

   The file is saved (on the Server) in `<Skybox_Home>\data\xml_models` with the extension `.xmlx`. If you are using fast backup, the file is saved in `<Skybox_Home>\data\sqlx_models` with the extension `.sqlx`.

   If you selected **Save copy to a local directory**, the file is also saved in the directory that you specified.

   The properties of the Save Model / Load Model dialog box are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>The type of model to be backed up or loaded.</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>This field is displayed only if fast backup (see page 81) is enabled.</td>
<td>Fast backup (see page 81) is an advanced option that should only be used with the guidance of Skybox Professional Services.</td>
</tr>
<tr>
<td></td>
<td>The backup type.</td>
<td></td>
</tr>
<tr>
<td>File Name (Save Model only)</td>
<td>(Save Model only) Type a name for the file to contain the backup.</td>
<td></td>
</tr>
<tr>
<td>File (Load Model only)</td>
<td>(Load Model only) Select the file to load.</td>
<td></td>
</tr>
<tr>
<td>Save Scope / Load Scope</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td>Specifies whether to back up or load the main part of the model, including all network, security, and business data.</td>
<td></td>
</tr>
<tr>
<td>Tasks and Report Definitions</td>
<td>Specifies whether to back up or load tasks and report definitions (which are not part of the model).</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>Specifies whether to back up or load users existing in Skybox.</td>
<td></td>
</tr>
<tr>
<td>Dictionary</td>
<td>Specifies whether to back up or load the Skybox Vulnerability Dictionary. Usually, this is unnecessary; it is better to update the Dictionary (see page 138).</td>
<td></td>
</tr>
<tr>
<td>Save copy to a local directory</td>
<td>(Save Model only) Specifies whether to back up an additional copy of the model to the Manager file system and the backup location.</td>
<td></td>
</tr>
<tr>
<td>Save without credentials and passwords</td>
<td>(Save Model only) Specifies whether to save the model without user names and passwords for Skybox tasks.</td>
<td>Note: Do not use this option when backing up the model for your organization; it is intended only for sending the</td>
</tr>
</tbody>
</table>
FAST BACKUP

*Fast backup* saves the model as a SQLX (encrypted SQL) file. This backup is much faster than the regular (XMLX) backup and is intended for situations where large models must be saved frequently.

**Turning on fast backup**
The fast backup option is hidden by default.

*To turn on fast backup*

- In `<Skybox_Home>\server\conf\sb_server.properties`, set `db_sqlx_backup_mode` to `true`.

**Using fast backup**
To use fast backup, select the fast backup (SQLX) option in **Backup Model and Settings** tasks or when saving the model manually via **File > Save > Model**.

*Note: We recommend that you save the model using regular (XMLX) backup on a regular basis (at least once a week) in addition to the fast backups, so that you can use this model after an upgrade.*

BACKING UP TO AN EXTERNAL LOCATION

We recommend that you back up (copy) the model and related data to an external location on a regular basis, so that you can restore the model after a disaster or if you need to uninstall and reinstall the Server for any reason.

*To back up the model*

1. Run a **Backup Model and Settings** task to back up the model. Files generated using the task include a timestamp in their name.
2. Back up the following directories (on the Server machine) to an external location:
   - `<Skybox_Home>\data\xml_models`
   - `<Skybox_Home>\data\sqlx_models` (when using fast backup)
   - `<Skybox_Home>\data\settings_backup` *(created in step 1; it contains tasks, report definitions, users, system settings, ticket attachments, and recent reports)*

LOADING A MODEL

You can load a backed-up model to the What If or Forensics model for additional investigation or to try out changes. You can reload the most recent model to the Live model after a system crash or other problem that made the Skybox database unusable.

You can load XMLX backups of the model even after upgrading Skybox to a newer version.
To load a model
1. Select **File > Models > Load**.
2. In the Load Model dialog box:
   a. Select the model (**Live, What If, or Forensics**) to which you want the file loaded.
   b. Select the file to load.
      If there are many files, use the date filter to narrow your selection.
   c. If necessary, change the parts of the data to load.
   d. Click **OK**.

RESTORING THE MODEL
You can restore the model on any machine on which the Skybox Server is installed.

To restore the model
1. Make sure that the Skybox Server and Collector are not running.
2. (Linux only) Make sure that the system account **skybox** exists on the Server machine.
3. Copy the latest versions of **xml_backup_task_<date>--<time>.xml** (or **sql_backup_task <date>--<time>.sql**) and **settings_backup_<date>--<time>.zip** from the external location where you saved them.
4. Run the **restore_settings** utility, providing the location of **settings_backup_<date>--<time>.zip** as an argument:
   - (Windows) `<Skybox_Home>/server/bin/restore_settings.bat`
   - (Linux) `<Skybox_Home>/server/bin/restore_settings.sh`
5. If Skybox Collectors are running on any other machines:
   a. Copy **settings_backup_<date>--<time>.zip** to each Collector machine.
   b. Run the **restore_settings** utility on each Collector machine.
6. Create and start the Skybox Server and Collector services:
   - On Windows, run:
     - `<Skybox_Home>/server/bin/install-server-service.bat`
     - `<Skybox_Home>/server/bin/install-collector-service.bat`
     - `<Skybox_Home>/server/bin/startserver.exe`
     - `<Skybox_Home>/collector/bin/startcollector.exe`
   - On Linux, run (as root):
     - `<Skybox_Home>/server/bin/install_service_server.sh`
     - `<Skybox_Home>/server/bin/install_service_collector.sh`
     - `service sbvserver start`
     - `service sbvcollector start`
7 Log in to Skybox Manager as the **skyboxview** user.

8 Select **File > Models > Load**. In the Load Model dialog box, select the Live model and select the file that you restored in step 3. The system is now fully restored.
Chapter 17

Administration via CLI commands

You can perform some common administrative tasks either via the Manager or via utilities run from the command line.

This chapter documents the CLI utilities.

Launch utilities from `<Skybox_Home>\server\bin` unless otherwise noted. In Windows, commands are run with a `bat` extension; in Linux, with an `sh` extension.

In this chapter

Package firewall configurations ............................................. 84
Launch tasks ...................................................................... 85
Load the latest Dictionary (deprecated) ......................... 85
Package log files ................................................................. 85
Scan log files ...................................................................... 86
Save the model to an XML file .............................................. 90
Load the model from an XML file ........................................... 91
Save the model to a SQL file ................................................ 92
Load the model from a SQL file ............................................. 92
Restore model settings ......................................................... 93

PACKAGE FIREWALL CONFIGURATIONS

The `firewall_config` utility packages firewall configuration files into ZIP files that you can send to Skybox for troubleshooting.

The output is split into 5 MB ZIP files; the files are named `firewall1_<date>_<organization name>.zip`, `firewall2_<date>_<organization name>.zip`, and so on.

Syntax

```
firewall_config [-s] [-c <case ID>] [-f "<list of firewall IDs>"]
[-g <number of generations>]
```

Arguments

The arguments of this command are described in the following table.
**Chapter 17    Administration via CLI commands**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c &lt;case ID&gt;</td>
<td>A string value representing the support case number. This string is added to the name of the output files. For example, if the support case number is 12345, the 1st file is named <code>firewall1_&lt;date&gt;_organization_name_12345.zip</code>.</td>
</tr>
</tbody>
</table>
| -f <firewall IDs> | (The *EID* is the Skybox ID number of the firewall in the model.) A comma-separated list of firewall EIDs. The list must be enclosed in double quotes. To find the EID of a firewall:  
  • Open the Manager to any table of firewalls; right-click in the header row of the table and select **Customize Current View**; select **EID** from the list of possible columns. |
| -g <generations> | The number of generations of firewall configuration files to include in the ZIP file. The default value is 2. |
| -s          | Generate a single ZIP file even if the output is over 5 MB.                                                                                  |

**LAUNCH TASKS**

The *launchtask* utility launches a Skybox task.

Specify the name of the task. If the name includes spaces, surround it with double quotes.

**Syntax**

```bash
launchtask.bat "<task name>"
```

**LOAD THE LATEST DICTIONARY (DEPRECATED)**

*Note: This utility is deprecated starting in version 10.0.200.*

The *loaddictionary* utility loads the latest Skybox Vulnerability Dictionary from the internet.

This utility has no arguments.

**Syntax**

```bash
loaddictionary.bat
```

**PACKAGE LOG FILES**

The *packlogs* utility packages relevant log and properties files for all Skybox components installed on the selected machine (and, optionally, the latest saved model) into a ZIP file that you can send to Skybox for troubleshooting.

If the Skybox Server, the Skybox Collector, and Skybox Manager are on separate machines, you must run the utility separately for each component. The utility is in the *bin* directory of each product (*<Skybox_Home>\<<component>>\bin*, where `<component>` is `server`, `collector`, or `app`).
The output file is named `<component>_packlogs_<date>_<organization name>[_caseID].zip`

**Syntax**

```
packlogs [-s | -p] [-c <case ID>] [-o <offset>] [-m | -q]
```

**Arguments**

The arguments of this command are described in the following table.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-m</code></td>
<td>Include the latest XMLX model found under <code>&lt;Skybox_Home&gt;\data\xml_models</code>. If you specify <code>-m</code> and <code>-q</code>, the utility packages the latest SQLX model only.</td>
</tr>
<tr>
<td><code>-q</code></td>
<td>Include the latest SQLX model found under <code>&lt;Skybox_Home&gt;\data\sqlx_models</code>.</td>
</tr>
<tr>
<td><code>-c &lt;case ID&gt;</code></td>
<td>A string value representing the support case number. This string is added to the name of the output files.</td>
</tr>
<tr>
<td><code>-o &lt;offset&gt;</code></td>
<td>A numeric offset limiting the age of log files to include in the ZIP files. The log files are limited to those created or modified within the previous specified number of days. The default value is 30.</td>
</tr>
<tr>
<td><code>-p</code></td>
<td>Split the output into ZIP files of 5 MB or less; the files are named: <code>&lt;component&gt;_packlogs1_&lt;date&gt;_&lt;organization name&gt;.zip</code>, <code>&lt;component&gt;_packlogs2_&lt;date&gt;_&lt;organization name&gt;.zip</code>, and so on.</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>(Default) Generate a single ZIP file.</td>
</tr>
</tbody>
</table>

**SCAN LOG FILES**

The `scanlogs` utility scans the content of any packlogs ZIP file found in the same local directory and lists any system issues that were found.

The utility, which is in `<Skybox_Home><component>\bin` (where `<component>` is server, collector, or app), has no arguments.

**Syntax**

```
scanlogs
```

The issues listed in the following table can be detected using this utility.

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OOM incidents</td>
<td>These are cases where the Java process ran out of memory. Each such incident is documented in a histogram file that lists the counts of and memory used by all instantiated Java class types.</td>
<td>If the OOM incidents are recent and have occurred multiple times, open a bug for Skybox R&amp;D</td>
</tr>
<tr>
<td>#</td>
<td>Name</td>
<td>Description</td>
<td>Comments</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>High thread count</td>
<td>A high thread count means that the Java process is overloaded and trying to handle too many concurrent execution flows. This may cause a slowdown or even total hang in extreme cases.</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td>3</td>
<td>JVM crash incidents</td>
<td>The Java process often creates a crash file just before it unexpectedly shuts down. A crash might indicate memory issues, OS issues, Java software bugs, or even hardware instability.</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td>4</td>
<td>Encrypted or corrupted packlogs files</td>
<td>The scanner failed to unzip a packlogs file. This may happen either because the file is protected with a password, or because it is truncated or corrupted.</td>
<td>Try to unzip the file manually and contact the file sender</td>
</tr>
<tr>
<td>5</td>
<td>Long debug lines</td>
<td>Very long debug lines indicate that very large data is being mistakenly written into the debug log.</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td>6</td>
<td>Debug message flood</td>
<td>The debug log files might be rotating very fast, with too many debug messages being written in a very short time.</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td>7</td>
<td>Low RAM size</td>
<td>The host machine has a relatively small RAM. This may cause OOM incidents.</td>
<td>If the host is a virtual machine, the RAM can be easily increased. Otherwise, contact Skybox Professional Services</td>
</tr>
<tr>
<td>8</td>
<td>Low swap size</td>
<td>The host machine has a small swap space, which might cause instability if memory use spikes. On Linux, this might trigger OOM killer incidents that can be seen in /var/log/messages.</td>
<td>The error can be ignored if no other symptoms are present. Otherwise swap space should be modified (if necessary, contact Skybox Professional Services).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• On Windows, the swap area should default to automatic management.</td>
<td>• On Windows, the swap area should default to automatic management. • On Linux, set 8 GB swap on 32 GB RAM, 32 GB swap on 128 GB RAM.</td>
</tr>
<tr>
<td>9</td>
<td>Low disk space</td>
<td>A partition on the host machine is nearing its disk capacity.</td>
<td>Depending on which partition is reported, consult Skybox Professional Services. <strong>Important:</strong> If the partition is hosting a Skybox installation, the issue is of critical importance.</td>
</tr>
<tr>
<td>#</td>
<td>Name</td>
<td>Description</td>
<td>Comments</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>Corrupt property files</td>
<td>A Skybox property file was corrupted.</td>
<td>Contact Skybox Professional Services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The file may have to be restored from backup.</td>
</tr>
<tr>
<td>11</td>
<td>Slow tasks</td>
<td>Extremely slow tasks.</td>
<td>Contact Skybox Professional Services.</td>
</tr>
<tr>
<td>12</td>
<td>Low Xmx</td>
<td>The Server may be misconfigured to use a low Xmx memory limit in jvmargs.properties, although the host machine has much more RAM available.</td>
<td>Contact Skybox Professional Services.</td>
</tr>
<tr>
<td>13</td>
<td>High Xmx</td>
<td>The Server may be misconfigured to use a high Xmx memory limit in jvmargs.properties, but the host machine has much less RAM available.</td>
<td>Contact Skybox Professional Services.</td>
</tr>
<tr>
<td>14</td>
<td>MySQL crash incidents</td>
<td>MySQL usually leaves evidence in its logs just before it unexpectedly crashes. Possible reasons are varied.</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td>15</td>
<td>Mismatched server Xmx</td>
<td>The effective memory limit that the Server is seeing is not the limit configured in jvmargs.properties. This typically happens on Windows if the Skybox service was not reinstalled after changing the value.</td>
<td>Contact Skybox Professional Services.</td>
</tr>
<tr>
<td>16</td>
<td>Multiple servers</td>
<td>Multiple Servers are running concurrently on the host machine. This may cause strange errors.</td>
<td>Contact Skybox Professional Services.</td>
</tr>
<tr>
<td>17</td>
<td>Multiple collectors</td>
<td>Multiple Collectors are running concurrently on the host machine. This may cause strange errors.</td>
<td>Contact Skybox Professional Services.</td>
</tr>
<tr>
<td>18</td>
<td>Server port already in use</td>
<td>There was a port clash because multiple Servers were running.</td>
<td>If the incident is recent, contact Skybox Professional Services, otherwise ignore.</td>
</tr>
<tr>
<td>19</td>
<td>Collector port already in use</td>
<td>There was a port clash because multiple Collectors were running.</td>
<td>If the incident is recent, contact Skybox Professional Services, otherwise ignore.</td>
</tr>
<tr>
<td>20</td>
<td>Permission denied</td>
<td>There is a file permission issue with the Skybox installation.</td>
<td>Check which user is running the process and verify that their permissions for installation files are appropriate. If necessary, contact Skybox Professional Services.</td>
</tr>
<tr>
<td>#</td>
<td>Name</td>
<td>Description</td>
<td>Comments</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>21</td>
<td>Unknown host</td>
<td>A problem with the DNS setup may cause failed connections. If the error refers to local host name, the DNS settings of the host machine might be incorrect.</td>
<td>Skybox Professional Services should check C:\Windows\System32\drivers\etc\hosts (on Windows) or /etc/hosts (on Linux).</td>
</tr>
<tr>
<td>22</td>
<td>Unassociated entities</td>
<td>There might be a problem in the referential integrity of the Skybox model and a potential corruption to data. This might be caused by sub-entities left behind after the deletion of a parent entity or it could be caused by inadvertent disappearance of model entities.</td>
<td>Usually should be handled as a bug by Skybox R&amp;D to find the root cause.</td>
</tr>
<tr>
<td>23</td>
<td>No daily backups</td>
<td>No daily backups of model data have taken place recently.</td>
<td>Contact Skybox Professional Services</td>
</tr>
<tr>
<td>24</td>
<td>Slow interactive calls</td>
<td>Lists all slow interactive calls from clients. Each call is listed with its most recent duration, and the average duration and number of worst calls processed recently by the server.</td>
<td>Frequent calls that have a long average duration should be handled as a bug by Skybox R&amp;D.</td>
</tr>
<tr>
<td>25</td>
<td>Failed tasks</td>
<td>Lists all Skybox tasks that have failed recently.</td>
<td>Contact Skybox Professional Services</td>
</tr>
<tr>
<td>26</td>
<td>Server logic errors</td>
<td>There are errors in Skybox Server logic. A count of each error type is provided. The severity of this error varies depending on the context and may well be inconsequential.</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td>27</td>
<td>Collector logic errors</td>
<td>There are errors in Skybox Collector logic. A count of each error type is provided. The severity of this error varies depending on context and may well be inconsequential.</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td>28</td>
<td>App logic errors</td>
<td>There are errors in Skybox Manager logic. A count of each error type is provided. The severity of this error varies depending on context and may well be inconsequential.</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td>29</td>
<td>MySQL data truncation</td>
<td>The size of a specific MySQL column is too small for the intended data, which may result in localized data corruption.</td>
<td>Contact Skybox R&amp;D for a temporary MySQL schema workaround and a permanent fix</td>
</tr>
<tr>
<td>30</td>
<td>Server linkage errors</td>
<td>There is a problem with the Java class files of the Server, possibly due to a deployment issue. For example, multiple Servers running, a defective installation, or a build problem.</td>
<td>Contact Skybox Professional Services to check the file integrity, and contact Skybox R&amp;D.</td>
</tr>
<tr>
<td>#</td>
<td>Name</td>
<td>Description</td>
<td>Comments</td>
</tr>
<tr>
<td>----</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>31</td>
<td>Collector linkage errors</td>
<td>There is a problem with the Java class files of the Collector, possibly due to a deployment issue. For example, multiple Collectors running, a defective installation, or a build problem.</td>
<td>Contact Skybox Professional Services to check the file integrity, and contact Skybox R&amp;D.</td>
</tr>
<tr>
<td>32</td>
<td>Server deployment errors</td>
<td>The Server failed to start correctly. There are many possible causes.</td>
<td>Contact Skybox Professional Services</td>
</tr>
<tr>
<td>33</td>
<td>Collector deployment errors</td>
<td>The Collector failed to start correctly. There are many possible causes.</td>
<td>Contact Skybox Professional Services</td>
</tr>
<tr>
<td>34</td>
<td>Server disk space shutdowns</td>
<td>Lists occurrences of Server shutdowns due to lack of free disk space.</td>
<td>Contact Skybox Professional Services</td>
</tr>
</tbody>
</table>

SAVE THE MODEL TO AN XML FILE

The `save2xml` utility saves a Skybox model to an XML file. You can select the parts of the model to save and the model to save; (by default, the Live model is saved).

**Syntax**

```bash
save2xml.bat <file name> [-model] [-core] [-coreusers] [-dic]
[-whatif | -forensics] [-plaintext]
```

The command to export all the information in the Live model and your task definitions is:

```bash
> save2xml.bat <file name> -model -core -coreusers -dic
```

**Arguments**

The arguments of this command are described in the following table.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;file name&gt;</td>
<td>The name of the file in which to save the data. The data is saved as an XML file. (If you include the <code>-plaintext</code> option, the data is saved as an XML file.)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The default path for the file is <code>&lt;Skybox_Home&gt;\data\xml_files</code>. To save the file in a different location, include the full path name.</td>
</tr>
<tr>
<td>-model</td>
<td>Include the main part of the Skybox model, including all network, security, and business data.</td>
</tr>
<tr>
<td>-core</td>
<td>Include task and report definition data from the Skybox model.</td>
</tr>
<tr>
<td>-coreusers</td>
<td>Include user data from the Skybox model.</td>
</tr>
<tr>
<td>-dic</td>
<td>Include the Skybox Vulnerability Dictionary from the Skybox model.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Unless you need this specific Dictionary, do not save it. You can always load the latest Dictionary via</td>
</tr>
</tbody>
</table>
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loaddictionary.bat.</td>
<td></td>
</tr>
<tr>
<td>-forensics</td>
<td>Save the specified data from the Forensics model rather than from the Live model.</td>
</tr>
<tr>
<td>-whatif</td>
<td>Save the specified data from the What If model rather than from the Live model.</td>
</tr>
<tr>
<td>-plaintext</td>
<td>Do not encrypt the XML file.</td>
</tr>
</tbody>
</table>

### LOAD THE MODEL FROM AN XML FILE

The `load` utility loads a saved XML model file to Skybox. You can specify the parts of the model to load and to which model in Skybox to load them.

By default:

- Only the model part is loaded
- Models are loaded to the Live model

### Syntax

```
```

### Arguments

The arguments of this command are described in the following table.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>The name of the model file to load.</td>
</tr>
<tr>
<td>-model</td>
<td>Load the main part of the model, including all network, security, and business data to your Skybox model.</td>
</tr>
<tr>
<td>-core</td>
<td>Load task and report definition data to your Skybox model.</td>
</tr>
<tr>
<td>-coreusers</td>
<td>Load user data to your Skybox model.</td>
</tr>
<tr>
<td>-dic</td>
<td>Load the Skybox Vulnerability Dictionary (from the file) to the Live model in Skybox.</td>
</tr>
<tr>
<td>-whatif</td>
<td>Load the specified data to the What If model rather than the Live model in Skybox.</td>
</tr>
<tr>
<td>-forensics</td>
<td>Load the specified data to the Forensics model rather than the Live model in Skybox.</td>
</tr>
</tbody>
</table>
SAVE THE MODEL TO A SQL FILE

The sqlxdump utility saves a Skybox model to a SQLX file. You can select whether to exclude specific data, and the model to save (by default, the Live model is saved).

**Syntax**

```
```

**Arguments**

The arguments of this command are described in the following table.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-noserver</td>
<td>Run the command directly in MySQL, bypassing the server.</td>
</tr>
<tr>
<td>-exclude_rua</td>
<td>Do not save rule usage analysis data.</td>
</tr>
<tr>
<td>-exclude_ct</td>
<td>Do not save change tracking data.</td>
</tr>
<tr>
<td>-forensics</td>
<td>Save the data from the Forensics model rather than from the Live model.</td>
</tr>
<tr>
<td>-whatif</td>
<td>Save the data from the What If model rather than from the Live model.</td>
</tr>
<tr>
<td>filename</td>
<td>The name of the file in which to save the data. The data is saved as a SQLX file.</td>
</tr>
</tbody>
</table>

Note: The default path for the file is `<Skybox_Home>\data\sqlx_files`. To save the file in a different location, include the full path name.

LOAD THE MODEL FROM A SQL FILE

The sqlxrestore utility loads a saved SQL model file to Skybox. You can specify the parts of the model to load and to which model in Skybox to load them.

By default:

- Only the model part is loaded
- Models are loaded to the Live model

**Syntax**

```
```

**Arguments**

The arguments of this command are described in the following table.

Note: If no table options are specified, all tables are restored.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-noserver</td>
<td>Runs the command directly in MySQL, bypassing the server.</td>
</tr>
<tr>
<td>-forensics</td>
<td>Load the specified data to the Forensics model rather than from the Live model.</td>
</tr>
</tbody>
</table>
### Argument Descriptions

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-whatif</td>
<td>Load the specified data to the What If model rather than the Live model in Skybox.</td>
</tr>
<tr>
<td>-user_tables</td>
<td>Load user data to your Skybox model.</td>
</tr>
<tr>
<td>-definition_tables</td>
<td>Load task and report definition data to your Skybox model.</td>
</tr>
<tr>
<td>-dictionary_tables</td>
<td>Load the Skybox Vulnerability Dictionary (from the file) to the Live model in Skybox. Note: Unless you need a specific Dictionary that was saved, it is better to load the latest Dictionary via loaddictionary.bat (on page 85).</td>
</tr>
<tr>
<td>-model_tables</td>
<td>Load the main part of the model, including all network, security, and business data to your Skybox model.</td>
</tr>
<tr>
<td>-ticket_tables</td>
<td>Load ticket-related tables. Note: This argument cannot be used with other table arguments. Note: This argument is supported only when restoring from the current build. It cannot be used to restore tickets from any previous build.</td>
</tr>
<tr>
<td>filename</td>
<td>The name of the model file to load. Note: The default path for the file is \Skybox_Home\data\sqlx_files. To load the file from a different location, include the full path name.</td>
</tr>
</tbody>
</table>

### RESTORE MODEL SETTINGS

The `restore_settings` utility restores (loads) configuration information and other settings to Skybox that were saved by a Back Up Model and Settings task. The backed-up files are saved under the \Skybox_Home\data\xml_models\ directory; file names have the format xml_backup_task_<date>--<time>.xmlx.

You must restore this file after a disaster or if you need to uninstall and reinstall the server for any reason; the model is not complete without this information.

**Syntax**

```
restore_settings <file name>
```

For additional information about this process, see Restoring the model (on page 82).
Chapter 18

Manager options

This chapter explains how to configure options for Skybox Manager from the UI. To configure the options, go to **Tools > Options > Manager Options**.

In this chapter

- **Access Analyzer: Manager** .................................................... 94
- **Messages** ........................................................................... 94
- **Model Validation Status Settings** ........................................... 95
- **Proxy Settings (Manager)** .................................................... 95
- **Regional Settings: Manager** .................................................. 96
- **Reports Configuration** .......................................................... 96
- **Risks Configuration** ............................................................. 96
- **View Settings** ...................................................................... 96

**ACCESS ANALYZER: MANAGER**

The properties in the Access Analyzer page define how results are displayed in Access Analyzer. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use existing entities only| Specifies whether to display results using only assets and services that exist in the model.  
|                           |   - If cleared, the results of access analysis include IP addresses that might be added to the network.  
|                           |   - Select this option if you made a significant scan of the network (that is, if most of your organization’s network is included in the model) and you want to filter the results based on this scan. |
| Display all blocking rules| Specifies whether, for blocked routes *all* access rules that potentially block traffic on the selected route are displayed  
|                           |   - If cleared, only the *1st* access rule that blocks traffic on the selected route is displayed. |

**MESSAGES**

The properties in the Messages page specify the circumstances under which warning messages are displayed to the Skybox user.
MODEL VALIDATION STATUS SETTINGS

The properties in the Model Validation Status Settings page specify whether to display model validation messages for assets. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show severity indication for the relevant entities</td>
<td>Specifies whether, in assets analyses, the Validation Indication column displays the highest severity indication from collection messages for that asset.</td>
</tr>
<tr>
<td>Show related validation status messages of an entity</td>
<td>Specifies whether, in assets analyses, the Messages tab is enabled to display collection messages for that asset. Note: You must enable messages before you can display them (see Enabling device messages (on page 95)).</td>
</tr>
</tbody>
</table>

Enabling device messages

You can configure Skybox to list information messages about device updates (by default, these messages are not displayed). The messages are useful when device updates are unsuccessful; they explain what went wrong and at which point in the update (offline file import or online collection) process.

Enable messages before running the update; otherwise, Skybox does not save these messages and you cannot view them.

To enable device messages

1. Enable saving the messages during device updates in Skybox by setting max_num_of_validation_messages_per_entity to a non-zero value in <Skybox_Home>\server\conf\sb_common.properties.
2. Enable displaying the messages in Skybox:
   a. Go to Tools > Options > Manager Options > Model Validation Status Settings.
   b. Select both check boxes and click OK.
      The Messages tab of the Details pane is enabled.

PROXY SETTINGS (MANAGER)

The properties in the Proxy Settings (Manager) page configure a proxy server for HTTP connections to the internet.

If the Manager machine is configured to connect to the internet via a proxy, configure these settings before downloading Skybox update files (see Downloading the update file (on page 42)).

The Proxy Settings (Manager) properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>The IP address of the proxy server.</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>The TCP port on which the proxy listens for HTTP requests</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name to use for proxy authentication</td>
</tr>
<tr>
<td>Password</td>
<td>The user password to use for proxy authentication</td>
</tr>
</tbody>
</table>
REGIONAL SETTINGS: MANAGER

The properties in the Regional Settings page specify how Skybox displays numbers, dates, and time.

A value selected here overrides the value specified in the Regional Settings: Server page (see page 113).

The Regional Settings properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locale</td>
<td>Specifies how Skybox displays numbers, dates, and time of day</td>
</tr>
</tbody>
</table>

REPORTS CONFIGURATION

The properties in the Reports Configuration page specify whether reports are generated in the background as a task or in the foreground, and where to save the generated reports. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Report Generation Method</td>
<td>Specifies whether default report generation is in the foreground or in the background (report generation can take several minutes for large reports). To set properties of the Report Task, see the Report generation tasks topic in the Skybox Reference Guide.</td>
</tr>
<tr>
<td>Save generated reports in the %HOMEPATH% directory</td>
<td>Specifies whether to save generated reports in the user home directory (as well as the Skybox directory).</td>
</tr>
</tbody>
</table>

RISKS CONFIGURATION

The properties in the Risks Configuration page specify how risk values are displayed in Skybox. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Value Style</td>
<td>Specifies how risk values are presented in Skybox.</td>
</tr>
<tr>
<td>• Level: Risk values are presented as icons.</td>
<td></td>
</tr>
<tr>
<td>• Monetary (value): Risk values are presented as monetary values. Only an Admin can specify the currency unit, see Regional Settings (on page 113).</td>
<td></td>
</tr>
<tr>
<td>• Score (0-100): Risk values are presented as a score between 0 and 100.</td>
<td></td>
</tr>
<tr>
<td>Show Implicit Dependency Rules</td>
<td></td>
</tr>
</tbody>
</table>

VIEW SETTINGS

The properties in the View Settings page specify how Skybox Manager is displayed on your screen. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable scaling according to screen size</td>
<td>Specifies whether to scale the Manager display (including font size) for the size of your screen. If cleared, you might need to scroll to see the entire display.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Include server name in the application window title</td>
<td>Specifies whether to include the server name and port in the title of the Manager window.</td>
</tr>
</tbody>
</table>
Chapter 19

Server options

This chapter explains how to use Skybox Manager to configure options for the Skybox Server.

Note: Only an Admin can change Server options.

To configure the Server options, go to Tools > Options > Server Options.

In this chapter

Access Analyzer: Server ...................................................... 99
Access Compliance .............................................................. 99
Archiving ........................................................................... 100
Asset Modification Settings .................................................. 100
Attack Simulation Configuration ........................................... 101
Business Attributes ............................................................ 101
Change Manager Settings ................................................... 102
Change Tracking Settings ................................................... 109
Customization ................................................................... 110
Dictionary Settings ............................................................. 111
Elasticsearch Export Settings .............................................. 111
Entity Settings ................................................................... 112
License ............................................................................. 112
Proxy Settings (Server) ...................................................... 112
Regional Settings: Server ................................................... 113
Report Configuration .......................................................... 113
Rule Usage ........................................................................ 114
Software Update Settings ................................................... 114
System ............................................................................. 115
Task Settings .................................................................... 116
Threat Manager ................................................................. 118
Ticket Configuration ........................................................... 118
User Settings .................................................................... 120
Vulnerability Control ........................................................... 127
Worm Settings .................................................................... 129
### ACCESS ANALYZER: SERVER

The properties in the Access Analyzer page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Speculative Routing Table</td>
<td>Specifies whether to create a speculative routing table for each asset if no routing table exists.</td>
</tr>
<tr>
<td>Show Location Path in Network Names</td>
<td>Specifies whether to display the location path of each network node as part of the node name when locations are hidden in the results tree.</td>
</tr>
</tbody>
</table>

### ACCESS COMPLIANCE

The properties in the Access Compliance page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments for Access Check Exceptions</td>
<td>Specifies whether Skybox requires users to add comments when they create Access Check exceptions.</td>
</tr>
<tr>
<td>Show Access Policy Exceptions</td>
<td>Specifies whether to display the Access Policy Exceptions tab in the &lt;firewall name&gt; Exceptions dialog box.</td>
</tr>
<tr>
<td>Maximum Number of Entities</td>
<td>The maximum number of ports or IP addresses to be displayed in the text of the violation details.</td>
</tr>
<tr>
<td>Maximum Number of Zone Entities</td>
<td>The maximum number of network entities permitted per zone.</td>
</tr>
<tr>
<td>Analyze Non-Firewalls for Violating Rules</td>
<td>Specifies whether, when analyzing compliance for Network Assurance, Skybox analyzes the access rules of non-firewall devices.</td>
</tr>
</tbody>
</table>

### Firewall Compliance

The properties in the Access Compliance > Firewall Compliance page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>The action Skybox takes to assign the IP addresses behind the network interfaces of each firewall.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disabled</strong>: The Addresses Behind Interface fields are empty on all interfaces (that is, Skybox uses Default Gateway/Unknown Addresses).</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Speculation</strong>: Addresses behind interfaces are assigned, based on the routing table of the firewall, but there is no routing speculation. If there are destination IP addresses that are not found in the routing table, they do not appear behind any interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Full</strong>: Addresses behind interfaces are assigned, based on the routing table of the firewall. There is routing speculation for destination IP addresses that are not found in the routing table; these addresses are added to all interfaces.</td>
</tr>
</tbody>
</table>
For additional information about addresses behind interfaces, see the Addresses behind network interfaces topic in the Skybox Firewall Assurance User Guide.

ARCHIVING

The properties in the Archiving page specify:

- How long to keep archived files
- The behavior of **Model – Outdated Removal** tasks

These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Files Archiving</strong></td>
<td></td>
</tr>
<tr>
<td>Archive backups threshold (days)</td>
<td>Specifies how long to retain automatic backup files. <strong>Note:</strong> This setting does not affect backup files generated manually.</td>
</tr>
<tr>
<td>Archive reports threshold (days)</td>
<td>Specifies how long to retain reports.</td>
</tr>
<tr>
<td><strong>Outdated Removal Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Outdated Removal Ignore Threshold (days)</td>
<td>Networks that were not scanned for this length of time are ignored by <strong>Model – Outdated Removal</strong> tasks (which mark old entities for deletion).</td>
</tr>
<tr>
<td><strong>Statistics Archiving</strong></td>
<td></td>
</tr>
<tr>
<td>Number of daily statistics snapshots to keep</td>
<td>The number of daily statistics snapshots to keep (1 per day). See the note following this table.</td>
</tr>
<tr>
<td>Number of weekly statistics snapshots to keep</td>
<td>The number of weekly statistics snapshots to keep (1 per week). See the note following this table.</td>
</tr>
<tr>
<td>Number of monthly statistics snapshots to keep</td>
<td>The number of monthly statistics snapshots to keep (1 per month). See the note following this table.</td>
</tr>
</tbody>
</table>

**Note:** The Statistics Archiving properties specify the number of statistics snapshots to keep, not how long to keep them.

ASSET MODIFICATION SETTINGS

The properties in the Asset Modification Settings page specify whether users of the What If and Forensics models are notified if another user changes an asset that they are editing. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark Changed Assets</td>
<td>(In What If and Forensics models) Specifies whether users are notified if another user changed an asset that they are editing.</td>
</tr>
</tbody>
</table>
ATTACK SIMULATION CONFIGURATION

The properties in the Attack Simulation Configuration page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Simulation Max Impact</td>
<td>The maximal quantitative impact of Business Asset Groups. (This property has no effect when the risk is set to be qualitative.)</td>
</tr>
</tbody>
</table>

BUSINESS ATTRIBUTES

The properties in the Business Attributes pages configure business attributes for various entities. Business attributes are metadata that provide additional information about an entity.

Access Rules

The properties in the Business Attributes > Access Rules page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Business Attributes)</td>
<td>Skybox includes predefined business attributes for access rules. Click Add to add a new business attribute (see Adding custom business attributes, in the Skybox Firewall Assurance User Guide).</td>
</tr>
</tbody>
</table>

Assets

The properties in the Business Attributes > Assets page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Business Attributes)</td>
<td>Skybox includes predefined business attributes for assets. In addition, business attributes are added automatically to assets via CMDB import. Click Add to add a new business attribute.</td>
</tr>
</tbody>
</table>

Asset Groups

The properties in the Business Attributes > Asset Groups page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Business Attributes)</td>
<td>Skybox does not include predefined business attributes for asset groups; an organization that wants to use them must create their own. Click Add to add a new business attribute.</td>
</tr>
</tbody>
</table>

Networks

The properties in the Business Attributes > Networks page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Business Attributes)</td>
<td>Skybox does not include predefined business attributes</td>
</tr>
</tbody>
</table>
Property Description
Attributes) for networks; an organization that wants to use them must create their own.
Click **Add** to add a new business attribute.

Services
The properties in the Business Attributes > Services page are described in the following table.

<table>
<thead>
<tr>
<th>Property (Business Attributes)</th>
<th>Description</th>
</tr>
</thead>
</table>
|                                | Skybox does not include predefined business attributes for services; an organization that wants to use them must create their own.
|                                | Click **Add** to add a new business attribute. |

Vulnerability Definitions
The properties in the Business Attributes > Vulnerability Definitions page are described in the following table.

<table>
<thead>
<tr>
<th>Property (Business Attributes)</th>
<th>Description</th>
</tr>
</thead>
</table>
|                                | Skybox does not include predefined business attributes for Vulnerability Definitions; an organization that wants to use them must create their own.
|                                | Click **Add** to add a new business attribute. |

Vulnerabilities
The properties in the Business Attributes > Vulnerabilities page are described in the following table.

<table>
<thead>
<tr>
<th>Property (Business Attributes)</th>
<th>Description</th>
</tr>
</thead>
</table>
|                                | Skybox does not include predefined business attributes for vulnerabilities; an organization that wants to use them must create their own.
|                                | Click **Add** to add a new business attribute. |

CHANGE MANAGER SETTINGS
The properties in the Change Manager Settings page affect performance issues in Skybox Change Manager.

The Change Manager Settings properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimization settings</td>
<td>Access Update change requests and Add Rule change requests can sometimes be optimized to Modify Rule change requests. This section specifies how requests are optimized.</td>
</tr>
<tr>
<td>Identical Match</td>
<td>Specifies whether 2 fields of the change request must match the corresponding fields of the access rule exactly.</td>
</tr>
<tr>
<td>Contained within</td>
<td>Specifies whether 2 fields of the change request must be contained within the corresponding fields of the access rule.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include contained in Any</td>
<td>Specifies whether to include matches where fields of the change request are contained within a field whose value is Any.</td>
</tr>
</tbody>
</table>

### Change Manager Mode

#### (Firewall identification mode)

**Firewall Mode**

For models that do not include routers or are not fully connected.

Identifies firewalls based on a comparison between the relevant fields of the change request and the addresses behind the firewalls in the Firewall Assurance tree.

**Note:** In firewall mode, access requests to a network device’s interface cannot be used as a source or destination.

**Network Mode**

For models that include routers and are fully connected.

Identifies firewalls by running access analysis. Enables users to view the routes that a change request would take in the network.

### (Policy compliance calculation mode)

**Firewall Mode**

Calculates violations by checking the access of firewall network interfaces.

**Network Mode**

Calculates violations by checking network access.

**Access Policy Scope**

This field is enabled only if you select **Network Mode**.

The parts of the Public Access Policies (policy folders, policy sections, or specific Access Checks) to use when calculating policy compliance violations.

### Verification

**Source and destination interface**

For Add Rule change requests, specifies whether to verify that the source and destination interfaces in the new rule match those in the change request. The interfaces in the change request are calculated by Skybox to be those that produce the requested access.

**Note:** For firewalls that support zones, specifies whether to verify that the source zone and destination zone in the new rule match those in the change request.

**Expiration date**

For Add Rule change requests that include an expiration date, specifies whether to verify that the expiration date specified in the change request matches the expiration date entered in the new rule.

**Note:** If selected, reconciliation of change requests (in change tracking) also takes expiration dates into consideration.
Change Requests

The properties in the Change Manager Settings > Change Requests page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upload Change Requests from File</strong></td>
<td></td>
</tr>
<tr>
<td>Enable uploading change requests from files</td>
<td>Enables users in Change Manager to upload Access Update change requests to a ticket from a file. After checking this box, map the parameters of the change request to the column names in the file specified in <strong>File Name</strong>. For more information about uploading change requests from a file, see Configuring upload of change requests from files, in the Skybox Change Manager User Manual.</td>
</tr>
<tr>
<td>File Name</td>
<td>The file to upload as the template for change requests. Users in Change Manager can download this template, fill in their change requests, and then upload the file to a ticket.</td>
</tr>
</tbody>
</table>

| **General**                               |                                                                                                                                               |
| Users                                    | The name of the column that contains users for each change request.                                                                           |
| Source                                   | The name of the column that contains the source for each change request.                                                                      |
| Destination                              | The name of the column that contains the destination for each change request.                                                                  |
| Services                                 | The name of the column that contains the services for each change request. (You can specify separate column names for port and protocol.)         |
| Applications                             | (For next-generation firewalls) The name of the column that contains the applications for each change request.                                  |
| Expiration Date                          | The name of the column that contains the expiration date for each change request.                                                             |
| Comment                                  | The name of the column that contains the comment for each change request.                                                                      |
| **Rule Business Attributes**             | The names of the columns that contain rule business attributes for each change request.                                                       |

| **Advanced**                             |                                                                                                                                               |
| Excel Sheet                              | The name of the sheet in the Excel file that contains the change requests. The default is the 1st sheet.                                         |
| Date Format                              | The date format used in the Excel file.                                                                                                         |

**Custom Change Requests**

| Custom Change Request Types              | Click **Add** to add a new type of change request. All custom types are available in Change Manager by clicking **Custom Changes**. **Note:** You cannot use names of existing change request types, whether predefined or custom. |
Display Settings

The properties in the Change Manager Settings > Display Settings page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records Per Page</td>
<td>Specifies how many entries are shown per page in Change Manager tables.</td>
</tr>
<tr>
<td>Custom Fields</td>
<td>Specifies the number of custom fields to use in each row.</td>
</tr>
<tr>
<td>Number of custom fields in a row</td>
<td>If any custom fields have very long names, put fewer fields per row.</td>
</tr>
</tbody>
</table>

Automatic Implementation

The properties in the Change Manager Settings > Automatic Implementation page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic implementation of pending requests</td>
<td>Specifies whether Change Manager automatically implements pending change requests for Check Point, FortiManager, and Panorama devices.</td>
</tr>
<tr>
<td>Suggest implementing relevant requests</td>
<td>Specifies whether, when implementation is requested, Change Manager asks the user whether to implement other pending change requests for the same management server.</td>
</tr>
<tr>
<td>Set the default values to be used for new rules</td>
<td>Set default values for rule fields that are not specified in the change request.</td>
</tr>
<tr>
<td>Rule Position</td>
<td>(Read-only) The position of the rule in the ACL.</td>
</tr>
<tr>
<td>Rule VPN</td>
<td>(Read-only) The VPN that the rule uses.</td>
</tr>
<tr>
<td>Rule Comment</td>
<td>The formula for comments that are added to each rule implemented by Change Manager. You must include at least 1 tag (&lt;DATE&gt;, &lt;USERNAME&gt;, or &lt;TICKET_ID&gt;) in the formula.</td>
</tr>
<tr>
<td>Modify Rule Comment</td>
<td>The formula for comments that are added to each rule modified by Change Manager. You must include at least 1 tag (&lt;DATE&gt;, &lt;USERNAME&gt;, or &lt;TICKET_ID&gt;) in the formula.</td>
</tr>
<tr>
<td>Panorama Add Rule Location</td>
<td>Specifies whether the new rules are added in Panorama as Pre Rules or Post Rules.</td>
</tr>
</tbody>
</table>

For additional information about automatic implementation, including how to set it up in the Check Point SmartDashboard application, and the types of change requests that can be implemented automatically, see the Configuring automatic implementation section in the Skybox Change Manager User Guide.
Object Suggestion

The properties in the Change Manager Settings > Object Suggestion page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Convert addresses and services to objects | Specifies whether to convert all addresses and services in change requests to objects.  
                                      | **Note**: Skybox uses existing objects when an exact match is found. Otherwise new objects are created.                                |
| Naming conventions              | The following fields set the naming conventions for new objects.  
                                      | Host object names must include the <IP> tag.                                                                                               |
| IP Range                        | IP address range object names must include the <IP_RANGE> tag.                                                                                |
| Network                         | Network object names must include the <NETWORK> tag.                                                                                         |
| Service                         | Service objects must include the <SERVICE> tag.                                                                                               |
| Object Comment                  | The formula for comments that are added to each object created by Change Manager. You must include at least 1 tag (<DATE>, <USERNAME>, or <TICKET_ID>) in the formula. |

Permissions

The properties in the Change Manager Settings > Permissions pages configure permissions for Change Manager **Requestors** and how to handle attachments to Change Manager tickets.

Attachment Permissions

The properties in the Change Manager Settings > Permissions > Attachment Permissions page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Ticket attachments can be deleted     | Specifies whether files that were added to tickets can be deleted.  
                                      | If ticket attachments can be deleted, this option specifies the users that are permitted to delete them.                                      |
| The following users are permitted to delete ticket attachments |                                                                                                                                           |

Requestor Permissions

The properties in the Change Manager Settings > Permissions > Requestor Permissions page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permitted request types for Web Ticket Requestor role</td>
<td>The types of change requests that <strong>Web Ticket Requestors</strong> can open.</td>
</tr>
<tr>
<td>Select the permitted request types for the Web Ticket Requestor</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Due Date Permissions</td>
<td></td>
</tr>
<tr>
<td>Allow to view and revise due dates</td>
<td>Specifies whether Web Ticket Requestors can view and revise due dates.</td>
</tr>
<tr>
<td>Ticket Permissions</td>
<td></td>
</tr>
<tr>
<td>Allow all requestors to view all tickets submitted by ...</td>
<td>The submitters whose tickets Web Ticket Requestors can view.</td>
</tr>
<tr>
<td>Allow to view access status details</td>
<td>Specifies whether Web Ticket Requestors can view access status details.</td>
</tr>
<tr>
<td>Allow requestors to use firewall objects</td>
<td>Specifies whether Web Ticket Requestors can use firewall objects.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>The properties in the Change Manager Settings &gt; Risk Assessment page are described in the following table.</td>
</tr>
<tr>
<td>Enforce Risk Justification comment</td>
<td>Specifies whether it is mandatory to add a comment (explaining how the risk is justified) in the Risk pane before promoting the ticket.</td>
</tr>
<tr>
<td>Use the Vulnerability Dictionary and enable import of vulnerability information</td>
<td>(For licenses that include only Firewall Assurance) Specifies whether vulnerability occurrence information is collected and displayed when working with Skybox Change Manager.</td>
</tr>
<tr>
<td>Show Exposed Vulnerability Occurrences</td>
<td>Specifies whether to show exposed vulnerability occurrences in the Risk Assessment phase.</td>
</tr>
<tr>
<td>Show risk assessment for already allowed change requests</td>
<td>Specifies whether risk assessment information is displayed for change requests that were already permitted.</td>
</tr>
<tr>
<td>Approve Risk</td>
<td></td>
</tr>
<tr>
<td>Set the default approval expiration date ... based on risk levels</td>
<td>The default expiration date of exceptions for each risk level.</td>
</tr>
</tbody>
</table>

Skybox version 10.0.200
Approve Risk

When you approve the risk of a change request in the Risk Assessment ticket phase, the Approve Request dialog box provides an approval expiration date based on the highest violation severity caused by the change request. Skybox uses these expiration dates for the corresponding exceptions that are created based on the approval. For each risk level, a specific length of time is specified for the expiration date; when you approve a change request, this time is added to the current date to calculate the expiration date.

You can change the expiration time for each severity according to your policy.

Tickets

The properties in the Change Manager Settings > Tickets page affect tickets in Skybox Change Manager.

The Tickets properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic closure of tickets</td>
<td>Specifies whether Access Change tickets are closed automatically after all their change requests are implemented.</td>
</tr>
<tr>
<td>Automatically close resolved tickets if all change requests were implemented</td>
<td>Specifies whether Access Change tickets are closed automatically if they are in the final phase (usually named Verified) for more than a given number of days.</td>
</tr>
<tr>
<td>Set status of automatically closed tickets to</td>
<td>Specifies the status to which tickets are set when they are automatically closed.</td>
</tr>
<tr>
<td>Default ticket priority</td>
<td>Specifies the default priority for new tickets.</td>
</tr>
<tr>
<td>Rule logging default settings</td>
<td>Specifies whether new rules implemented on firewalls have logging enabled by default.</td>
</tr>
<tr>
<td>Shared Objects default settings</td>
<td>Specifies whether new objects created for Panorama are created as shared by default.</td>
</tr>
</tbody>
</table>

Workflows

The properties in the Change Manager Settings > Workflows page are described in the following table.
Property Description

(Workflows) Click Add to add a new workflow using the wizard. Select Add > Template Workflow to add another standard workflow (which you can then edit). Double-click an existing workflow to edit it.

For information about workflows, see the Customizing ticket phases and workflows section in the Skybox Change Manager User Guide.

**Default Work Time**

**Work Week** Specifies the work week for your organization. Skybox only uses these days to calculate ticket due dates for workflows based on the default work time.

**Holiday Dates** (Optional) Specifies the dates in the year that are non-working holidays for your organization.
- Enter these dates in the regional format that you chose, comma-separated.
- You can create a text file of the dates and import the file into Skybox. The values in the text file must be comma-separated or on new lines.

**Work Hours** Specify the working hours for your organization. Skybox only uses these hours to calculate ticket due dates for workflows based on the default work time.

**CHANGE TRACKING SETTINGS**

The properties in the Change Tracking Settings page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract ticket ID</td>
<td>Specifies whether to extract the (external) ticket ID of the requested change from the Comments field of access rules and objects.</td>
</tr>
<tr>
<td>Ticket ID Regex</td>
<td>Specifies the regular expression used to extract the ticket ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The default regular expression represents a 5-digit number.</td>
</tr>
<tr>
<td></td>
<td>For information about regular expressions, see <a href="http://www.regular-expressions.info/">http://www.regular-expressions.info/</a></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Changes to the regular expression are relevant for future change tracking records only. Existing records are not affected.</td>
</tr>
<tr>
<td>Enable change reconciliation</td>
<td>Specifies whether to enable the Change Reconciliation feature.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Selecting this property enables the other fields in this section.</td>
</tr>
<tr>
<td>Authorized changes must have tickets</td>
<td>Specifies whether a change can be authorized if no matching tickets (in Skybox) are found for the change.</td>
</tr>
</tbody>
</table>
Property Description

Pending changes are automatically unauthorized within <n> days
Specifies the number of days to leave changes in the Pending state. After this number of days, the status of Pending changes becomes Unauthorized.

Pending changes that haven’t started the reconciliation process are automatically unauthorized within <n> days
Specifies whether pending changes that are not even partially reconciled are automatically marked as Unauthorized and, if so, within how many days.

Enable auto-matching by ticket ID
Specifies whether change tracking analysis attempts to match changes and Skybox tickets by external ticket IDs.

Enable auto-matching by addresses & ports
Specifies whether change tracking analysis attempts to match changes and Skybox tickets by IP addresses and ports.

CUSTOMIZATION

These properties enable you to customize the look and feel of Skybox Change Manager and Skybox Horizon to better match your organization.

Note: Click Reset to Default to restore the Skybox look and feel at any point.

The properties in the Customization page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logo</td>
<td></td>
</tr>
<tr>
<td>Company Name</td>
<td>The company name to display; default is SKYBOX.</td>
</tr>
<tr>
<td>Website Address</td>
<td>Specifies the URL that opens when users click the logo at the top left of the Change Manager or Skybox Horizon page; default is <a href="http://www.skyboxsecurity.com">www.skyboxsecurity.com</a></td>
</tr>
<tr>
<td>Logo Image</td>
<td>The logo to be shown at the top left of the Change Manager or Skybox Horizon page. Note: The logo must be in PNG format and should be 75 x 43 pixels. Larger images are resized to 75 x 43 for display.</td>
</tr>
<tr>
<td>Welcome Logo Image</td>
<td>The logo to be shown at the top of the Change Manager home page. Note: The logo must be in PNG format and should be 250 x 101 pixels. Larger images are resized to 250 x 101 for display.</td>
</tr>
<tr>
<td>Login Screen Image</td>
<td>The logo to be shown on the login screen of Change Manager and Skybox Horizon. Note: The logo must be in PNG format and should be 500 x 305 pixels. Larger images are resized to 500 x 305 for display.</td>
</tr>
</tbody>
</table>
Chapter 19  Server options

Property | Description
---|---
Toolbar Background Colors | The colors to display on the Change Manager or Skybox Horizon toolbar.

Toolbar Foreground Colors | The colors of the text to display on the Change Manager or Skybox Horizon toolbar. Note: Each text color is displayed directly underneath the background color on which it will be used. (There is no text on the 3rd section of the toolbar.)

Message of the Day
Enter message of the day in HTML format | The message to display after a user logs in to Skybox Change Manager. Note: The <html>, <body>, <header>, and <script> tags cannot be used in the message.

Dashboards
Maximal number of dashboards | The maximum number of dashboards in a Skybox web interface.

DICTIONARY SETTINGS
The properties in the Dictionary Settings page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity Score</td>
<td>Specifies whether the source of the severity score is the CVSS Base Score or the CVSS Temporal Score.</td>
</tr>
<tr>
<td>Severity Levels</td>
<td>Specifies the severity ranges per level. For example, any severity score between 9 and 10 has the level Critical (by default) and is displayed in the Manager as, for example, Critical (9.1).</td>
</tr>
</tbody>
</table>

About the severity levels
- Level names cannot be changed, only upper and lower bounds.
- Modification of these levels also affects the security metric severity levels in Security Metric Properties dialog boxes, and security metrics analysis.

ELASTICSEARCH EXPORT SETTINGS
The properties in the Elasticsearch Export Settings page are used to describe an external Elasticsearch instance to which Skybox exports information. The properties are described in the following table.

Note: Changing these properties requires server restart.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Elasticsearch Hostname</td>
<td>The hostname of your Elasticsearch server. Note: Do not use localhost.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>The HTTP port for connecting to Elasticsearch.</td>
</tr>
</tbody>
</table>
Property Description

Note: When working with Elastic Cloud, this is the REST endpoint port (443 or 9243).

HTTP Protocol The HTTP protocol for connecting to Elasticsearch.

HTTP Authentication Indicates whether HTTP authentication is used when connecting to Elasticsearch.

HTTP Username The username to use when connecting to Elasticsearch. The clear text will be encrypted after server restart.

HTTP Password The password to use when connecting to Elasticsearch. The clear text will be encrypted after server restart.

ENTITY SETTINGS

The properties in the Entity Settings page specify the number of days that entities are marked as new or modified. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark Entity as New for &lt;n&gt; Days</td>
<td>The number of days that an asset, vulnerability occurrence, policy violation, or access rule is marked as New.</td>
</tr>
<tr>
<td>Mark Access Rule as Modified for &lt;n&gt; Days</td>
<td>The number of days that an access rule is marked as Modified.</td>
</tr>
<tr>
<td>Exception about to be expired &lt;n&gt; Days</td>
<td></td>
</tr>
</tbody>
</table>

LICENSE

The properties in the License page define how many days of notification are given before the Skybox license expires. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify on license expiration &lt;n&gt; days before expiration date</td>
<td>The number of days before the license for Skybox expires that user notifications are given.</td>
</tr>
</tbody>
</table>

PROXY SETTINGS (SERVER)

The properties in the Proxy Settings (Server) page configure a proxy server for HTTP connections to the internet.

If the relevant Server or Collector machine is configured to connect to the internet via a proxy, configure these settings before downloading Skybox dictionary update files (see Dictionary updates (on page 138)).

These settings are also used by some collection tasks (if they are configured to use proxy settings that are not defined in the task properties).

The Proxy Settings (Server) properties are described in the following table.
### Property Description

**Proxy Server**  The IP address of the proxy server

**Proxy Port**  The TCP port on which the proxy listens for HTTP requests

**Local IP**  The local IP address of the interface to use for updating the Skybox Vulnerability Dictionary

**User Name**  The user name to use for proxy authentication

**Password**  The user password to use for proxy authentication

**NTLM authentication**

**Domain**  The domain to use for NTLM authentication

**Client Host Name**  The name of the client host for NTLM authentication

**Enable NTLM v2**  Specifies whether to enable NTLM v2

### REGIONAL SETTINGS: SERVER

The properties in the Regional Settings page specify how Skybox displays numbers, dates, time, and currency values. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Locale</strong></td>
<td>Specifies how Skybox displays numbers, dates, and time of day.</td>
</tr>
<tr>
<td><strong>Currency</strong></td>
<td>Specifies how Skybox displays monetary values (for example, currencies, prices, and quantitative risks).</td>
</tr>
</tbody>
</table>

Note: By default, all users of Skybox work with the locale (and currency) set here, but they can change the locale using the Manager Options – Regional Settings page (see page 96).

### REPORT CONFIGURATION

The properties in the Report Configuration page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reports Footer Text</strong></td>
<td>The text to display at the bottom of each page of generated reports, to a maximum of 60 characters.</td>
</tr>
<tr>
<td><strong>Max Number of Vulnerability Occurrences (Overview)</strong></td>
<td>The maximum number of vulnerability occurrences in vulnerability occurrences overview reports.</td>
</tr>
<tr>
<td><strong>Max Number of Vulnerability Occurrences (Detailed)</strong></td>
<td>The maximum number of vulnerability occurrences in vulnerability occurrences detailed reports.</td>
</tr>
<tr>
<td><strong>Show PDF Bookmarks</strong></td>
<td>(If PDF format is selected for a report) Specifies whether to display the table of PDF bookmarks.</td>
</tr>
<tr>
<td><strong>Paper Size</strong></td>
<td>The paper size to use when formatting the reports.</td>
</tr>
</tbody>
</table>
CSV Export

The properties in the Report Configuration > CSV Export page define the format of the CSV files generated when Skybox tables are exported to CSV files. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV line termination</td>
<td>Specifies how to terminate each line of the CSV files.</td>
</tr>
<tr>
<td></td>
<td>• LF (‘\n’): Line feed</td>
</tr>
<tr>
<td></td>
<td>• CRLF (‘\r\n’): Carriage return + line feed</td>
</tr>
<tr>
<td>Note:</td>
<td>Line termination might be important if the exported files are processed in a 3rd-party program.</td>
</tr>
</tbody>
</table>

RULE USAGE

Rule Usage shows the actual use of each access rule for all the addresses and ports in the rule. Addresses and ports that are never used or used very little are potential candidates for cleanup. You can edit the definitions of the percentage that is considered poor (Critical), fair, and good.

The properties in the Rule Usage page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not show disabled rules in rule usage views or reports</td>
<td>Specifies that disabled access rules are not shown in rule usage views, reports, or counters.</td>
</tr>
<tr>
<td>Usage Levels</td>
<td>Specifies usage levels as rule usage percentages.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>• A rule for which only 0% of its addresses and 10% of its ports are used has poor rule usage.</td>
</tr>
<tr>
<td></td>
<td>• A rule that has over 40% of its addresses and ports used is a well-used rule.</td>
</tr>
<tr>
<td>(These examples are based on the default values.)</td>
<td></td>
</tr>
</tbody>
</table>

Rule Usage Period

These fields enable you to define a custom rule usage period.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting on</td>
<td>The start date for the custom rule usage period.</td>
</tr>
<tr>
<td>Ending on</td>
<td>The end date for the custom rule usage period.</td>
</tr>
</tbody>
</table>

SOFTWARE UPDATESETTINGS

The properties in the Software Update Settings page specify whether automatic software updating of Skybox Managers and Collectors is enabled. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic software updates</td>
<td>Specifies whether automatic (remote) software updating is enabled.</td>
</tr>
<tr>
<td>Note:</td>
<td>If remote software updating is disabled, the Server does not check whether the versions of the Managers and Collectors match its own version; you must apply patches for Managers and Collectors locally.</td>
</tr>
</tbody>
</table>
Chapter 19  Server options

Property | Description
---|---
Enable automatic update of Skybox Collectors | Specifies whether Skybox checks Collector versions and update Collectors after the Server is updated.

**SYSTEM**

The properties in the System pages configure system-level settings.

Property | Description
---|---
Block simultaneous sessions of a single user on different machines | Specifies whether a single user is permitted to be logged in on more than one machine at the same time. In many organizations, this is forbidden for security reasons.

**Backup Settings**

The properties in the System > Backup Settings page define how Skybox saves and loads the model. These properties are described in the following table.

Property | Description
---|---
Model Encryption Password | Skybox encrypts the model with a password when saving it and uses the same password to decrypt it when loading the model. If this field is empty, Skybox uses the default password. You can change the password for security purposes. However, if you change the password you cannot load models encrypted with the previous password.

**Warning**: We recommend that you do not change this password unless required by your organization security policy.

**Email Configuration**

The properties in the System > Email Configuration page define how Skybox sends email messages (for example, alerts) to users. These properties are described in the following table.

Property | Description
---|---
SMTP Server | The server used by Skybox to send messages.
SMTP Port | The SMTP server port used by Skybox.
Mail Server Authentication | The SMTP server used by Skybox.
Username | The user name for mail server authentication.
Password | The password for mail server authentication.
Confirm Password | The password for mail server authentication.
Email Address | The email address from which Skybox messages are sent.
Email Caption | The email caption from which Skybox messages are sent.
Property Description

Test Message Opens the Test Message dialog box from which the administrator setting up emails in Skybox can send a test message to validate the email configuration settings.

Events and Triggers

The properties in the System > Events and Triggers page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Events</strong></td>
<td></td>
</tr>
<tr>
<td>Send System Events</td>
<td>Specifies whether to send Skybox events to remote logging servers.</td>
</tr>
<tr>
<td>Remote Logging Server</td>
<td>A comma-separated list of the names or IP addresses of the remote logging servers, with the format <code>&lt;server name&gt;[:&lt;port&gt;]</code> or <code>nnn.nnn.nnn.nnn[:&lt;port&gt;]</code>. The default port is 514.</td>
</tr>
</tbody>
</table>

The type of events to send
- **System**: Specifies whether to send system events. System events include starting and stopping the Server and Collector, and the start and finish of each task that runs.
- **Audit log**: Specifies whether to send events that go to the audit log. These are user-related events.
- **Activity log**: Specifies whether to send activity log events. These events include many Skybox actions.

The format of the sent messages Specifies whether to send messages that match the format of the Skybox Server operating system.

Triggers

Controls the frequency at which overdue notifications are sent Specifies how often overdue notifications for tickets are sent. Select a frequency and then define the schedule.

For additional information, see Skybox logs (on page 140).

TASK SETTINGS

The properties in the Task Settings pages configure task settings and task alert settings.

Global Task Settings

The properties in the Task Settings > Global Task Settings page specify settings for multiple Skybox tasks. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude Devices</td>
<td>A list of devices that are not to be imported into the model. These devices are ignored when you run an offline file import task. Click Add to add names of devices to exclude. This creates a basic exclude list. Select Add &gt; Advanced Exclude to create a list of</td>
</tr>
</tbody>
</table>
### Property Description

- **assets to exclude based on specific filters.**
  Double-click an existing entity in the list (single device or filter list) to edit it.

- **CyberArk Authentication**
  Settings used by all tasks that authenticate via CyberArk.

- **CyberArk Folder**
  The CyberArk directory.

- **CyberArk Application ID**
  The application ID to use for connecting to CyberArk.

The filters that can be used in an advanced exclude list are described in the following table.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Name</td>
<td>The names of assets to exclude from the model (regular expression).</td>
</tr>
<tr>
<td>Network Scope</td>
<td>The networks to exclude from the model.</td>
</tr>
<tr>
<td>Asset Type</td>
<td>The types of assets to exclude from the model.</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>The operating systems to exclude from the model.</td>
</tr>
<tr>
<td>OS Vendor</td>
<td>The OS vendors to exclude from the model.</td>
</tr>
<tr>
<td>Features</td>
<td>Assets with the selected features are excluded from the model.</td>
</tr>
<tr>
<td>No Services</td>
<td>Only exclude assets from the model if they have no services. (If you select <strong>No Services</strong>, the <strong>Services</strong> filter cannot be used.)</td>
</tr>
<tr>
<td>Services</td>
<td>Assets with the specified services are excluded from the model.</td>
</tr>
<tr>
<td>Products</td>
<td>Assets with these products are excluded from the model.</td>
</tr>
</tbody>
</table>

#### Task Alert Settings

The properties in the Task Settings > Task Alert Settings page specify the global conditions and recipients of email messages that are sent when Skybox tasks finish. These properties are described in the following table.

Note that:

- Alerts are enabled by default for all new tasks (and all predefined tasks), but you can turn off alerts for specific tasks. In this case, no alerts are sent for the task.
- In each task, you can set specific conditions and users for the task alert messages. If present, these settings override the global settings.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email to</td>
<td>The Skybox users and external email addresses that receive task alert emails.</td>
</tr>
<tr>
<td>Email on</td>
<td>The task exit codes for which to send task alert emails.</td>
</tr>
<tr>
<td>Message Count</td>
<td>The maximum number of most recent task messages to include in the text of task alert emails.</td>
</tr>
</tbody>
</table>
THREAT MANAGER

The properties in the Threat Manager page configure some default values of security metrics in Skybox Vulnerability Control.

The Vulnerability Control properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Alert Source</td>
<td>The alert source for which Vulnerability Definitions are displayed in the Threat Manager workspace.</td>
</tr>
<tr>
<td>Threat Alert Mode</td>
<td>If the alert source is Skybox, this parameter controls whether threat alerts in Threat Manager are managed as security bulletins and advisories, or as stand-alone Vulnerability Definitions. Note: For other alert sources, the threat alerts are managed as stand-alone Vulnerability Definitions.</td>
</tr>
</tbody>
</table>

Custom Vulnerability Definitions

<table>
<thead>
<tr>
<th>Source Name</th>
<th>The source name to display for custom Vulnerability Definitions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Prefix</td>
<td>The 3-letter prefix to use for custom Vulnerability Definitions.</td>
</tr>
</tbody>
</table>

For additional information, see the Setting up the Threat Manager environment topic in the Skybox Threat Manager User Guide.

TICKET CONFIGURATION

The properties in the Ticket Configuration page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize model with tickets</td>
<td>Specifies whether to synchronize the model with changes resulting from processed tickets. If selected, closing a vulnerability occurrence ticket causes changes in the model, including changing the status of the vulnerability occurrence to Fixed and changing the asset or service to reflect the selected solution. (A vulnerability occurrence ticket usually lists several solutions, one of which is specified as the selected solution for that specific vulnerability occurrence problem.)</td>
</tr>
<tr>
<td>Attachments</td>
<td></td>
</tr>
<tr>
<td>Max File Size (MB)</td>
<td>The maximum size of files that can be attached to tickets in Skybox.</td>
</tr>
</tbody>
</table>

External Ticketing System Synchronization

| Manual Synchronization                                  | Specifies whether external ticket IDs and statuses can be changed manually in Skybox tickets. Use this option when the Skybox ticketing system is not integrated with the external ticketing system. |
About ticket priority levels

If you disable a priority level, you also disable all lower levels (that is, the levels representing less important tickets). If there are any tickets with these priority levels, they are reassigned to the lowest remaining priority level.

If you enable a priority level, you also enable any higher levels that are disabled. For example, if levels P3, P4, and P5 are disabled and you enable level P5, levels P3 and P4 are also enabled.

Custom Fields

The properties in the Ticket Configuration > Custom Fields page define additional (custom) fields for tickets. You can use custom fields in all ticket types. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Field list)</td>
<td>The details of each custom field, including the title of the field, the type of the field, and the ticket types to which the field applies.</td>
</tr>
</tbody>
</table>

Custom Ticket Statuses

The properties in the Ticket Configuration > Custom Ticket Statuses page define custom ticket statuses for Skybox.

Skybox supports up to 5 custom ticket statuses in addition to the predefined ticket statuses.

When you define custom ticket statuses, specify a status group value (Open, Done, or Invalid) for each custom status.

Custom Ticket Status properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Status &lt;n&gt;</td>
<td>A custom ticket status name. You can add up to 5 custom ticket statuses. If empty, this custom ticket status is not supported and does not appear in the list of statuses displayed to users.</td>
</tr>
<tr>
<td>Status Group</td>
<td>The status group for each Custom Ticket Status. Ticket status groups (Open, Done, and Invalid) classify tickets.</td>
</tr>
</tbody>
</table>

General

The properties on the Ticket Configuration > General page provide control over ticket priorities and phases, and how to handle email cc lists.

Ticket priority and phase properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket Priority Levels</td>
<td>The name of each priority level. You can disable lower priority levels if they are not necessary. For example, if your organization only uses 3 priority levels, you can disable levels 4 and 5. <strong>Note</strong>: If you disable a priority level, all lower levels are also disabled; when you enable a priority level, any higher levels that are disabled are also enabled.</td>
</tr>
</tbody>
</table>
**Ticket Phases**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket Type</td>
<td>The type of tickets for which to use the phases specified in <strong>Phase List</strong>. Each ticket type can have a separate phase list.</td>
</tr>
<tr>
<td>(Phase List)</td>
<td>This table is not displayed if <strong>Ticket Type</strong> = <strong>Access Change</strong>. A list of information about each phase of the selected ticket type, including number (that is, order in the list), name, default owner, and user comments. The final phase (named <strong>Verification</strong> by default) is added automatically and can only be deleted after all other phases are deleted.</td>
</tr>
</tbody>
</table>

**Ticket CC List**

Manage ticket cc lists automatically Specifies whether to add users to the cc list of tickets automatically.

If selected, the following users are added to the cc list:

- Ticket creator
- Ticket owner
- Rule owners
- Users in the **Email** field of rule business attributes (for tickets opened on specific access rules)
- Users in custom fields in Change Manager

For information about ticket phases, see:

- The Ticket phases and due dates section in the Skybox Threat Manager User Guide.
- The Defining ticket phases topic in the Skybox Reference Guide.

For information about ticket phases and priorities for Skybox Change Manager, see the Creating ticket phases and workflows section in the Skybox Change Manager Guide.

**Threat Alerts**

The properties in the Ticket Configuration > page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Custom Solutions)</td>
<td>Skybox includes predefined fields for custom solutions. You can use these and add your own. Click <strong>Add</strong> to add a new custom field. The details of each custom field include the title of the field, the type of the field, the size of the field, and an optional hint for the field.</td>
</tr>
</tbody>
</table>

**USER SETTINGS**

The user settings properties are described in the following topics.

**Authentication**

The properties in the User Settings > Authentication page specify how Skybox authenticates users.
These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skybox</td>
<td>(Read-only) Skybox authentication is always enabled. You can use it in conjunction with external authentication systems.</td>
</tr>
<tr>
<td>Support External Authentication</td>
<td>Specifies whether to use external methods of authentication in addition to Skybox authentication.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Specifies whether authentication using LDAP is enabled.</td>
</tr>
<tr>
<td>Note: Before using LDAP, set the necessary LDAP properties on the External User Management page (see page 126).</td>
<td></td>
</tr>
<tr>
<td>LDAP server properties (on page 121)</td>
<td>The properties of the LDAP servers. Skybox supports up to 10 LDAP servers for different domains. Double-click an existing server in the table to define its properties; click Add to add an additional server. Note: You must define the properties of the default LDAP server before you can use it.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Specifies whether authentication using RADIUS is enabled.</td>
</tr>
<tr>
<td>Note: To use RADIUS authentication, configure the primary and secondary servers, as explained following this table.</td>
<td></td>
</tr>
<tr>
<td>Port Number</td>
<td>The RADIUS server port. Do not change this value.</td>
</tr>
<tr>
<td>Server</td>
<td>The name or IP address of the primary RADIUS server.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>The name or IP address of the secondary RADIUS server.</td>
</tr>
<tr>
<td>SiteMinder</td>
<td>Specifies whether authentication using SiteMinder is enabled.</td>
</tr>
<tr>
<td>Note: Before using SiteMinder, set up integration with SiteMinder (see page 122).</td>
<td></td>
</tr>
</tbody>
</table>

To configure the primary or secondary server for RADIUS

1. Click **Configure**.
2. In the Configure Radius Server dialog box, type the name or IP address of the server and provide the shared secret for the selected server.
3. Click **Test**.
   Skybox attempts to connect to the server and retrieve its certificate.
   
   If the certificate is not trusted by Skybox, a message with the main details of the certificate is displayed. Otherwise, continue at the next step.
4. If you trust the certificate, it is added to the Skybox client keystore.
5. Click **OK**.

**LDAP server properties**

The properties of the LDAP server for each domain are described in the following table.
<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Number</td>
<td>The LDAP server port. The default is 389.</td>
</tr>
<tr>
<td>Server</td>
<td>The name or IP address of the primary LDAP server.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Test</strong> to test connection to the server.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>(Optional) The name or IP address of the secondary LDAP server.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Test</strong> to test connection to the server.</td>
</tr>
<tr>
<td>Default Domain</td>
<td>The initial domain to use when defining new LDAP-authenticated users.</td>
</tr>
<tr>
<td></td>
<td>(In Microsoft Active Directory, each user is associated with a domain.)</td>
</tr>
<tr>
<td>LDAP UID</td>
<td>The attribute in the LDAP server that stores a user’s login name.</td>
</tr>
<tr>
<td>Note</td>
<td>• If you are using multiple LDAP servers,</td>
</tr>
<tr>
<td></td>
<td><strong>userPrincipalName</strong> is the only supported UID after the first LDAP server.</td>
</tr>
<tr>
<td></td>
<td>• If you use <strong>userPrincipalName</strong> for any LDAP server,</td>
</tr>
<tr>
<td></td>
<td>you must define an external user.</td>
</tr>
<tr>
<td>LDAP root DN</td>
<td>The DN to use when connecting to the LDAP server. For example, DC=il,DC=skyboxsecurity,DC=com</td>
</tr>
<tr>
<td>Connection Type</td>
<td>The connection to use when connecting to the LDAP server.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Specifies whether this server is enabled for authentication.</td>
</tr>
</tbody>
</table>

Before using LDAP authentication, configure the primary server for each domain and, if necessary, the secondary server.

**To configure the primary or secondary server for a domain**

1. In the **Server** (or **Secondary Server**) field, type the name or IP address of the server.

2. Click **Test**. Skybox attempts to connect to the server and retrieve its certificate.

   If the certificate is not trusted by Skybox, a message with the main details of the certificate is displayed. Otherwise, continue at the next step.

3. If you trust the certificate, it is added to the Skybox client keystore.

4. Click **OK**.

**Troubleshooting LDAP authentication**

If the primary LDAP server does not respond within a specified period, Skybox tries to log in to the secondary LDAP server. You can change the timeout for login using LDAP by changing the value of **LDAP_connection_timeout** in `<Skybox_Home>\server\conf\sb_server.properties`

**Setting up integration with SiteMinder**

Note: Integration with SiteMinder is supported only when Skybox Server is installed on a Linux machine.
To set up integration with SiteMinder

1. Install the communication agent (see page 123) on the Server machine.
2. Configure SiteMinder (see page 123) to permit communication with Skybox.
3. Create a SiteMinder properties file (see page 124). Copy the file to the `<Skybox_Home>/server/conf` directory.
4. Enable Skybox to work with SiteMinder:
   a. Go to Tools > Options > Server Options > User Settings > Authentication.
   b. Select Support External Authentication.
   c. Select SiteMinder.

Installing the communication agent

You must install the communication agent on the Skybox Server machine.

To install the communication agent

1. Copy the SMAgent binary file from `<Skybox_Home>/data/others/sm/bin` to `<Skybox_Home>/server/bin`
2. Add this directory to `LD_LIBRARY_PATH`.
   For example, `LD_LIBRARY_PATH=/smagent:$LD_LIBRARY_PATH`
3. Execute the command: `export LD_LIBRARY_PATH`
4. Install the `libgcc` standard package on the Server machine.

Configuring SiteMinder to communicate with Skybox

You must define a type 5.x agent in SiteMinder.

Note: In production environments, 5.x is required. In other environments, you can configure a 4.x agent if 5.x configuration fails.

To define a 5.x agent

1. In SiteMinder, create an agent.
2. Create a host configuration object (you can duplicate it from `DefaultHostSettings`). The PolicyServer field must contain the IP address of the SiteMinder server.
3. Create an agent configuration object (you can duplicate it from another configuration object). Fill the fields AgentName and DefaultAgentName with the value `<new agent name>`.
4. Register the host on which SMAgent is to run (that is, the Skybox Server):
   • `smreghost -i <SM server IP address> -u <admin name> -p <admin password> -hn <host name> -hc <host configuration object name>`

   `SmHost.conf` is created.
5. Create a `WebAgent.conf` file that includes the following lines:

   ```
   agentconfigurationobject=<agent configuration object name>
   hostconfigfile=<path to SmHost.conf>
   enablewebagent=YES
   ```
To define a 4.x agent

1. In SiteMinder, create an agent.
2. Select 4.x Support.
3. Type the IP address of the host on which SMAgent is to run.
4. Provide a shared secret.

Additional steps after the agent is defined

Under Domains, create a Realm. Type <new agent name> as the name of the agent.

› Use the resource filter here as the value of the resource property in the properties file to be created in the next section.

SiteMinder properties file

SiteMinder integration requires the file <Skybox_Home>/server/conf/sm_properties.txt. This file must have the format:

› <key1>=<value1>
› <key2>=<value2>

The properties that must be included in the file depend on the version of the agent (5.x or 4.x).

Properties common to 4.x and 5.x agents are described in the following table.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_ip</td>
<td>The IP address of the SiteMinder Policy Server.</td>
<td>Yes</td>
</tr>
<tr>
<td>agent_name</td>
<td>The agent name defined on the SiteMinder Server.</td>
<td>Yes</td>
</tr>
<tr>
<td>resource</td>
<td>The resource protected by the agent.</td>
<td>Yes</td>
</tr>
<tr>
<td>max_cookie_size</td>
<td>Advanced: The memory allocated for updated cookies. The default value is 4096.</td>
<td>No</td>
</tr>
<tr>
<td>user_attrib</td>
<td>Advanced: The attribute number in which to look for the user name. You might have multiple entries of user_attrib.</td>
<td>No</td>
</tr>
</tbody>
</table>

Properties for 5.x agents only are described in the following table.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent_version</td>
<td>The agent version. The value must be set to 5.</td>
<td>Yes</td>
</tr>
<tr>
<td>sm_host_conf_file</td>
<td>The path to the WebAgent.conf file.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Properties for 4.x agents only are described in the following table.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent_version</td>
<td>The agent version. Do not change the default value (4).</td>
<td>No</td>
</tr>
</tbody>
</table>
### Chapter 19  Server options

**Skybox version 10.0.200**

**shared_secret** The shared secret defined on the SiteMinder Server side.  
*Yes*

**agent_ip** The IP address of the host that runs the agent.  
*Yes*

---

**Additional configuration properties for SiteMinder**

The SiteMinder properties in `<Skybox_Home>/server/conf/sb_server.properties` are described in the following table.

*Note: There is usually no reason to change the values of these properties.*

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM_authentication_enabled</td>
<td>Specifies whether to enable user authentication using SiteMinder (Controlled by selecting <strong>Tools</strong> &gt; <strong>Options</strong> &gt; <strong>Server Options</strong> &gt; <strong>User Settings</strong> &gt; <strong>Authentication</strong>)</td>
<td>&lt;disabled&gt;</td>
</tr>
<tr>
<td>SM_properties_file</td>
<td>The name of the SiteMinder properties file under <code>&lt;Skybox_Home&gt;/server/conf</code></td>
<td>sm_properties.txt</td>
</tr>
<tr>
<td>SM_agent_name</td>
<td>The name of the SiteMinder agent utility under <code>&lt;Skybox_Home&gt;/server/bin</code></td>
<td>smagent</td>
</tr>
<tr>
<td>SM_agent_params</td>
<td>For internal use only</td>
<td></td>
</tr>
<tr>
<td>SM_session_cookie</td>
<td>The name of the SiteMinder cookie that stores the SiteMinder SSO Token</td>
<td>SMSESSION</td>
</tr>
<tr>
<td>SM_cookie_max_age</td>
<td>The maximum age of the session cookie in seconds</td>
<td>3600</td>
</tr>
</tbody>
</table>

---

**Testing communication**

You can test communication between SiteMinder and Skybox after you finish the setup.

**To test communication**

› On the Server machine, launch SMAgent by running:

   ```
   smagent sm_properties.txt –user nofile
   ```

   The message *Initializing Agent is Successful* means that the SMAgent was configured successfully.

---

**Disabling Inactive Users**

The properties in the User Settings > Disabling Inactive Users page specify how Skybox handles inactive users.

These properties are described in the following table.
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically Disable Inactive Users</td>
<td>Specifies whether Skybox disables and deletes inactive user accounts. <strong>Note:</strong> The other fields are disabled if this flag is cleared. In this case, delete and disable inactive users manually (for additional information, see Users (on page 67)).</td>
</tr>
<tr>
<td>Disable inactive users after (&lt;n&gt;) days</td>
<td>The number of days of inactivity before a user account is disabled.</td>
</tr>
<tr>
<td>Delete accounts of disabled users after (&lt;n&gt;) days</td>
<td>The number of days a user account is disabled before it is deleted.</td>
</tr>
<tr>
<td>Reassign tickets of deleted users to</td>
<td>When a user is automatically deleted, any tickets they own are reassigned to this user. <strong>Note:</strong> This user is never deleted even if their account becomes inactive.</td>
</tr>
</tbody>
</table>

### External User Management

To use LDAP to manage users:

- Define the LDAP server on the Authentication page (see page 120).
- Create a Skybox user group to correspond to the LDAP users (see page 75).
- Define the properties explained here.

The properties in the User Settings > External User Management page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Specifies whether external user management via LDAP is enabled.</td>
</tr>
<tr>
<td>Global User</td>
<td>Click <strong>Configure</strong> to specify the global user name and password.</td>
</tr>
<tr>
<td>Default Authentication Method</td>
<td>The default method to use for authenticating LDAP users who are managed externally.</td>
</tr>
<tr>
<td>Advanced</td>
<td>The names of attributes used in user records in LDAP, used for pulling user information from the LDAP server. <strong>Note:</strong> The attribute names provided are standard in LDAP; only change them if your organization uses other or customized attribute names.</td>
</tr>
</tbody>
</table>

### User Permissions

The properties in the User Settings > User Permissions page limit the parts of the model to which users have access. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Assurance, Network Assurance (Access Analyzer) &amp; Vulnerability Control Permissions</td>
<td>Specifies whether Skybox limits the parts of the model</td>
</tr>
</tbody>
</table>
Chapter 19    Server options

Property Description
Firewall Assurance, Network Assurance (Access Analyzer) & Vulnerability Control that users can view.

Apply Firewall Assurance permissions to Change Manager tickets Specifies whether users handling Change Manager tickets are only able to view change requests for firewalls for which they have Firewall Assurance permissions.

Change Manager Permissions

Permits for Change Manager Specifies whether Skybox limits the phases of Access Change tickets that users can change.

Tickets can only be edited by their owner Specifies whether users, even with Change Manager permissions, can only edit their own tickets.

Permissions are available for:

- Skybox Firewall Assurance: Firewall folders
- Skybox Network Assurance: Devices shown in Access Analyzer
- Skybox Vulnerability Control: Business Units and locations
- Skybox Change Manager: Phases of Access Change tickets

If permissions are enabled, Admins must set permissions for each User type user and for each user group. If no permissions are set for a User-type user or for any of that user’s user groups, the user cannot see any information in Skybox Firewall Assurance or Skybox Vulnerability Control, and cannot make any changes to tickets in Skybox Change Manager. All Admins have full permissions.

Note: For Skybox Change Manager, you can apply additional editing restrictions on the phases themselves from Tools > Options > Server Options > Change Manager > Workflows. Additional permissions related to Change Manager users are defined in Tools > Options > Server Options > Change Manager > Permissions > Requestor Permissions.

VULNERABILITY CONTROL

The properties in the Vulnerability Control page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain ‘Unassigned Assets’ Site Asset Group</td>
<td>Sites and site asset groups are primarily used for Skybox Horizon. Skybox can include a group for all assets that are not part of any other site asset group. This helps you to see assets that are not part of any site asset group, and can be used to troubleshoot your group definitions.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maintain 'Unassigned Assets' Business Asset Group</td>
<td>Skybox can include a group for all assets that are not part of any other Business Asset Group. This helps you to see assets that are not part of any Business Asset Group, and can be used to troubleshoot your group definitions. <strong>Note:</strong> This group is also part of the security metric calculations.</td>
</tr>
<tr>
<td>Standards Definition</td>
<td>How data is presented in the Vulnerability Control centers.</td>
</tr>
<tr>
<td>Default SLA Values for New Security Metrics</td>
<td>The default values when creating a new security metric. You can leave fields empty.</td>
</tr>
<tr>
<td>Critical</td>
<td>The number of days within which a vulnerability occurrence with <strong>Critical</strong> severity should be fixed.</td>
</tr>
<tr>
<td>High</td>
<td>The number of days within which a vulnerability occurrence with <strong>High</strong> severity should be fixed.</td>
</tr>
<tr>
<td>Medium</td>
<td>The number of days within which a vulnerability occurrence with <strong>Medium</strong> severity should be fixed.</td>
</tr>
<tr>
<td>Low</td>
<td>The number of days within which a vulnerability occurrence with <strong>Low</strong> severity should be fixed.</td>
</tr>
<tr>
<td>Info</td>
<td>The number of days within which a vulnerability occurrence with <strong>Info</strong> severity should be fixed.</td>
</tr>
<tr>
<td>Business Asset Groups Update Warning</td>
<td>Specifies how many days after the Business Asset Groups were most recently updated until a warning is shown in the Manager. The warning is shown on the Summary page and in the Discovery Center, Analytics Center, and Remediation Center.</td>
</tr>
<tr>
<td>Analytics Center</td>
<td>Specifies whether to display the old Center page in Vulnerability Control. <strong>Note:</strong> The information on this page is also found on the Prioritization and Remediation pages; the page is generally considered redundant.</td>
</tr>
</tbody>
</table>

**Risk Score for Web Client**

The properties in the Risk Score for Web Client pages configure the default values to use in calculating risk scores in Skybox Web Client – Vulnerability Control.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Score – Severity Mapping</td>
<td>Maps risk score ranges to severity levels. You can edit the upper bound of any level except the highest level.</td>
</tr>
</tbody>
</table>

**Assets**

The properties in the Vulnerability Control > Assets page define parameters used in calculating the risk for assets and vulnerability occurrences.
These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Importance Scale</td>
<td>A score (by default from 1-5) that reflects how important an asset is to the organization. Asset importance is a factor in the vulnerability occurrence and asset risk score equations. Either numbers or ranges can be used.</td>
</tr>
<tr>
<td>Default Asset Importance</td>
<td>The default importance to be assigned to new assets.</td>
</tr>
<tr>
<td>Asset Importance Range Mapping</td>
<td>Maps the score levels of the asset importance scale to names. For example, 1=Very Low; 5=Very High.</td>
</tr>
<tr>
<td>Calculation Method</td>
<td>Specifies the formula to use for calculating an asset's vulnerability rating and risk score.</td>
</tr>
<tr>
<td>'Vulnerability Rating' or</td>
<td>When using the weighted calculation method, this is the weight to use for each vulnerability rating (or each vulnerability risk score divided by 10) in the function.</td>
</tr>
<tr>
<td>'Vulnerability Risk Score ÷ 10’</td>
<td></td>
</tr>
<tr>
<td>Weight Mapping</td>
<td></td>
</tr>
</tbody>
</table>

**Vulnerabilities**

The properties in the Risk Score for Web Client > Vulnerabilities page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Rating Formula</td>
<td>Specifies the formula to use for calculating the vulnerability rating, which is used to calculate asset and vulnerability risk.</td>
</tr>
</tbody>
</table>

**WORM SETTINGS**

The properties in the Worm Settings page specify whether to include worm risk when analyzing the risk for entities. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Worms</td>
<td>Specifies whether to include risk from existing worms as part of the total risk for each entity</td>
</tr>
<tr>
<td>Zero-day Worms</td>
<td>Specifies whether to include risk from zero-day worms as part of the total risk for each entity</td>
</tr>
</tbody>
</table>

**Automatic Worm Settings**

The properties in the Worm Settings > Automatic Worm Settings page define the set of worms that are available for each Threat Origin. These properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Worms per Threat Origin</td>
<td>The maximum number of worms per Threat Origin.</td>
</tr>
<tr>
<td><strong>Worm selection preferences</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum Worm Age</td>
<td>The maximum age of worms to be used.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Minimum Commonality</td>
<td>The minimum commonality of worms to be used.</td>
</tr>
<tr>
<td>Excluded and Available lists</td>
<td>The list of worms that you can select for each Threat Origin; worms that you exclude are not available in any Threat Origin.</td>
</tr>
</tbody>
</table>
This section provides set up information for Skybox Web Client.

**Supported web browsers**
The following browsers are supported when working with Skybox Web Client:

- Firefox
- Google Chrome
- Microsoft Edge (version 40 and up)

**Scheduling reports**
The reports feature in Skybox Client supports scheduled tasks that can be configured from the Manager (Java client). Each scheduled report requires a separate task.

To configure scheduled reports:

1. Create a task of type **Reports – Auto Generation**.
2. Select **Web Client Reports** as the type.
3. In the **Web Client Reports** field, select the report that you want to schedule.

**Reports in Skybox Web Client running on Linux servers**
If your Skybox Server is running on Linux, an administrator (as root user) must do the following to support the reporting engine in Skybox Web Client:

1. Install the following packages:
   - `yum -y install libX11 libXcomposite libXcursor libXdamage libXext libXi libXtst cups-libs libXScrnSaver libXrandr alsalib pango atk at-spi2-atk gtk3`

2. Run the following commands:
   - `echo user.max_user_namespaces=1000 >> /etc/sysctl.conf`
   - `sysctl -p`
Chapter 21

Working with IPv6

Skybox currently provides partial support for IPv6.

The following devices are supported:

- Palo Alto Networks
- Cisco Firepower

The following scanners are currently supported:

- Qualys

**Limitations on support for IPv6**

In this version, Skybox support for IPv6 includes the following limitations:

- Change Manager does not support IPv6
- Skybox Appliance on IPv6 is not supported
- For Qualys scans, only Host List Detection reports support IPv6, not JSON
- Hybrid (IPv4 and IPv6) perimeter clouds are not supported
- Interoperability of IPv4 and IPv6 is not supported

**How to enable IPv6 in this version**

IPv6 support is currently disabled by default. To enable it, set the following flags and then restart the Server, the Collector, and the Manager (Java client).

**Server side**

- /server/conf/sb_server.properties
  - model_ipv6=true
- /server/conf/sb_common.properties
  - ipv6_collection_toggle=true
  - paloalto.shouldModelIPv6=true
  - qualys.shouldModelIPv6=true
  - cisco_firepower.shouldModelIPv6=true

**Collector side**

- /collector/conf/sb_collector.properties
  - model_ipv6=true
- /collector/conf/sb_common.properties
  - ipv6_collection_toggle=true
• paloalto.shouldModelIPv6=true
• qualys.shouldModelIPv6=true
• cisco_firepower.shouldModelIPv6=true

**UI side**

• \app\conf\sb_common.properties
  • ipv6_collection_toggle=true
  • paloalto.shouldModelIPv6=true
Chapter 22

Configuring Skybox using the properties files

This chapter describes the main Skybox properties files, which configure and fine-tune the behavior of Skybox components.

Edit the properties files using a standard text editor. Unless specified otherwise (in the file), all changes to these files are applied as soon as the file is saved.

In this chapter

Server properties file .......................................................... 134
Collector properties file ....................................................... 134
Manager properties file ....................................................... 134
Common properties file ...................................................... 134
Port properties file ............................................................. 135

SERVER PROPERTIES FILE

The file <Skybox_Home>\server\conf\sb_server.properties contains options that control Server activity.

You can modify many of the properties in this file in Skybox Manager (Tools > Options).

COLLECTOR PROPERTIES FILE

The file <Skybox_Home>\collector\conf\sb_collector.properties contains options that control the Collector’s activity. These options can change the behavior of online collection or offline file import tasks.

MANAGER PROPERTIES FILE

The file <Skybox_Home>\app\conf\sb_app.properties contains options that control Manager activities and change the display in the Manager window.

You can modify most of the properties in this file in the Manager (Tools > Options).

COMMON PROPERTIES FILE

The sb_common.properties file contains properties used by the Server and the Collector; some properties are also used by the Manager.

There are 3 sb_common.properties files:
If multiple Skybox components are installed on the same machine, changes to an `sb_common.properties` file affect only the relevant Skybox component.

**PORT PROPERTIES FILE**

The `sb_ports.properties` file specifies the ports used by Skybox components for communication between themselves.

**Caution:** Do not change the default ports. This is only necessary if 2 Skybox Servers or 2 Skybox Collectors are running on the same machine (*not recommended*).

There are 2 `sb_ports.properties` files:

- **(Server)** `<Skybox_Home>/server/conf/sb_ports.properties`
- **(Collector)** `<Skybox_Home>/collector/conf/sb_ports.properties`

**Note:** Restart the relevant Skybox component to apply port changes.

Synchronize changes made to the `sb_ports.properties` file on the Server machine and on the Collector machines to enable proper communication. For example, if the Collector expects the Server to work on a specific port, set the Server to listen on that port.

**Note:** If you change the Skybox Server port, you must inform all Skybox users so that they can modify the login from Skybox Manager.

**Note:** If you change the value of `skyboxview.ssl.port` in the Collector file, you must also change the value of `springboot.server.port` in `sb_collector.properties`. 

---

Skybox version 10.0.200
Managing multiple Appliances

This chapter explains how to manage multiple Skybox Appliances.

In this chapter

Viewing Appliance information ............................................. 136
Disabling tasks on the secondary Appliance Server .................136

VIEWING APPLIANCE INFORMATION

You can view information about the Skybox Appliances that your organization is using.

To view information about Skybox Appliances

1. From the Tools menu, select Administrative Tools > Appliances.
   You can see a list of all the Appliances and basic information about each, including:
   - Name
   - IP address
   - Version
   - Dictionary
   - License

2. Select an Appliance to display the following additional information:
   - The name of the model file that was loaded and the date it was loaded
   - Whether tasks are enabled or disabled
   - The model number of the Appliance
   - The serial number of the Appliance

DISABLING TASKS ON THE SECONDARY APPLIANCE SERVER

If you work with 2 Appliances as a high availability solution, only 1 Server runs tasks; no tasks or task sequences are run on the secondary (stand-by) Appliance Server.

You disable and enable scheduled tasks and task sequences via the task_scheduling_activation flag (of the secondary Appliance) in <Skybox_Home>\server\conf\sb_server.properties. The default value of this flag is true.
If the flag is set to **false**, all invocation of task and task sequence scheduling is disabled. The scheduler is running, but the tasks and sequences are skipped. Skipped tasks are logged to the debug log with the relevant message:

- Task <task name> scheduling invocation disabled, skipping.
- Task sequence <sequence name> scheduling invocation disabled, skipping.

**To disable or enable the task and sequence invocation on an Appliance**

- **From the** `<Skybox_Home>/server/bin directory`, **run:**
  - In Windows: `settaskschedulingactivation.bat`
  - In Linux: `settaskschedulingactivation.sh`

The utility takes a single argument:

- `enable`: Enable task and sequence invocation
- `disable`: Disable task and sequence invocation
Chapter 24

Dictionary updates


Skybox includes the most up-to-date Vulnerability Dictionary at the time of release, but new updates are issued at least weekly. Keep the Vulnerability Dictionary up-to-date to detect and handle new Vulnerability Definitions, worms, and IPS signatures as they are published.

This chapter contains information about updating the Vulnerability Dictionary.

In this chapter

About Vulnerability Dictionary updates .................................. 138
Updating the Skybox Vulnerability Dictionary ...................... 139

ABOUT VULNERABILITY DICTIONARY UPDATES

You retrieve a new (updated) Vulnerability Dictionary from Skybox by running the Dictionary Update – Daily task. During this task, the Skybox Server retrieves updates from the internet.

Dictionary updates include:

› Updated Vulnerability Definition information
› Updated worm information
› Updated IPS signatures for supported devices.

Checking the Vulnerability Dictionary version

To view information about the Vulnerability Dictionary version

› Select File > Dictionary > Show Dictionary Info.

Frequency of Vulnerability Dictionary updates

Usually, Dictionary updates are released once a week; they are released within one business day whenever a new critical Vulnerability Definition is published. A critical Vulnerability Definition is a severe Vulnerability Definition on a popular product.

Configuring Vulnerability Dictionary updates

You can modify all Dictionary update access properties in the dictionary auto update section of <Skybox_Home>\server\conf\sb_server.properties
Chapter 24  Dictionary updates

UPDATING THE SKYBOX VULNERABILITY DICTIONARY

To update your Vulnerability Dictionary automatically

› Use a Dictionary – Auto Update task, described in the Skybox Reference Guide.

Skybox comes with a predefined daily task named Dictionary Update – Daily, but you can change the task schedule as described in the Task schedule properties topic in the Skybox Reference Guide.

Note: To run the task, enable auto-launch in the General tab of the task’s Properties dialog box.

By default, Dictionary – Auto Update tasks use an auto-update process run by the Skybox Server. However, there is an option for the auto-update process to be run by a Skybox Collector. This option is required if the Server cannot access the update server (for example, when the Server is protected behind a firewall and cannot access the internet).

To use the Skybox Collector for a Dictionary update task

1  Open the task’s Properties dialog box.
2  In the General pane, select the Collector to use for this task.
3  In the Properties pane, select Collector via internet.

Updating the Vulnerability Dictionary manually

If neither the Skybox Server nor the Skybox Collector can access the update server (for example, when they are behind firewalls and cannot access the internet), use the Manager or another computer to download the latest Vulnerability Dictionary and then update the Dictionary manually.


Note: Some web browsers download the Dictionary file with the extension zip; change the extension to sbd before updating the Dictionary.

To update the Vulnerability Dictionary manually

1  Select Tools > Administrative Tools > Update Dictionary.
2  In the Update Dictionary dialog box:
   a. Select the model whose Dictionary is to be updated.
   b. Navigate to the location of the new Dictionary file.
   c. Select the file.
   d. Click Update Dictionary.

For additional help with manual updates, contact Skybox Support.
Chapter 25

Skybox logs

Log information is available in the **System** folder in the Admin tree, via event logging, and in Skybox log files.

In this chapter

- Activity log ........................................................................ 140
- Audit log ........................................................................... 140
- Event logging .................................................................... 140
- Log files ............................................................................ 141
- Activity and audit log messages ................................. 147

**ACTIVITY LOG**

User actions that change the model are logged in the activity log. Actions logged include:

- Changes to and creation or deletion of assets, networks, network interfaces, tickets, security metrics, and notifications
- Vulnerability Dictionary updates and alert service feeds
- Online updates of Skybox

To view the activity log

1. Select **Tools** > **Administrative Tools** > **System**.
2. Click **Activity Log**.

**AUDIT LOG**

The audit log includes all important user management and login actions for all users, and messages about the creation, modification, and deletion of tasks.

To view the audit log

1. Select **Tools** > **Administrative Tools** > **System**.
2. Click **Audit Log**.

**EVENT LOGGING**

Skybox can write messages to Event Viewer (Windows) and syslog (Linux) for the following events:

- Starting and stopping the Server
- Starting and ending a task
User actions (see Audit log messages (on page 150) for a list of these actions)

Actions performed by Skybox (see Activity log messages (on page 147) for a list of these actions)

To enable event logging
1. From the Tools menu, select Options > Server Options > System > Events and Triggers.
2. Select Send System Events.
3. In the Remote Logging Server field, specify the host name or address of the remote logging server.
   - If the logs are to go to a port other than the default system UDP port (514), add a colon and the port number after the host name.
   - To send events to multiple remote servers, use a comma-separated list.
4. Specify the events that are logged to syslog or Event Viewer.

For additional information about enabling event logging, see System Events (on page 116).

Troubleshooting event logging
By default, Skybox events are sent to the syslog server in the following format:

%r [%t] %p %c %x - %m%n

%r is a timestamp for the event. In some cases, the external parser is not expecting the timestamp and cannot parse it. The following instructions explain how to configure Skybox to send events without the timestamp.

To send syslog events without the timestamp
1. Add the following parameter (the value is the same as the default, but without the timestamp) to the file
   <Skybox_Home>\server\conf\sb_server.properties
   - syslog_message_pattern=[%t] %p %c %x - %m%n
2. Restart the Skybox Server.

LOG FILES
Skybox creates many different log files. These include:

- Startup log files (see page 143): These files can help you if you have trouble running Skybox.
- Skybox task output log files (see page 144): These files contain the output of tasks.
- Troubleshooting log files: Skybox produces log files that the Skybox technical support team use for troubleshooting, see Packing log files for technical support (on page 145).

The main log files that may be helpful if something goes wrong are listed in the following table. If a location is not specified, the files are in

<Skybox_Home>\server\log.
<table>
<thead>
<tr>
<th>File path name</th>
<th>File description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activity.log</td>
<td>Includes changes to and creation or deletion of assets, networks, network interfaces, tickets, security metrics, and notifications; Vulnerability Dictionary updates and alert service feeds; and online updates of Skybox (for additional information, see Activity log (see page 140) and Activity log messages (on page 147))</td>
</tr>
<tr>
<td>aging\aging.log</td>
<td>Output of Model – Outdated Removal tasks For information, see Task output logs (see page 144)</td>
</tr>
<tr>
<td>app.log</td>
<td><code>&lt;Skybox_Home&gt;\app\log\app.log</code> ERROR, FATAL, WARNING, and INFO operational messages <strong>Note:</strong> This file is located on the Manager machine</td>
</tr>
<tr>
<td>audit.log</td>
<td>Includes all important user management and login actions for all users, and messages about the creation, modification, and deletion of tasks (for additional information, see Audit log (see page 140) and Audit log messages (on page 150))</td>
</tr>
<tr>
<td>boot.log</td>
<td>Skybox boot log</td>
</tr>
<tr>
<td>collector.log</td>
<td><code>&lt;Skybox_Home&gt;\collector\log\collector.log</code> ERROR, FATAL, WARNING, and INFO operational messages <strong>Note:</strong> This file is located on the Collector machine</td>
</tr>
<tr>
<td>debug\banners.log</td>
<td>Banner translation log</td>
</tr>
</tbody>
</table>
| debug\debug.log | Includes:  
  - General information (for example, memory consumption)  
  - Internal debug ERROR, FATAL, WARNING, INFO, and DEBUG messages  
If verbose logging is enabled for the merging process, the messages are stored at `<Skybox_Home>\app\log\debug\debug.log` For additional information, see Task output logs (see page 144) |
| debug\mail_trace.log | Mail event log |
| debug\requests.log | Request and response log |
| debug\session.log | Login and logout events |
| debug\table.log | Table record count log |
| debug\tasks.log | Includes information about the Server starting and stopping, and tasks starting and stopping |
| debug\vul_detection.log | Vulnerability detection log |
| error.log      | ERROR and FATAL errors reported by the Server |
| install-collector.log | Log messages from Collector installation when the Collector is installed as a service **Note:** This file is located on the Collector machine |
| install-service.log | Log messages from Server installation when the Server is installed as a service |
| model.log      | Model entity count log |
Skybox logs

<table>
<thead>
<tr>
<th>File path name</th>
<th>File description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restclient\debug.log</td>
<td>Debug log for the Web UI</td>
</tr>
<tr>
<td>server.log</td>
<td>ERROR, FATAL, WARNING, and INFO operational messages and output from all tasks except Model – Outdated Removal and Model – Completion and Validation</td>
</tr>
<tr>
<td>validation.log</td>
<td>Output of Model – Completion and Validation tasks For information, see Task output logs (see page 144)</td>
</tr>
<tr>
<td>webapp\debug.log</td>
<td>Debug log for Skybox Change Manager</td>
</tr>
<tr>
<td>webapp\requests.log</td>
<td>Requests log for Skybox Change Manager</td>
</tr>
</tbody>
</table>

**Startup log files**

Skybox creates log files at startup. These files contain information that can help you to troubleshoot problems running Skybox.

**Server startup**

If the Skybox Server runs as a service, it has no console. However, the startup procedure creates a log file, `<Skybox_Home>\server\log\install-service.log`, that contains the output (for example, warning and error messages) that normally is sent to the console.

If there is a problem at Server startup, you can check this log file for possible causes of the problem.

**Collector startup**

If the Skybox Collector runs as a service, it has no console. However, the startup procedure creates a log file, `<Skybox_Home>\collector\log\install-collector.log`, that contains the output (for example, warning and error messages) that normally are sent to the console.

If there is a problem at Collector startup, you can check this log file for possible causes of the problem.

**Memory consumption**

You can view snapshots of the memory consumed by a Skybox component in that component’s debug log file:

- **(Server)** `<Skybox_Home>\server\log\debug\debug.log`
- **(Collector)** `<Skybox_Home>\collector\log\debug\debug.log`
- **(Manager)** `<Skybox_Home>\app\log\debug\debug.log`

You can modify the memory consumption statistics that are logged and the frequency at which they are logged in the gauge properties section of the component’s `sb_common.properties` file:

- **(Server)** `<Skybox_Home>\server\conf\sb_common.properties`
- **(Collector)** `<Skybox_Home>\collector\conf\sb_common.properties`
- **(Manager)** `<Skybox_Home>\app\conf\sb_common.properties`
Task output logs

Task output

➢ Output of Delete outdated entities tasks, which are described in the Skybox Reference Guide

All task messages are written to the 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.

➢ Output of Model completion and validation tasks, which are described in the Skybox Reference Guide

All task messages are written to the log file on the Skybox Server at \<Skybox_Home>\server\log\validation.log

A new log file is created for each run of a validation 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 validation log file contains all output of the task.

➢ Output from all other tasks

All task messages are written to the log file on the Skybox Server at \<Skybox_Home>\server\log\server.log

Skybox messages

These log files are in \<Skybox_Home>\server\log unless otherwise specified.

➢ activity.log: Includes changes to and creation or deletion of assets, networks, network interfaces, tickets, security metrics, and notifications; Vulnerability Dictionary updates and alert service feeds; and online updates of Skybox (for additional information, see Activity log (see page 140) and Activity log messages (on page 147))

➢ audit.log: Includes all important user management and login actions for all users, and messages about the creation, modification, and deletion of tasks (for additional information, see Audit log (see page 140) and Audit log messages (on page 150))

➢ error.log: Includes ERROR and FATAL errors reported by the Server

➢ Component logs:
  • (Manager) \<Skybox_Home>\app\log\app.log: Includes ERROR, FATAL, WARNING, and INFO operational messages
  • (Collector) \<Skybox_Home>\collector\log\collector.log: Includes ERROR, FATAL, WARNING, and INFO operational messages
  • (Server) \<Skybox_Home>\server\log\server.log: Includes ERROR, FATAL, WARNING, and INFO operational messages and output from tasks

➢ debug.log: Includes internal debug ERROR, FATAL, WARNING, INFO, and DEBUG messages
Chapter 25    Skybox logs

- `<Skybox_Home>\server\log\debug\tasks.log`: Includes information about the Server starting and stopping, and tasks starting and stopping

### Verbose logging for the merging process

You can enable verbose logging for the merging process. Messages are saved to `<Skybox_Home>\app\log\debug\debug.log`

The log provides essential information about decisions made by Skybox during the merging process, including:

- Merging candidates for networks and assets
- Decision making during the merge
- Information about overlapping networks

This information can be useful when troubleshooting merging problems encountered when constructing the model.

To enable verbose log messages for the merger

- Set `com.skybox.view.logic.discovery.ModelsMerger.verbose_log` to `true` in `<Skybox_Home>\server\conf\sb_common.properties`.

### Packing log files for technical support

Skybox produces log files that Skybox technical support uses for troubleshooting. The Pack Logs tool (Tools > Pack Logs) packs the relevant log and properties files for all Skybox components installed on the selected machine into a ZIP file, which can then be sent to technical support. The Pack Logs tool stores a copy of the ZIP file on the Server file system and another copy in a specified directory.

Pack Logs properties are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logs from</td>
<td>The Skybox component for which to collect logs.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you select a component on a machine where multiple Skybox components are installed, logs are collected for all the Skybox components on the machine.</td>
</tr>
<tr>
<td>Split output into files of 5MB or less</td>
<td>Specifies whether to split the packed logs into separate ZIP files of 5 MB.</td>
</tr>
<tr>
<td>Add Case Number</td>
<td>If selected, you can add a case ID of up to 8 characters to the name of the ZIP file.</td>
</tr>
<tr>
<td>Include Latest Saved Model</td>
<td>This field is not displayed if Logs from = Firewall Configurations. This field is enabled only if Logs from = Server and Local Collector. Specifies whether to include the latest XMLX model in the ZIP file.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Latest SQLX model</td>
<td>This field is not displayed if <strong>Logs from = Firewall Configurations</strong>. This field is enabled only if <strong>Logs from = Server and Local Collector</strong>. Specifies whether to include the latest SQLX model in the ZIP file.</td>
</tr>
<tr>
<td>Number of Days Back</td>
<td>This field is not displayed if <strong>Logs from = Firewall Configurations</strong>. Limits some of the logs included in the ZIP file to those created within the specified number of days up to the date when the logs are packed. Other logs are included no matter when they were collected.</td>
</tr>
<tr>
<td>Firewall Scope</td>
<td>This field is displayed only if <strong>Logs from = Firewall Configurations</strong>. The firewalls and firewall folders to include in the ZIP file.</td>
</tr>
<tr>
<td>Generations</td>
<td>This field is displayed only if <strong>Logs from = Firewall Configurations</strong>. The number of generations of firewall configuration files to include in the ZIP file.</td>
</tr>
<tr>
<td>Save copy to a local directory</td>
<td>The directory on the local machine where a copy of the packed logs is saved.</td>
</tr>
</tbody>
</table>

### Sending the packed logs to technical support

After packing the logs, open a support site case at the [Skybox Support portal](#) and attach the ZIP files.

### Advanced options

By default, the logs are packed in a single ZIP file named `packlogs_<yyMMdd>_<organization name>[_<case>].zip` but this might result in a very large file, which might be difficult to send or upload. The logs can be packed in multiple files of no more than 5 MB each (by selecting **Split output into files**). The files are named sequentially: `packlogs01_<yyMMdd>_<organization name>[_<case>].zip`, `packlogs02_<yyMMdd>_<organization name>[_<case>].zip`, and so on.

If remote connection to the Server or Collector is down, you can access the packed logs at:

- (Server) `<Skybox_Home>\server\bin\packlogs_<yyMMdd>_<organization name>[_<case>].zip`
- (Collector) `<Skybox_Home>\collector\bin\packlogs_<yyMMdd>_<organization name>[_<case>].zip`

(Or `packlogs01_<yyMMdd>_<organization name>[_<case>].zip`, `packlogs02_<yyMMdd>_<organization name>[_<case>].zip`, and so on.)
Running the utility from the command line

You can run the `<Skybox_Home>\<component>\bin\packlogs.bat` utility locally on any component’s machine (where `<component>` is server, collector, or app). For additional information, see Package log files utility (on page 85).

ACTIVITY AND AUDIT LOG MESSAGES

This section details the messages shown in the activity log and audit log.

Activity log messages

The following event types can be included in the activity log:

- **Configuration Item** event types specify changes to entities in the Application & Service repository.
  - Configuration_Item Configuration Item Created
  - Configuration_Item Configuration Item Deleted
  - Configuration_Item Configuration Item Updated
  - Configuration_Item Configuration Item Enabled
  - Configuration_Item Configuration Item Disabled
  - Configuration_Item Configuration Item Renamed

**Example of a configuration item message**

```
2019-03-18 12:06:54,961 INFO  Configuration_Item Configuration Item Disabled - <skyboxview@127.0.0.1:SFA:1> Application Object Disabled: Development Machines
```

- **Host** event types specify changes to hosts (assets) in the model.
  - Host Access Rules Modification
  - Host Routing Rules Modification
  - Host Virtual Routing Setting Modification
  - Host Dynamic Routing Setting Modification
  - Host Layer2 Setting Modification
  - Host Vpn Update
  - Host Virtual Routers Update
  - Host Asset Manually Created
  - Host Asset Manually Deleted

**Example of a host message**

```
2019-03-16 22:23:34,021 INFO  Host Asset Manually Deleted - <skyboxview@127.0.0.1:SFA:1> Asset deleted. Name: vlab-cisco, Type: Firewall
```

- **Network Interface** event types specify changes to network interfaces.
  - Network Interface Zone Mapping
  - Network Interface Network Assignment Modification
Network Interface Address Behind Interface Modified
Network Interface IP Address Modification
Network Interface Status Change

Example of a network interface message
2019-03-16 22:46:11,796 INFO Network Interface Zone Mapping -
<skyboxview@127.0.0.1:SFA:1> Zone mapping of Interface: netIterface2088
192.170.33.1/24 (asset: prod FW) was modified to Zone=Partners

Network event types specify changes to networks.
Network Zone Mapping
Network IP Address Modification

Example of a network message
2019-03-16 23:04:56,862 INFO Network Zone Mapping -
<skyboxview@127.0.0.1:SFA:1> Zone mapping of Network: nocServers
192.170.23.0/24 was modified to Zone=Internal

Online updates events specify software update changes:
Online-updates Check for Updates
Online-updates Blocked
Online-updates Update Available Status
Online-updates Uptodate Status
Online-updates Get Release Notes
Online-updates Get Hot Fix
Online-updates Download Update Started
Online-updates Download Update Ended

SPA (Security metric) events specify changes to security metrics.
SPA Analysis_Security Metric_Calculation Started
SPA Analysis_Security Metric_Calculation_Ended
SPA Security Metric_Level_Increase_Notification
SPA Security Metric_Level_Decrease_Notification

Example of a SPA message
2019-03-17 11:34:46,676 INFO SPA Analysis_Security Metric_Calculation_Started - <> Analysis - Security Metrics task started running on the Live model

TAM events specify changes to entities in the model that are not covered by the other event types.
Dictionary Auto Update Started
Dictionary Auto Update Ended
New Dictionary
Alert Service Deepsight Collection Started
- Alert Service Deepsight Collection Ended
- Vulnerability Definition Status Updated
- Vulnerability Definition Details User Updated
- Unhandled Vulnerability Definition More
- Ticket Deleted
- Ticket Reopened
- Product Details Updated
- Product Request Deleted
- Updated Vulnerability Notification
- Updated Vulnerability Status Notification
- Ticket Phase Deleted
- Updated Ticket Notification
- Predue Ticket Notification
- Deleted Ticket Notification
- Promoted Ticket Notification
- Request To Close Ticket Notification
- Reassigned Ticket Notification
- Alert Service Idefense Collection Started
- New Custom VT
- Deleted Custom VT
- Access Policy Deleted
- Access Policy Renamed
- Access Policy Enabled
- Access Policy Section Changed
- New Vulnerability Definition
- Vulnerability Definition Details System Updated
- Unhandled Vulnerability Definition
- New Ticket
- Ticket Closed
- New Product
- Product Deleted
- New Vulnerability Notification
- Unhandled Vulnerability Notification
- New Ticket Phase
- New Ticket Notification
- Overdue Ticket Notification
- Closed Ticket Notification
- Cloned Ticket Notification
- Demoted Ticket Notification
- Reopened Ticket Notification
- Minor Ticket Updates Notification
- Alert Service Idefense Collection Ended
- Modified Custom VT
- Access Policy Added
- Access Policy Changed
- Access Policy Disabled
- Access Policy Section Added
- Access Policy Section Renamed
- Access Policy Section Deleted
- Access Policy Section Enabled
- Access Check Changed
- Access Check Deleted
- Access Check Enabled
- Rule Policy Changed
- Rule Policy Disabled
- Rule Policy Enabled
- Rule Check Added
- Rule Check Renamed
- Rule Check Disabled
- Configuration Policy Added
- Configuration Policy Renamed
- Configuration Policy Disabled
- Configuration Check Added
- Configuration Check Renamed
- Configuration Check Disabled
- Vulnerability Occurrence Manually Added
- Vulnerability Occurrence status changed
- Exception Modified
- Access Policy Section Disabled
- Access Check Added
- Access Check Renamed
- Access Check Disabled
- Rule Policy Deleted
- Rule Policy Renamed
- Rule Policy Enabled
- Rule Check Deleted
- Rule Check Enabled
- Rule Check Disabled
- Configuration Policy Changed
- Configuration Policy Deleted
- Configuration Policy Enabled
- Configuration Check Changed
- Configuration Check Deleted
- Configuration Check Enabled
- Vulnerability Occurrence Manually Deleted
- Exception Added
- Exception Deleted

**Example of a TAM message**

```
2019-03-17 11:06:22,512 INFO TAM New_Dictionary - <> New dictionary version 75.893, date: 3/16/19 12:00 AM loaded successfully
```

**Audit log messages**

The audit log includes:

- System messages
- Messages about task creation, deletion, and modification
- User management messages

A complete message has additional information, including a timestamp.
## Sample message for user login

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Level</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-03-16</td>
<td>11:18</td>
<td>INFO</td>
<td>User_Management Login - User <code>skyboxview</code> logged in</td>
</tr>
</tbody>
</table>

<skyboxview@127.0.0.1:TRAY:1>