<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparing to update</td>
<td>35</td>
</tr>
<tr>
<td>Updating the Server and local components</td>
<td>35</td>
</tr>
<tr>
<td>Updating remote components</td>
<td>36</td>
</tr>
<tr>
<td>Updating multi-tiered servers</td>
<td>36</td>
</tr>
<tr>
<td>Skybox licenses</td>
<td>37</td>
</tr>
<tr>
<td>Uninstalling Skybox from a Linux machine</td>
<td>39</td>
</tr>
<tr>
<td>Product security</td>
<td>40</td>
</tr>
<tr>
<td>Communication and certificates</td>
<td>40</td>
</tr>
<tr>
<td>Encryption</td>
<td>43</td>
</tr>
<tr>
<td>Limiting login attempts</td>
<td>43</td>
</tr>
<tr>
<td>Security check: last login message</td>
<td>43</td>
</tr>
<tr>
<td>Customizable login warning messages</td>
<td>43</td>
</tr>
<tr>
<td>User session timeout</td>
<td>44</td>
</tr>
<tr>
<td>Part II: Administration</td>
<td>45</td>
</tr>
<tr>
<td>User management</td>
<td>46</td>
</tr>
<tr>
<td>User roles</td>
<td>46</td>
</tr>
<tr>
<td>Managing users and user groups</td>
<td>53</td>
</tr>
<tr>
<td>Working with external authentication systems</td>
<td>60</td>
</tr>
<tr>
<td>Managing users externally using LDAP</td>
<td>61</td>
</tr>
<tr>
<td>Changing the password for database clients</td>
<td>62</td>
</tr>
<tr>
<td>Backup and restore</td>
<td>64</td>
</tr>
<tr>
<td>Backup and restore scenarios</td>
<td>64</td>
</tr>
<tr>
<td>About the model</td>
<td>64</td>
</tr>
<tr>
<td>Backing up the model</td>
<td>65</td>
</tr>
<tr>
<td>Fast backup</td>
<td>66</td>
</tr>
<tr>
<td>Backing up to an external location</td>
<td>67</td>
</tr>
<tr>
<td>Loading a model</td>
<td>67</td>
</tr>
<tr>
<td>Restoring the model</td>
<td>68</td>
</tr>
<tr>
<td>Administration via CLI commands</td>
<td>70</td>
</tr>
<tr>
<td>Package firewall configurations</td>
<td>70</td>
</tr>
<tr>
<td>Launch tasks</td>
<td>71</td>
</tr>
<tr>
<td>Load the latest Dictionary</td>
<td>71</td>
</tr>
<tr>
<td>Package log files</td>
<td>71</td>
</tr>
<tr>
<td>Scan log files</td>
<td>72</td>
</tr>
<tr>
<td>Save the model</td>
<td>76</td>
</tr>
<tr>
<td>Load the model</td>
<td>77</td>
</tr>
<tr>
<td>Restore model settings</td>
<td>78</td>
</tr>
<tr>
<td>Manager options</td>
<td>79</td>
</tr>
<tr>
<td>Access Analyzer: Manager</td>
<td>79</td>
</tr>
<tr>
<td>Messages</td>
<td>79</td>
</tr>
<tr>
<td>Model Validation Status Settings</td>
<td>80</td>
</tr>
<tr>
<td>Proxy Settings (Manager)</td>
<td>80</td>
</tr>
<tr>
<td>Regional Settings: Manager</td>
<td>81</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Reports Configuration</td>
<td>81</td>
</tr>
<tr>
<td>Risks Configuration</td>
<td>81</td>
</tr>
<tr>
<td>View Settings</td>
<td>81</td>
</tr>
<tr>
<td>Server options</td>
<td>83</td>
</tr>
<tr>
<td>Access Analyzer: Server</td>
<td>84</td>
</tr>
<tr>
<td>Access Compliance</td>
<td>84</td>
</tr>
<tr>
<td>Archiving</td>
<td>85</td>
</tr>
<tr>
<td>Asset Modification Settings</td>
<td>85</td>
</tr>
<tr>
<td>Attack Simulation Configuration</td>
<td>86</td>
</tr>
<tr>
<td>Business Attributes</td>
<td>86</td>
</tr>
<tr>
<td>Change Manager Settings</td>
<td>86</td>
</tr>
<tr>
<td>Change Tracking Settings</td>
<td>92</td>
</tr>
<tr>
<td>Customization</td>
<td>93</td>
</tr>
<tr>
<td>Dictionary Settings</td>
<td>93</td>
</tr>
<tr>
<td>Entity Settings</td>
<td>94</td>
</tr>
<tr>
<td>License</td>
<td>94</td>
</tr>
<tr>
<td>Proxy Settings (Server)</td>
<td>94</td>
</tr>
<tr>
<td>Regional Settings: Server</td>
<td>95</td>
</tr>
<tr>
<td>Report Configuration</td>
<td>95</td>
</tr>
<tr>
<td>Rule Usage</td>
<td>96</td>
</tr>
<tr>
<td>Software Update Settings</td>
<td>96</td>
</tr>
<tr>
<td>System</td>
<td>97</td>
</tr>
<tr>
<td>Task Settings</td>
<td>98</td>
</tr>
<tr>
<td>Threat Manager</td>
<td>100</td>
</tr>
<tr>
<td>Ticket Configuration</td>
<td>100</td>
</tr>
<tr>
<td>User Settings</td>
<td>102</td>
</tr>
<tr>
<td>Vulnerability Control</td>
<td>109</td>
</tr>
<tr>
<td>Worm Settings</td>
<td>110</td>
</tr>
<tr>
<td>Configuring Skybox using the properties files</td>
<td>111</td>
</tr>
<tr>
<td>Server properties file</td>
<td>111</td>
</tr>
<tr>
<td>Collector properties file</td>
<td>111</td>
</tr>
<tr>
<td>Manager properties file</td>
<td>111</td>
</tr>
<tr>
<td>Common properties file</td>
<td>111</td>
</tr>
<tr>
<td>Port properties file</td>
<td>112</td>
</tr>
<tr>
<td>Managing multiple Appliances</td>
<td>113</td>
</tr>
<tr>
<td>Viewing Appliance information</td>
<td>113</td>
</tr>
<tr>
<td>Disabling tasks on the secondary Appliance Server</td>
<td>113</td>
</tr>
<tr>
<td>Dictionary updates</td>
<td>115</td>
</tr>
<tr>
<td>About Vulnerability Dictionary updates</td>
<td>115</td>
</tr>
<tr>
<td>Updating the Skybox Vulnerability Dictionary</td>
<td>116</td>
</tr>
<tr>
<td>Skybox logs</td>
<td>117</td>
</tr>
<tr>
<td>Activity log</td>
<td>117</td>
</tr>
<tr>
<td>Audit log</td>
<td>121</td>
</tr>
<tr>
<td>Event logging</td>
<td>123</td>
</tr>
<tr>
<td>Log files</td>
<td>123</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’s 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 the 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 opening a case, you need the following information:

› 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 125)).
Chapter 1

Introduction

This chapter explains the Skybox platform and its basic architecture.

In this chapter

Skybox platform ........................................................................................................ 7
Skybox architecture .................................................................................................. 9
Platform technology ................................................................................................. 10

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 more information visit the Skybox Security 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 of them. Your license controls which products 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 the following components:

› **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: The UIs for Skybox Horizon and Skybox Change Manager are web-based; Skybox Horizon and Change Manager 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 diagram shows the relationships between the various 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.
Chapter 2

Installation overview

There are several 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 13)</td>
</tr>
<tr>
<td>Server</td>
<td>For organization or enterprise deployment</td>
<td>Server installation (on page 15)</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 17)</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>Installing additional Collectors (on page 28)</td>
</tr>
</tbody>
</table>
Chapter 3

Manager installation

This chapter explains how to install the Skybox Manager by itself.

In this chapter

Installing the Manager ......................................................... 13
Manager system requirements .............................................. 13

INSTALLING THE MANAGER

Note: Skybox Manager runs on most Microsoft Windows operating systems. For details, see Manager system requirements (on page 13).

Installing the Manager requires administrator privileges.

To install the 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.

Important: The Manager communicates with the server over 8443/TCP by default. If there is a firewall between the Manager and the Server, access on this port should be explicitly permitted.

MANAGER SYSTEM REQUIREMENTS

The 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 or 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 equivalent</td>
<td>Intel i5 or equivalent</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Available disk space</td>
<td>1 GB</td>
<td>2 GB</td>
</tr>
</tbody>
</table>
Chapter 4

Server installation

There are several possible Server installation scenarios, each of which requires a different installation process.

In this chapter

Installation environment ...................................................... 15
Installation workflow ........................................................... 15
Server system requirements ................................................ 16
Installing the Server on Windows .......................................... 17
Silent installation ................................................................ 17
Installing the Server on Linux ............................................... 20
Starting and stopping components via the Windows system tray 22
Post-installation steps ......................................................... 22
Enabling Perl-based Collectors............................................. 26

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 Quick Start Guide</td>
</tr>
</tbody>
</table>
| Windows for corporate environment          | • Installing the Server on Windows (on page 17) (via a wizard)  
                                           | • Silent installation (on page 17) (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 17) |
| Linux                                      | Installing the Server on Linux (on page 20) |

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 16).

2. Follow the installation instructions that are described in the following sections:
   - (Windows) Installing the Server on Windows (on page 17) (wizard-driven) or Silent installation (on page 17) (without user intervention)
   - (Linux) Installing the Server on Linux (on page 20)

3. Perform any necessary post-installation steps (see page 22).

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 34)).

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 more than 1 Skybox Server (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). You should 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, you must change the ports used by 1 of them, to prevent port collision (see Installing multiple components on a single host (on page 23)).

Operating system

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

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Windows 7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows 10</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 6</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7</td>
</tr>
<tr>
<td></td>
<td>CentOS 6</td>
</tr>
<tr>
<td></td>
<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.

---

Skybox version 9.0.100
### 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 16).

To install Skybox

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

   The options that you must select in specific screens 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. Browse 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>Screen</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Install Folder</td>
<td>Specify the installation directory.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Installation under &lt;Drive&gt;:\Program Files (or any other path containing a space) is not supported.</td>
</tr>
<tr>
<td></td>
<td>If another (previous) version of Skybox is installed, do not install to the same directory.</td>
</tr>
</tbody>
</table>

| Preferences           | 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. |

### SILENT INSTALLATION

Use silent installation to:

- Install Skybox on Linux machines
- Install Skybox on Windows without user intervention

**Note:** You must have administrator privileges.
Before running a silent installation, ensure that:

- The minimum free disk space requirement (10 GB) is met
- If you previously installed Skybox (any version), you specify a different directory for this installation

To prepare for silent installation

1. Locate the installation file on the installation CD or on the file system (if downloaded from the Skybox customer site):
   - (Windows) SkyboxInstaller-<version#>-<build>.exe
   - (Linux) SkyboxInstaller-<version#>-<build>.bin
2. Copy the file to your computer.
3. From the Silent directory on the CD or the file system, select a properties file:
   - installer.properties: For full installation (all 3 components)
   - installer-collector.properties: For Collector installation; contains properties required for Collector installation only
4. Copy the properties file to the same directory on your computer where you copied the installation program (in step 1).
5. When installing only the Collector, rename the copied installer properties file (installer-collector.properties) to installer.properties
6. Customize the properties file (see page 18) 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: When installing silently, 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. If the Server and Manager are on the same machine, use localhost.</td>
</tr>
<tr>
<td>CHOSEN_INSTALL_SET</td>
<td>The set of Skybox components to install.</td>
</tr>
<tr>
<td></td>
<td>• (Default) Server(Full): Install all components:</td>
</tr>
</tbody>
</table>
**Property** | **Description**
---|---
| 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 will not start.  
| **SB_PATH_OF_LICENSE_FILE** | The directory-level path to the license file. There is no default value.  
  This property is used only if you are installing the Server.  
  **Note:** If you do not provide a license file now, add the license file manually (after the installation) to `<Skybox_Home>\server\conf`.  
| **USER_INPUT_RESULT_ENGLISH** | Specifies whether to install the English version of Skybox.  
  • 1: Yes (default)  
  • 0: No  
| **USER_INPUT_RESULT_JAPANESE** | Specifies whether to install the Japanese version of Skybox.  
  • 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.  
  This property is used only if you are installing the Server.  
  **Note:** This information can be added later using the GUI.  
| **SB_MAIL_ADDRESS** | Mail server name or IP address for sending Admin email.  
  The default address is `skybox_admin@skyboxsecurity.com`  
  This property is used only if you are installing the Server.  
  **Note:** This information can be added later using the GUI.  
| **SB_MANAGER_ACR OBAT** | Specifies whether to install Adobe Reader on the Manager machine:
**Property** | **Description**
--- | ---
• 1: Yes  
• 0: No (default)  
This property is used only if you are installing the Manager.

**USER_SHORTCUTS** (Windows only) Location of the user shortcut.  
The default location is:  
C:\Documents and Settings\All Users\Start Menu\Programs\SkyboxView  
**Note:** By default, this property is commented out—there is no user shortcut.

**SHORTCUT_NAME** (Windows only) The name of the user shortcut.  
The default name is skyboxview.  
**Note:** By default, this property is commented out—there is no user shortcut.

**SB_INSTALL_NEW** Specifies whether to perform a new installation:  
• 1: Yes (default)  
• 0: No  
Do not change this value.

**SB_INSTALL_UPGRADE** Do not change this value.

**SB_PREV_HOME_DIR** Do not change this value.

The following is an example of installer.properties:

```properties
INSTALLER_UI=silent
SB_SERVER_HOST=localhost
USER_INSTALL_DIR=/opt/SkyboxView
CHOSEN_INSTALL_SET=Server(Full)
SB_LICENSE_FILE=license.xml
SB_PATH_OF_LICENSE_FILE=
SB_SERVER_SERVICE=1
SB_COLLECTOR_SERVICE=1
SB_SERVER_SERVICE_START=0
SB_COLLECTOR_SERVICE_START=0
SB_SERVER_MAIL=
SB_MAIL_ADDRESS=skybox_admin@skyboxsecurity.com
SB_MANAGER_ACRROBAT=0
SB_INSTALL_NEW=1
SB_INSTALL_UPGRADE=0
SB_PREV_HOME_DIR=/opt/SkyboxView
```

**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 21)
3. **Install required packages** (see page 21)
Harden platforms according to your organization’s hardening policy

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 the Skybox Manager, you must specify 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 17).

Users

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

- root: Created by 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 following topics explain how to install CentOS 7 to work with the 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/
   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):
     - /boot 500MB
     - / - LVM <all free disk space>

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

- Use the following commands to enable the EPEL repository:
  - a. `yum -y install epel-release`
  - b. `yum repolist`

Packages to install

- Add the following packages using `yum`. Note that this requires internet connection.

<table>
<thead>
<tr>
<th>Package</th>
<th>Usage</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>glibc 64bit</td>
<td>Skybox Appliance</td>
<td><code>yum install glibc</code></td>
</tr>
<tr>
<td>pam.i686</td>
<td>Skybox Appliance</td>
<td><code>yum install pam.i686</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

When 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 (🔧) 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

- Run the following at the command line:
  `<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 the 2nd installation (see Installing multiple components on a single host (on page 23)).

- (Linux) Check that the machine’s resource limits are configured optimally for running Skybox (see Verifying resource limits in Linux (on page 23)).

- 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 24)).

verbs
• 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 26)).
• (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.

verbs
• After logging in to Skybox, specify the SMTP server for Skybox to use and the Skybox administrator’s email address (see Email Configuration (on page 97)). Without this, Skybox cannot send alerts or receive emails.
• Enable event logging (to syslog or Windows Event Viewer) for various system events (see System Events (on page 98)).

Installing multiple components on a single host
You can install multiple Skybox components of a single type on a single machine with the following limitations.

Skybox Servers
Install each Server on a separate machine. If you install multiple Servers on a single machine:

verbs
• Each installation must use a unique set of ports. These ports are set in the port properties file (see page 112).
• Only 1 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 24)).

Skybox Managers
There are no limitations to installing and running multiple Managers on a single machine.

Skybox Collectors
Install each Collector on a separate machine. If you install multiple Collectors on a single machine:

verbs
• Each installation must use a unique set of ports. These ports are set in the port properties file (see page 112).
• Only 1 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 24)).

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 the command ulimit -a.
3. Compare the output results with the recommended values in the table following 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, in the following format:
   •  #<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. When installed 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 either of the following commands:
  • 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 either of the following commands:
  • 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 the following command: ./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 the following command: ./startcollector.sh&
**Stopping the Server and Collector on Linux**

*To stop the Server*

> From the `<Skybox_Home>/server/bin` directory, execute the following command:
> ./*stopserver.sh&

*To stop the Collector*

> From the `<Skybox_Home>/collector/bin` directory, execute the following command:
> ./*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 various data sources that you imported to the model.

**ENABLING PERL-BASED COLLECTORS**

Perl version 5.20 or higher must be installed on your machine:

> To run many collection tasks
> To import files in Skybox’s Integration XML (iXML) format into the model

Note: Perl is preinstalled on Skybox Appliance.

> (Windows) You can download the latest version of Perl from [http://www.activestate.com/activeperl/downloads](http://www.activestate.com/activeperl/downloads)
You can discover the installed version of Perl by executing the command `perl -v`. The 1st line of the output states the version.

› (Linux) You can download the latest version of Perl from

[https://www.perl.org/get.html](https://www.perl.org/get.html)

All 3rd-party libraries required for working with the iXML engine are installed as part of the Skybox installation.
Chapter 5

Installing additional Collectors

This chapter explains how to install the Skybox Collector by itself. There are several possible Collector installation scenarios, each of which requires a different installation process.

Before you start, check Collector system requirements (on page 29).

After you install a Collector, you must connect it to the Server. See Connecting Skybox Connectors (on page 30).

In this chapter

Installation environment ...................................................... 28
Installing the Collector on Windows ....................................... 28
Installing the Collector on Linux ............................................ 29
Collector system requirements ............................................. 29
Connecting Skybox Collectors .............................................. 30

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 28)</td>
</tr>
<tr>
<td>Linux</td>
<td>Installing the Collector on Linux (on page 29)</td>
</tr>
</tbody>
</table>

INSTALLING THE COLLECTOR ON WINDOWS

To install the Skybox Collector on Windows, you must:

▷ 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 17).
1 Run the installation file (SkyboxInstaller-<version#>-<build>.exe).

2 Follow the directions in the wizard.

The options that you must select in specific screens are listed in the following table. In all other places, either use the default option or make any necessary changes.

<table>
<thead>
<tr>
<th>Screen</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Install Set</td>
<td>Select Collector.</td>
</tr>
<tr>
<td>Choose Install Folder</td>
<td>Specify the installation directory.</td>
</tr>
<tr>
<td></td>
<td>Note: Installation under &lt;Drive&gt;:\Program Files (or any other path containing a space) is not supported.</td>
</tr>
<tr>
<td></td>
<td>If another (previous) version of Skybox is installed, do not install to the same directory.</td>
</tr>
<tr>
<td>Preferences</td>
<td>To run the Collector as a batch program rather than an OS service, clear Install as operating system service.</td>
</tr>
</tbody>
</table>

For instructions about starting the Collector, see Starting and stopping the Server and Collector (on page 24).

INSTALLING THE COLLECTOR ON LINUX

Before installing the Collector

Before installing the Collector on Linux, you must:

› Turn off previously installed versions of Skybox to prevent port collision
› Be the root user
› Install all required packages (see Installing packages (on page 21))

To install the Skybox Collector on Linux

› Use the installation procedure provided in Silent installation (on page 17).

For instructions about starting the Collector, see Starting and stopping the Server and Collector (on page 24).

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.

You should 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 23)).
Operating system

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

<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>Red Hat Enterprise Linux 6</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7</td>
</tr>
<tr>
<td>CentOS 6</td>
</tr>
<tr>
<td>CentOS 7</td>
</tr>
</tbody>
</table>

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

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>2 cores</td>
<td>8 cores</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>Available disk space (see note)</td>
<td>50 GB</td>
<td>100 GB</td>
</tr>
</tbody>
</table>

Note: Collectors that will be used for syslog collection require more disk space. For further information, contact Skybox Support.

CONNECTING SKYBOX COLLECTORS

After installing a Skybox Collector, you must:

› 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

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: Do not change the port value unless you also explicitly changed 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 it is 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, select either of the following options:

› Include several 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 several 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:
Chapter 7

Multi-tiered servers for Change Manager

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 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’s 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: Currently, the following scenarios are not supported: Skybox Server running on Linux and web servers running on Windows, and vice versa.
Chapter 8

Updating Skybox

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

You update Skybox by downloading a software update file from the Skybox update management server and then running the update tool (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.

To update the Skybox Vulnerability Dictionary, see Dictionary updates (on page 115).

In this chapter

Skybox update file .............................................................. 34
Downloading the update file ................................................. 34
Preparing to update ............................................................ 35
Updating the Server and local components ......................... 35
Updating remote components ............................................. 36
Updating multi-tiered servers ............................................. 36
Skybox licenses .................................................................. 37

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, read-me.txt, that contains information about the update.

DOWNLOADING THE UPDATE FILE

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

Note: If the Manager machine is configured to connect to the internet via a proxy, set the proxy settings before downloading an update file for the 1st time (select 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 current 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 the following sections:
- Preparing to update (on page 35)
- Updating the Server and local components (on page 35)

PREPARING TO UPDATE

Before running the Update tool:

1 Read the read-me.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.

2 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 65)).

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 located 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.*

5 **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.

6 **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’s 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 automatic update.

**UPDATING MULTI-TIERED SERVERS**

When working 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.

SKYBOX LICENSES

The Skybox license file is installed by uploading it to the Server. The license controls which Skybox products are available, the license expiration date, and the maximum size of the network model (for example, the maximum number of firewalls).

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 Security, save it on your file system and upload it to Skybox.

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.

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 obtain a new license. When 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. When the grace period expires, the Server is locked and you must obtain a new license to continue working with Skybox.

The following entities are limited according to Skybox products:

- **Firewall Nodes**: The license limits the number of physical and virtual devices in the Firewall Assurance workspace; relevant when using Skybox Firewall Assurance

  Note: The Add Firewalls Wizard does not permit you to exceed the licensed number of firewall nodes.

- **Network Nodes**: The license limits the number of network devices in the model; relevant when using Skybox Network Assurance

- **Virtual Nodes**: The license limits the number of virtual assets in the model; relevant when using Skybox Network Assurance in clouds and virtualized environments

- **Vulnerability Control Nodes**: The license limits the total number of assets in the model; relevant when using Skybox Vulnerability Control

The following table shows which entities are limited per Skybox product.

<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>Network Assurance</td>
<td>Network devices in the model</td>
</tr>
<tr>
<td></td>
<td>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 9

Uninstalling Skybox from a Linux machine

The following instructions explain how to uninstall Skybox from a machine running on CentOS or Red Hat Enterprise Linux.

To uninstall Skybox from a Linux machine

Execute the following commands using root permissions.

1. Uninstall the server service and the collector service:
   - `<Skybox_Home>/server/bin/uninstall_server_service.sh`
   - `<Skybox_Home>/collector/bin/uninstall_collector_service.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`
Product security

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

- Authenticating and securing communication between Skybox components and data collection devices
- Encrypting the saved XML files that contain your Skybox model
- Locking an account after 3 failed login attempts
- Verifying that the last use of your Skybox user name was legitimate
- Automatic Skybox Manager timeout after user inactivity

In this chapter

Communication and certificates ............................................ 40
Encryption ......................................................................... 43
Limiting login attempts ........................................................ 43
Security check: last login message ........................................ 43
Customizable login warning messages ................................... 43
User session timeout ............................................................ 44

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 (for example, the password) 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 42).
For information about changing the default keystore password, see Changing the default password of the keystore (on page 42).

Generating a self-signed certificate for Skybox

1. Connect to the server as the skyboxview user.
2. Navigate to the following directory: <Skybox_Home>\server\conf

**Important:** You must 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 using the following command and replacing each instance of the term `<string>` with the relevant text.
   
   **Note:** In this step and all following steps, replace `<version#>` with the JDK version (for example, 1.8.0_152d).

   ```
   ..\..\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 mykey1 -keypass skyboxview -keystore server.keystore -storepass skyboxview -validity 90
   ```
   
   **Note:** The keysize value (-keysize) and algorithm number (-sigalg) may vary.

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 `mykey1`.

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 mykey1 -keystore server.keystore -storepass skyboxview
   ```

7 Using the generated request file, follow the internal certificate request procedure to sign and obtain 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 mykey1 -file <certificate file> -keystore server.keystore -storepass skyboxview
   ```

11 Delete the predefined default key:

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

12 Add the CA root certificate to the customer cacerts keystore:

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

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

14 Restart all Skybox Servers, Collectors, and Managers.

**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 also import the RootCA certificate to their cacerts_customer.keystore.

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) indicates that 1 or more 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 current version number of the JDK.
2. Type the command:

```
keytool.exe -v -list -keystore ..\.\..\server\conf\client.keystore -keypass skyboxview
```

**Changing the default password of the keystore**

The following procedure 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*

1. Use the following command to move to the directory where the files are located:

   ```
   cd /opt/skyboxview/server/conf/
   ```

2. Enter the following command:

   ```
   Note: In this step and all following steps, replace <version#> with the JDK version (for example, 1.8.0_152d).
   
   ../../thirdparty/<version#>/bin/keytool -keypasswd -keystore server.keystore -alias skyboxkey
   
   Note: If the Change certificate procedure was done before this one, the alias should be changed to mykey1.
   ```

3. Enter the keystore password: (skyboxview).

4. Enter a new key password for `<skyboxkey>`. You will need to do this a second time, for confirmation purposes.
5 Enter the following command:
   
   ```
   ../../../thirdparty/<version#>/bin/keytool -storepasswd -keystore server.keystore
   ```

6 Enter the keystore password: (skyboxview).

7 Enter a new key password for <skyboxkey>.
   You will need to do this a second time, for confirmation purposes.

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

9 Start the Server.

**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 65).)

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

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

**LIMITING LOGIN ATTEMPTS**

By default, after 3 failed login attempts, the 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 amount of time for which the account is locked using the following properties in 

- `elapsed_lock_milliseconds`
- `retry_allowed`

**SECURITY CHECK: LAST LOGIN MESSAGE**

During the login process, Skybox Manager displays the date and time of the last successful login using your user name. For security reasons, check the date and time of this login to verify that the last 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 the login_warning_banner property in
> <Skybox_Home>/server/conf/sb_server.properties to the desired text.

You can add HTML tags to the text; it is not necessary to add the <html> and
</html> tags: they are added by Skybox.

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 the client_session_timeout property 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 11

User management

Skybox is a multi-user system. There is a predefined **Admin** user (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 ................................................................. 46
- Managing users and user groups ................................. 53
- Working with external authentication systems .................. 60
- Managing users externally using LDAP ......................... 61
- Changing the password for database clients .................. 62

**USER ROLES**

The 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><strong>Admins</strong> have permissions for all actions, including those that regular users do not.</td>
</tr>
<tr>
<td>Admin – Users</td>
<td>Same as <strong>Admin</strong> but functionality is limited to user administration only.</td>
</tr>
<tr>
<td>Admin – Operational</td>
<td>Same as <strong>Admin</strong> but functionality is limited to everything except user administration.</td>
</tr>
<tr>
<td>Admin – Vulnerability Control</td>
<td>Same as <strong>Admin</strong> but Skybox access is limited to Vulnerability Control and Threat Manager.</td>
</tr>
<tr>
<td>Admin – Assurance</td>
<td>Same as <strong>Admin</strong> but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.</td>
</tr>
<tr>
<td>User</td>
<td><strong>Users</strong> have permissions for all actions except administrative tasks (for example, user management and model building).</td>
</tr>
<tr>
<td>User – Vulnerability</td>
<td>Same as <strong>User</strong> but Skybox access is limited to users.</td>
</tr>
</tbody>
</table>
## Chapter 11  User management

### Role Description

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>Vulnerability Control and Threat Manager.</td>
</tr>
<tr>
<td>User – Assurance</td>
<td>Same as User but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.</td>
</tr>
<tr>
<td>Read-only User</td>
<td><strong>Read-only Users</strong> 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. <strong>Read-only Users</strong> can access Vulnerability Control, Threat Manager, Firewall Assurance, Change Manager, Network Assurance, or any combination of these products.</td>
</tr>
<tr>
<td>Read-only User – Vulnerability Control</td>
<td>Same as <strong>Read-only User</strong> but Skybox access is limited to Vulnerability Control and Threat Manager.</td>
</tr>
<tr>
<td>Read-only User – Assurance</td>
<td>Same as <strong>Read-only User</strong> but Skybox access is limited to Firewall Assurance, Change Manager, and Network Assurance.</td>
</tr>
<tr>
<td>Ticket User</td>
<td><strong>Ticket Users</strong> 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.</td>
</tr>
<tr>
<td>Web Ticket User</td>
<td><strong>Web Ticket Users</strong> can log in to Change Manager, where they can manage tickets. They cannot log in to the Manager GUI. This role is for Change Manager.</td>
</tr>
<tr>
<td>Web Ticket Requestor</td>
<td><strong>Web Ticket Requestors</strong> can create tickets (that is, submit change requests) in Change Manager and close tickets that they created. This role is for Change Manager.</td>
</tr>
<tr>
<td>Recipient</td>
<td><strong>Recipients</strong> can receive tickets, alerts, and reports. They cannot log in to Skybox or access any other Skybox features.</td>
</tr>
</tbody>
</table>

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

### Administrative users

The following table indicates which features and entities each type of Admin user can manage (create, modify, delete, and read). Further clarification is provided after the table.

<table>
<thead>
<tr>
<th>User role / 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>Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users, user groups, and user roles</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
<td>✓ (See note)</td>
<td>✓ (See note)</td>
</tr>
<tr>
<td>Triggers</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>System logs (read-only)</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### User role / Feature or Entity

<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>Tools &gt; Options &gt; Server Options</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Model instances (Live, What If, Forensics)</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

#### Vulnerability Control and Threat Manager related entities

<table>
<thead>
<tr>
<th>Vulnerability Control and Threat Manager related entities</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></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></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></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></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>Reports and analyses</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>Other</th>
<th>Admin</th>
<th>Admin – Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skybox Horizon</td>
<td>✓</td>
<td>No</td>
</tr>
</tbody>
</table>

In addition to this list, **Admin** users 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.

Note the following:
Chapter 11    User management

› **Admin – Vulnerability Control** users can only create users with the following roles:
  - 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 following table indicates the features and entities available to each type of **User** user role, and whether they can manage (create, modify, delete, and read) them or only read them. Further clarification is provided after the table.

<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><strong>Tools</strong></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>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Tools &gt; Options &gt; Manager Options</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Workspaces</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Control and Threat Manager</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>Firewall Assurance and Network Assurance</td>
<td>✓</td>
<td>No</td>
<td>✓</td>
</tr>
<tr>
<td>Model workspace</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Reports, tickets, and analyses</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public reports</td>
<td>Generate</td>
<td>Generate</td>
<td>Generate</td>
</tr>
<tr>
<td>Private reports</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tickets</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Public ticket analyses</td>
<td>Read only</td>
<td>Read only</td>
<td>Read only</td>
</tr>
</tbody>
</table>
### User role/Feature or Entity

<table>
<thead>
<tr>
<th></th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private ticket analyses</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 public 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>

### Operational Console

<table>
<thead>
<tr>
<th></th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collectors</td>
<td>Read only</td>
<td>Read only</td>
<td>Read only</td>
</tr>
<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></th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployed products</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<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></th>
<th>User</th>
<th>User – Vul Control</th>
<th>User – Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exceptions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Policy management (access, rule, and configuration policies)</td>
<td>Edit, export, import</td>
<td>Edit, export, import</td>
<td></td>
</tr>
<tr>
<td>Application &amp; Service repository</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

### Read-only users

The following table indicates the features and entities available to each type of **Read-only User** user, and whether they can manage (create, modify, delete, and read) them or only read them.

<table>
<thead>
<tr>
<th></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>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>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>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>
<tr>
<td>Firewall Assurance and Network Assurance related entities</td>
<td>Exceptions</td>
<td>Read only</td>
<td>No</td>
</tr>
</tbody>
</table>
### Custom user roles

Skybox provides the ability to create custom user roles for Firewall Assurance, Network Assurance, and Change Manager, 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

  **Note:** Since there are permissions for other features that are not included in the customization, it is recommended to start with the existing user role that is closest to the role that you want to create.

- For Change Manager, you can create a role based on **Web Ticket User** and define which tickets users of this role can view: tickets assigned to themselves, their group, or anyone.

**To create a custom user role**

1. From the **Tools** menu, select **Administrative Tools > User Roles**.
2. In the Admin window, click ![UserRole](UserRole.png).
3. Provide a name and description for the role.
4. Select the template: the existing user role that most closely describes the permissions that you want this new role to have.

The roles that can be used as templates are:

- **Admin – Assurance**
- **User – Assurance**
• Read-only – Assurance
• Web Ticket User

5 Adjust the permissions as necessary.

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

Default user
Skybox includes a predefined Admin user 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. For additional information, see Managing users externally using LDAP (on page 61).

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>General</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>This field is displayed only if LDAP authentication is enabled (see page 61). When users are managed using LDAP, specifies the name of the LDAP group or groups to match to this Skybox group. Specify the LDAP group name or use a comma-separated list. You can use * as a wildcard in the group names. Use Any rather than specifying a specific group name if this group is intended for all LDAP-managed users. See also Setting up Skybox user groups for LDAP users (on page 61).</td>
</tr>
</tbody>
</table>

Skybox version 9.0.100
### Property | Description
--- | ---
**Default Role** | This field is displayed only if **LDAP authentication is enabled** (see page 61). When users are managed using LDAP, specifies the Skybox role for those users. 
**Note:** When LDAP users belong to multiple Skybox groups, the highest default role is used.

**Group Members** | The users who are members of this group.

**Default Member** | If a ticket is promoted to this 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, open 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 58) 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 still 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 LDAP authentication is enabled (see page 61). Specifies whether this user is managed using LDAP. <strong>Note</strong>: Users who are managed in LDAP are added to the Skybox user table on their 1st login, to make their details available. The properties of these users are updated whenever 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. <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’s permissions in Skybox (see User roles (on page 46)).</td>
</tr>
<tr>
<td>First Name</td>
<td>User’s first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>User’s last name.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The method to use for authenticating this user (Skybox,</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Method            | LDAP, RADIUS, or SiteMinder).  
**Note:** This field is enabled only if an external authentication system is enabled (Tools > Options > Server Options > User Settings > Authentication).  
For additional information, see [Working with external authentication systems](on page 60). |
| Password          | The password this user must use when logging in to Skybox. The password must contain at least 8 characters, including:  
• At least 1 upper case letter  
• At least 1 lower case letter  
• At least 1 digit  
• At least 1 non-alphanumeric symbol  
The password must not contain the username 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 an attempt is made 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.                          |
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Permission)</td>
<td>Each permission consists of:</td>
</tr>
<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>

**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’s 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, you must select a new owner.

To change a user’s password

› Right-click the user in the Table pane and select **Change Password**.

The user can use the 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 108), **Admin** users 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), any Business Units or locations (in Vulnerability Control), and cannot view or edit any Change Request tickets (in Change Manager).

*Note: Admin users 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.

**Disabling and deleting inactive user accounts**

Skybox provides an option whereby users who are inactive for a specified amount of time are automatically disabled, and then deleted from Skybox after an additional amount of time. 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 of time after which inactive users should be disabled, and the period of time after which users who are still inactive should be deleted from Skybox.
3. Specify the user who should receive all tickets belonging to users who were disabled or deleted.

WORKING WITH EXTERNAL AUTHENTICATION SYSTEMS

By default, Skybox’s 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®

When Skybox is integrated with these systems, their users log in to Skybox using their SiteMinder, RADIUS, 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

2. Select Support External Authentication and then select the types of external authentication to use.
3. Fill in the fields as described in Authentication (on page 102).

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`.

**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.

To integrate an external user management system with Skybox, set up Skybox:

1. **Enable user management using LDAP** (see page 61).
2. **Set up Skybox user groups for the LDAP users** (see page 61).

These user groups define the role of the LDAP users in Skybox.

**Enabling user management using LDAP**

To enable user management using LDAP

1. Select **Tools > Options > Server Options > User Settings > Authentication**. Make sure that an LDAP server is defined.
2. Select **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**

You must 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—including what permissions 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 example below 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 LDAP_default_group_name property to be the name of the default LDAP user group.

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 can become a member of all the matching Skybox groups.

For example, if Skybox includes the following user groups 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 1 LDAP user is a member of the following LDAP user groups: IT_Europe, IT_World, and Everybody, then in Skybox, this user is a member of the following Skybox user groups: GroupA, GroupC, and GroupE.

Authentication to a super domain

When Active Directory includes multiple forests, it is possible to represent the domain name in Skybox using an asterisk ‘*’ character in the LDAP_root_DN property. The ‘*’ character (if present) is replaced by the domain name. In such cases, the user must login with <domain name>\<user name>.

CHANGING THE PASSWORD FOR DATABASE CLIENTS

The following instructions explain 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 enter the following commands to set the new password:
   - For the root user:
     ```
     ALTER USER 'root'@'localhost' IDENTIFIED BY 'newrootpassword';
     ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY 'newrootpassword';
     ALTER USER 'root'@'::1' IDENTIFIED BY 'newrootpassword';
     ```
   - For the skyboxview user:
     ```
     ALTER USER 'skyboxview'@'localhost' IDENTIFIED BY 'newSBpassword';
     ALTER USER 'skyboxview'@'127.0.0.1' IDENTIFIED BY 'newSBpassword';
     ALTER USER 'skyboxview'@'::1' IDENTIFIED BY 'newSBpassword';
     ALTER USER 'skyboxview'@'localhost.localdomain' IDENTIFIED BY 'newSBpassword';
     ```
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 SHA1 and AES128 upon Server start.
Chapter 12

Backup and restore

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

In this chapter

Backup and restore scenarios ............................................... 64
About the model ..................................................................... 64
Backing up the model .......................................................... 65
Fast backup ....................................................................... 66
Back up to an external location ............................................ 67
Loading a model ................................................................... 67
Restoring the model ............................................................ 68

BACKUP AND RESTORE SCENARIOS

This chapter explains how to prepare for and deal with the following situations:

▶ Restoring the model on a working Server
  You can load an old version of the model if you need 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 65).

▶ 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 67) and Restoring the model (on page 68).

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.

The What If model is used 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.

You must back up and load each of these models separately. In general, changes made to one model are not copied to the other models; the only exception is the structure of the Access Policy, where changes are made in all the models.

Using Skybox Manager, you can switch between models as necessary. 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. When fast backup (see page 66) is enabled, you can back up in SQLX (encrypted SQL) format.

When you back up the model, you can choose 1 or more 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 plus various settings files.

- The model is saved as:
  \[\text{<Skybox\_Home>\data\xml\_models\xml\_backup\_task\_<date>--\<time>.xmlx}\]

- The settings files are saved as:
  \[\text{<Skybox\_Home>\data\settings\backup\settings\backup\_<date>--\<time>.zip}\]

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 \text{<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:
   - Select the model to back up (Live, What If, or Forensics).
b. Type a name for the file.

c. Clear the check boxes 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. Click **OK**.

The file is saved (on the Server) in `<Skybox_Home>\data\xml_models` with the extension `xmlx`. When 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>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>The type of model to be backed up or loaded.</td>
</tr>
<tr>
<td>Type</td>
<td>This field is displayed only if fast backup (see page 66) is enabled.</td>
</tr>
<tr>
<td></td>
<td>The type of the backup.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Fast backup (see page 66) is currently an advanced option that should only be used with the guidance of Skybox Professional Services.</td>
</tr>
<tr>
<td>File Name</td>
<td>Type a name for the file to contain the backup.</td>
</tr>
<tr>
<td>File</td>
<td>Select the file to load.</td>
</tr>
<tr>
<td><strong>Save Scope / Load Scope</strong></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>
</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>
</tr>
<tr>
<td>Users</td>
<td>Specifies whether to back up or load users existing in Skybox.</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 115).</td>
</tr>
<tr>
<td>Save copy to a local directory</td>
<td>Specifies whether to back up an additional copy of the model to the Manager file system and the backup location.</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.

**Note**: This feature is currently in beta version.
Turning on fast backup

The fast backup option is hidden by default.

To turn on fast backup

> Set the db_sqlx_backup_mode property in
  <Skybox_Home>\server\conf\sb_server.properties to true.

Limitation

Often, even minor software updates to Skybox change the database schema of
the model. Until further notice, Skybox cannot load a SQL model with an old
schema. 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 if loading a SQL model fails.

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.

BACKING UP TO AN EXTERNAL LOCATION

It is recommended to 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 Back Up Model and Settings task to back up the model. Files
generated using the task include a timestamp in their names.

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 further
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 current 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 a large number of 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 is 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:
   a. Run: `<Skybox_Home>/server/bin/install_server_service.bat`
   b. Run: `<Skybox_Home>/server/bin/install_collector_service.bat`
   c. Run: `<Skybox_Home>/server/bin/startserver.exe`
   d. Run: `<Skybox_Home>/collector/bin/startcollector.exe`
   a. Run (as root): `<Skybox_Home>/server/bin/install_server_service.sh`
   b. Run (as root): `<Skybox_Home>/server/bin/install_collector_service.sh`
   g. Run (as root): `service sbvserver start`
h. Run (as root): `service sbvcollector start`

7 Log in to the Skybox Manager as the default user (**skyboxview**).

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 13

Administration via CLI commands

You can perform some common administrative tasks either via the Manager GUI or via utilities run from the command line. This chapter documents the CLI utilities. You must 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 ............................................. 70
Launch tasks ...................................................................... 71
Load the latest Dictionary .................................................... 71
Package log files .................................................................. 71
Scan log files ...................................................................... 72
Save the model .................................................................. 76
Load the model .................................................................. 77
Restore model settings ......................................................... 78

PACKAGE FIREWALL CONFIGURATIONS

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

The zipped output is split into 5MB zipped 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.
### Argument Description

- **-c <case ID>**
  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 `firewall1_<date>_organization_name_12345.zip`.

- **-f <firewall IDs>**
  A comma-separated list of firewall EIDs. The list must be enclosed in double quotes. The EID is the Skybox ID number of the firewall in the model. 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 5MB.

### LAUNCH TASKS

The `launchtask` utility launches a Skybox task. You must specify the name of the task. If the name includes spaces, surround it with double quotes.

**Syntax**

```
launchtask.bat "["<task name>["]
```

### LOAD THE LATEST DICTIONARY

The `loaddictionary` utility loads the latest Skybox Vulnerability Dictionary from the internet. This utility has no arguments.

**Syntax**

```
loaddictionary.bat
```

### PACKAGE LOG FILES

The `packlogs` utility packages the 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.

You might need to do this for the Skybox Server, the Skybox Collector, and the Skybox Manager if they are on separate machines. The utility for each product is located under its `bin` directory (`<Skybox_Home>\<component>\bin`, where `<component>` is server, collector, or app).

The output file is named `<component>_packlogs_<date>_organization_name[_caseID].zip`.
**Syntax**

```bash
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>-m</td>
<td>Include the latest XMLX model found under <code>&lt;Skybox_Home&gt;\data\xml_models</code>. If you specify -m and -q, the utility packages the latest SQML model only.</td>
</tr>
<tr>
<td>-q</td>
<td>Include the latest SQLX model found under <code>&lt;Skybox_Home&gt;\data\sqlx_models</code>.</td>
</tr>
<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.</td>
</tr>
<tr>
<td>-o &lt;offset&gt;</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>-p</td>
<td>Split the zipped output into ZIP files of 5MB 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. This is useful if the output is very large.</td>
</tr>
<tr>
<td>-s</td>
<td>(Default) Generate a single ZIP file.</td>
</tr>
</tbody>
</table>

**SCAN LOG FILES**

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

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

**Syntax**

```bash
scanlogs
```

The following system faults can be detected using this utility.

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Description</th>
<th>Action / Contact</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 and memory usage of 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>Action / Contact</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. It may cause a slowdown or even total hang in extreme cases.</td>
<td>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 suggest memory issues, OS issues, Java software bugs, or even hardware instability.</td>
<td>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’s sender as necessary</td>
</tr>
<tr>
<td>5</td>
<td>Long debug lines</td>
<td>Very long debug lines suggest that some very large data is being mistakenly written into the debug log.</td>
<td>Skybox R&amp;D</td>
</tr>
<tr>
<td>6</td>
<td>Debug message flood</td>
<td>The debug log files may be rotating very fast, with too many debug messages being written in a very short time.</td>
<td>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 lead to 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 been defined with a small swap space, which might cause instability if memory usage spikes. On Linux, this might trigger OOM killer incidents which can be seen in /var/log/messages.</td>
<td>The fault can be ignored if no other symptoms are present. Otherwise swap space should be modified by Skybox Professional Services. 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. Important: If the partition is hosting a Skybox installation, the issue is of critical importance.</td>
</tr>
<tr>
<td>10</td>
<td>Corrupt property files</td>
<td>A Skybox property file was corrupted.</td>
<td>Contact Skybox Professional Services. The file may have to be restored from backup.</td>
</tr>
<tr>
<td>#</td>
<td>Name</td>
<td>Description</td>
<td>Action / Contact</td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>11</td>
<td>Slow tasks</td>
<td>Extremely slow tasks.</td>
<td>Contact Skybox Professional Services. It may need to be handled as a bug by Skybox R&amp;D.</td>
</tr>
<tr>
<td>12</td>
<td>Low Xmx</td>
<td>The Server may have been misconfigured to use a low Xmx memory limit in jvmargs.properties, but the host machine has much more RAM available.</td>
<td>Skybox Professional Services</td>
</tr>
<tr>
<td>13</td>
<td>High Xmx</td>
<td>The Server may have been misconfigured to use a high Xmx memory limit in jvmargs.properties, but the host machine has much less RAM available.</td>
<td>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>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 one configured in jvmargs.properties. This typically happens on Windows if the Skybox service was not reinstalled after changing the value.</td>
<td>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>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>Skybox Professional Services</td>
</tr>
<tr>
<td>18</td>
<td>Server port already in use</td>
<td>At some point, 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>At some point, there was a port 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>Indicates 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>Action / Contact</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</td>
<td>Skybox Professional Services should check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>refers to local host name, the DNS settings of the host machine may be</td>
<td>C:\Windows\System32\drivers\etc\hosts (on Windows) or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>incorrect.</td>
<td>/etc/hosts (on Linux).</td>
</tr>
<tr>
<td>22</td>
<td>Unassociated entities</td>
<td>Indicates a problem in the referential integrity of the Skybox model, and</td>
<td>Usually should be handled as a bug by Skybox R&amp;D to find</td>
</tr>
<tr>
<td></td>
<td></td>
<td>implies a potential corruption to data. It might be caused by sub-entities</td>
<td>the root cause.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>that were left behind after the deletion of a parent entity or it could be</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>caused by inadvertent disappearance of model entities.</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>No daily backups</td>
<td>Indicates that no daily backups of model data have taken place recently.</td>
<td>Skybox Professional Services</td>
</tr>
<tr>
<td>24</td>
<td>Slow interactive calls</td>
<td>Lists all slow interactive calls from the various clients. Each call is</td>
<td>Frequent calls that have a long average duration should be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>listed with its most recent duration, as well as the average duration and</td>
<td>handled as a bug by Skybox R&amp;D.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the number of worst calls that have been processed recently by the server.</td>
<td></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></td>
<td></td>
<td></td>
<td>It may need to be handled as a bug by Skybox R&amp;D.</td>
</tr>
<tr>
<td>26</td>
<td>Server logic errors</td>
<td>Indicates errors in Skybox Server logic. A count of each error type is</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provided. The severity of this fault varies depending on the context and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>may well be inconsequential.</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Collector logic errors</td>
<td>Indicates errors in Skybox Collector logic. A count of each error type is</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provided. The severity of this fault varies depending on context and may</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>well be inconsequential.</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>App logic errors</td>
<td>Indicates errors in Skybox Manager logic. A count of each error type is</td>
<td>Contact Skybox R&amp;D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provided. The severity of this fault varies depending on context and may</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>well be inconsequential.</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>MySQL data truncation</td>
<td>Indicates that the size of a specific MySQL column is too small for the</td>
<td>Contact Skybox R&amp;D for a temporary MySQL schema workaround</td>
</tr>
<tr>
<td></td>
<td></td>
<td>intended data, which may result in localized data corruption.</td>
<td>and a permanent fix</td>
</tr>
<tr>
<td>#</td>
<td>Name</td>
<td>Description</td>
<td>Action / Contact</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>30</td>
<td>Server linkage</td>
<td>Indicates a problem with the Java class files of the Server, and may suggest a deployment issue such as 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>linkage errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Collector linkage</td>
<td>Indicates a problem with the Java class files of the Collector, and may suggest a deployment issue such as 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></td>
<td>linkage errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Server deployment</td>
<td>Indicates that the Server failed to start up correctly. There are many possible causes.</td>
<td>Skybox Professional Services</td>
</tr>
<tr>
<td></td>
<td>errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Collector deployment</td>
<td>Indicates that the Collector failed to start up correctly. There are many possible causes.</td>
<td>Skybox Professional Services</td>
</tr>
<tr>
<td></td>
<td>errors</td>
<td></td>
<td></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>Skybox Professional Services</td>
</tr>
</tbody>
</table>

### SAVE THE MODEL

The `save2xml` utility saves a Skybox model to an XML file. You can select which parts of the model to save and which model to save: Live, Forensics, or What If. By default, the Live model is saved.

### Syntax

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

The command to export all the information in the Live model plus the 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 unless you use the -plaintext option (in which case it 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>
</tbody>
</table>
Chapter 13  Administration via CLI commands

Argument Description
-coreusers Include user data from the Skybox model.
-dic Include the Skybox Vulnerability Dictionary from the Skybox model.
Note: Unless you need this specific Dictionary, do not save it. You can always load the latest Dictionary via loaddictionary.bat.
-forensics Save the specified data from the Forensics model rather than from the Live model.
-whatif Save the specified data from the What If model rather than from the Live model.
-plaintext Do not encrypt the XML file.

LOAD THE MODEL

The load utility loads a saved model to Skybox. You can specify which parts of the model to load and to which model in Skybox you want 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. Note: The default path for the file is &lt;Skybox_Home&gt;\data\xml_files. To load the file from a different location, include the full path name.</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. Note: Unless you need the specific Dictionary that was saved in the past, it is better to load the latest Dictionary via loaddictionary.bat. Note: This argument cannot be used with -whatif or -forensics.</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| -whatif  | Load the specified data to the What If model rather than the Live model in Skybox.  
**Note**: This argument cannot be used with -dic. |
| -forensics | Load the specified data to the Forensics model rather than the Live model in Skybox.  
**Note**: This argument cannot be used with -dic. |

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 68).
Chapter 14

Manager options

This chapter explains how to configure options for the Skybox Manager using the GUI.

To configure the options, select **Tools > Options > Manager Options**.

In this chapter

- **Access Analyzer: Manager** ................................................................. 79
- **Messages** .................................................................................. 79
- **Model Validation Status Settings** ................................................. 80
- **Proxy Settings (Manager)** ............................................................. 80
- **Regional Settings: Manager** ....................................................... 81
- **Reports Configuration** ................................................................. 81
- **Risks Configuration** .................................................................... 81
- **View Settings** ................................................................................ 81

**ACCESS ANALYZER: MANAGER**

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use existing entities only</td>
<td>Specifies whether to display results using only assets and services that exist in the model.</td>
</tr>
<tr>
<td></td>
<td>• Clear this option if you want the results of access analysis to include IP addresses that might be added to the network.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Display all blocking rules</td>
<td>Specifies whether, for blocked routes all access rules that potentially block traffic on the selected route are displayed.</td>
</tr>
<tr>
<td></td>
<td>If cleared, only the 1st access rule that blocks traffic on the selected route is displayed.</td>
</tr>
</tbody>
</table>

**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 80)).</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.

You must 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:
   - Set the max_num_of_validation_messages_per_entity property in <Skybox_Home>\server\conf\sb_common.properties to a non-zero value.
2. Enable displaying the messages in Skybox:
   a. Select 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 the proxy server for HTTP connections to the internet. The proxy server is used by tasks that retrieve information from the internet.

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 for the proxy server for the HTTP.</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>The TCP port at which the proxy waits 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 95).

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’s 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</td>
<td>Risk values are presented as icons.</td>
</tr>
<tr>
<td>- Monetary (value)</td>
<td>Risk values are presented as monetary values. Only an Admin can specify the currency unit, see Regional Settings (on page 95).</td>
</tr>
<tr>
<td>- Score (0-100)</td>
<td>Risk values are presented as a score between 0 and 100.</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>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>

Note: You must restart the Manager to apply these changes.
Chapter 15

Server options

This chapter explains how to configure options for the Skybox Server using the GUI.

Note: Only an Admin can change Server options.

To configure the Server options, select Tools > Options > Server Options.

In this chapter

Access Analyzer: Server ...................................................... 84
Access Compliance .............................................................. 84
Archiving ........................................................................... 85
Asset Modification Settings ................................................... 85
Attack Simulation Configuration ............................................ 86
Business Attributes ............................................................. 86
Change Manager Settings .................................................... 86
Change Tracking Settings .................................................... 92
Customization .................................................................... 93
Dictionary Settings .............................................................. 93
Entity Settings .................................................................... 94
License .............................................................................. 94
Proxy Settings (Server) ....................................................... 94
Regional Settings: Server .................................................... 95
Report Configuration ........................................................... 95
Rule Usage .......................................................................... 96
Software Update Settings .................................................... 96
System .............................................................................. 97
Task Settings ..................................................................... 98
Threat Manager ................................................................. 100
Ticket Configuration ........................................................... 100
User Settings .................................................................... 102
Vulnerability Control ........................................................... 109
Worm Settings .................................................................... 110
### ACCESS ANALYZER: SERVER

The properties that you can set 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's name when locations are hidden in the results tree.</td>
</tr>
</tbody>
</table>

### ACCESS COMPLIANCE

The properties that you can set 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’s 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 that you can set in the 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, Default Gateway/Unknown Addresses is used).</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</td>
</tr>
</tbody>
</table>
For additional information about addresses behind interfaces, see the Addresses behind network interfaces topic in the Skybox Firewall Assurance User’s 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 Model – Outdated Removal 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 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 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 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 changed 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>
</table>
| Mark Changed Assets | (In What If and Forensics models) Specifies whether users are notified if another user
ATTACK SIMULATION CONFIGURATION

The properties that you can set 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 (for example, its owner and business function).

Access Rules

The properties in the 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. You can use (or delete) these and add your own. Click Add to add a new business attribute.</td>
</tr>
</tbody>
</table>

Assets

The properties in the 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. You can use (or delete) these and add your own. Click Add to add a new business attribute.</td>
</tr>
</tbody>
</table>

CHANGE MANAGER SETTINGS

The properties in the Change Manager Settings page configure settings that 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 that 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 that 2 fields of the change request must be...</td>
</tr>
</tbody>
</table>
### Property Description

- **Include contained in Any**
  Specifies whether to include matches where fields of the change request are contained within a field whose value is Any.

---

### Change Manager Mode

**(Firewall identification mode)**
Controls whether firewalls in change requests are identified in **Firewall Mode** or **Network 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.

- **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)**
Controls whether policy compliance violations in Change Manager are calculated in **Firewall Mode** or **Network 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 to calculate policy compliance violations.

### Verification
- **Source and destination interface**

---

### Change Requests

The properties in the 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>Enables users in Change Manager to upload Access Update change requests to a ticket from a file. After checking this box, you must map the parameters of the change request to the column names in the file specified in <strong>File Name</strong>.</td>
</tr>
<tr>
<td>Enable uploading change requests from files</td>
<td></td>
</tr>
<tr>
<td><strong>File Name</strong></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>
Property | Description
---|---
**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 page.
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 Display Settings page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Records Per Page</strong></td>
<td>Records per page</td>
</tr>
<tr>
<td><strong>Custom Fields</strong></td>
<td>Number of custom fields in a row</td>
</tr>
</tbody>
</table>

**Implementation Automation**
The properties in the Implementation Automation page are described in the following table.
### Server options

#### Chapter 15

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic implementation of pending requests for Check Point devices</td>
<td>Specifies whether Change Manager automatically implements pending change requests for Check Point devices.</td>
</tr>
<tr>
<td>Suggest implementing relevant requests</td>
<td>Specifies whether, when implementation is requested, Change Manager should ask 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 logging</td>
<td>Indicates whether new rules implemented on firewalls have logging enabled.</td>
</tr>
<tr>
<td>Rule Position</td>
<td>(Read-only) The position of the rule in the ACL. Note: New rules are always positioned at the end of the policy.</td>
</tr>
<tr>
<td>Rule VPN</td>
<td>(Read-only) The VPN that the rule uses. Note: New rules are set with VPN=Any.</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>
</tbody>
</table>

For more information about implementation automation, including how to set it up in the Check Point SmartDashboard application, and which types of change requests can be implemented automatically, see the Configuring implementation automation section in the Skybox Change Manager User’s Guide.

### Object Suggestion

The properties in the Object Suggestion page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convert addresses and services to objects</td>
<td>Specifies whether to convert all addresses and services in change requests to objects. <strong>Note:</strong> Existing objects are used when an exact match is found. Otherwise new objects are created.</td>
</tr>
<tr>
<td>Naming conventions</td>
<td>The following fields set the naming conventions for new objects.</td>
</tr>
<tr>
<td>Host</td>
<td>Host object names must include the &lt;IP&gt; tag.</td>
</tr>
<tr>
<td>IP Range</td>
<td>IP range object names must include the &lt;IP_RANGE&gt; tag.</td>
</tr>
<tr>
<td>Network</td>
<td>Network object names must include the &lt;NETWORK&gt; tag.</td>
</tr>
<tr>
<td>Service</td>
<td>Service objects must include the &lt;SERVICE&gt; tag.</td>
</tr>
</tbody>
</table>
Property | Description
--- | ---
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.

**Requestor Permissions**

The properties in the Requestor Permissions page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the permitted request types for the Web Ticket Requestor role</td>
<td>The types of change requests that Web Ticket Requestors can open.</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>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>
</tbody>
</table>

**Risk Assessment**

The properties in the Risk Assessment page are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 panel 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>
</tbody>
</table>
**Property** | **Description**
--- | ---
**Occurrences** |  
**Approve Risk** |  
Set the default approval expiration date ... based on risk levels | The default expiration date of exceptions for each risk level.

**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. These expiration dates are used 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 organization’s policy.

**Tickets**

The properties in the Tickets page configure settings that affect tickets in Skybox Change Manager.

The Tickets properties are described in the following table.

**Property** | **Description**
--- | ---
**Automatic closure of tickets** |  
Automatically close resolved tickets if all change requests were implemented | Specifies whether Access Change tickets are closed automatically after all their change requests are implemented.

Automatically close tickets in the last phase for more than <n> days | Specifies whether Access Change tickets are closed automatically if they are in the last phase (usually named Verified) for more than a given number of days.

Set status of automatically closed tickets to | Specifies the status to which tickets are set when they are automatically closed.

**Default ticket priority** |  
Default priority of newly created tickets | Specifies the default priority for new tickets.
Workflows

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Workflows)</td>
<td>Click <strong>Add</strong> to add a new workflow using the wizard. Select <strong>Add &gt; Template Workflow</strong> to add another standard workflow (which you can then edit). Double-click an existing workflow to edit it. For additional information about workflows, see the Customizing ticket phases and workflows section in the Change Manager User’s Guide.</td>
</tr>
</tbody>
</table>

**Default Work Time**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Week</td>
<td>Specifies the work week for your organization. Only these days are used to calculate ticket due dates for workflows based on the default work time.</td>
</tr>
</tbody>
</table>
| 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. Only these hours are used to calculate ticket due dates for workflows based on the default work time. |

CHANGE TRACKING SETTINGS

The properties that you can set 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 <strong>Comments</strong> field of access rules and objects.</td>
</tr>
</tbody>
</table>
| Ticket ID Regex | Specifies the regular expression used to extract the ticket ID.  
  **Note**: The default regular expression represents a 5-digit number.  
  You can find information about regular expressions at [http://www.regular-expressions.info/](http://www.regular-expressions.info/)  
  **Note**: Changes to the regular expression are relevant for future change tracking records only. Existing records are not affected. |

**Change Reconciliation**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable change reconciliation            | Specifies whether to enable the Change Reconciliation feature.  
  **Note**: Selecting this property enables the other fields in this section. |
### Chapter 15    Server options

#### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Pending changes are automatically unauthorized within &lt;n&gt; days</td>
<td>Specifies the number of days to leave changes in the Pending state. After this number of days, the status of Pending changes becomes Unauthorized.</td>
</tr>
<tr>
<td>Pending changes that haven’t started the reconciliation process are automatically unauthorized within &lt;n&gt; days</td>
<td>Specifies whether change tracking analysis attempts to match changes and Skybox tickets by external ticket IDs.</td>
</tr>
<tr>
<td>Enable auto-matching by ticket ID</td>
<td>Specifies whether change tracking analysis attempts to match changes and Skybox tickets by external ticket IDs.</td>
</tr>
<tr>
<td>Enable auto-matching by addresses &amp; ports</td>
<td>Specifies whether change tracking analysis attempts to match changes and Skybox tickets by IP addresses and ports.</td>
</tr>
</tbody>
</table>

### CUSTOMIZATION

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>Specifies the URL that opens when users click the logo at the top-right of the Change Manager or Skybox Horizon page.</td>
</tr>
<tr>
<td>Website Address</td>
<td>Specifies the URL that opens when users click the logo at the top-right of the Change Manager or Skybox Horizon page.</td>
</tr>
<tr>
<td>Logo Image</td>
<td>The logo to be shown at the top-right of the Change Manager or Skybox Horizon page.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Reset to Default</strong> if you want to reset the logo to the Skybox Security logo at any point.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The logo must be in PNG format and should be 112 x 43 pixels. Images at other sizes are resized to 112 x 43 for display.</td>
</tr>
<tr>
<td>Message of the Day</td>
<td>The message to display after a user logs in to Skybox Change Manager.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The following tags cannot be used in the message: &lt;html&gt;, &lt;body&gt;, &lt;header&gt;, &lt;script&gt;.</td>
</tr>
</tbody>
</table>

### 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.

**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 the proxy server for HTTP connections to the internet. The proxy server is used by tasks that retrieve information from the internet.

The Proxy Settings (Server) properties are described in the following table.
### Chapter 15  
**Server options**

<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>The IP address for the proxy server for the HTTP.</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>The TCP port at which the proxy waits for HTTP requests.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the interface to use for updating the Skybox Vulnerability Dictionary.</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>
<tr>
<td><strong>NTLM authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>The domain to use for NTLM authentication.</td>
</tr>
<tr>
<td>Client Host Name</td>
<td>The name of the client host for NTLM authentication.</td>
</tr>
<tr>
<td>Enable NTLM v2</td>
<td>Specifies whether to enable NTLM v2.</td>
</tr>
</tbody>
</table>

### 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><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Locale</td>
<td>Specifies how Skybox displays numbers, dates, and time of day.</td>
</tr>
<tr>
<td>Currency</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 81).

### REPORT CONFIGURATION

The properties that you can set in the Report Configuration page are described in the following table.

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

The properties in the 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></td>
<td><strong>Note</strong>: 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 usage 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 what percentage of use is considered poor usage (Critical), fair usage, and good usage.

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>Indicates that disabled access rules are not shown in rule usage views, reports, or counters.</td>
</tr>
<tr>
<td>Usage Levels</td>
<td>Specifies the usage levels for 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></td>
<td>(These examples are based on the default values.)</td>
</tr>
</tbody>
</table>

SOFTWARE UPDATE SETTINGS

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><strong>Note</strong>: If remote software updating is disabled, the Server does not check whether the versions of the Managers and Collectors match its own version and you must apply patches for Managers and Collectors locally.</td>
<td></td>
</tr>
<tr>
<td>Enable automatic update of Skybox Collectors</td>
<td>Specifies whether Skybox checks Collector versions and update Collectors after the Server is updated.</td>
</tr>
</tbody>
</table>
SYSTEM

The properties in the System pages configure various system-level settings (for example, emails (on page 97) and system events (on page 98)).

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block simultaneous sessions of a single user on different machines</td>
<td>Specifies whether a single user is permitted to be logged in on several machines at the same time. In many organizations, this is forbidden for security reasons.</td>
</tr>
</tbody>
</table>

Backup Settings

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Encryption Password</td>
<td>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, the default password is used. You can change the password if required for security purposes. However, if you change the password you cannot load models encrypted with the previous password.</td>
</tr>
</tbody>
</table>

**Warning**: It is recommended to *not* change this password unless required by your organization's security policy.

Email Configuration

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>The server used by Skybox to send messages.</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>The SMTP server port used by Skybox.</td>
</tr>
<tr>
<td>Mail Server Authentication</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>The user name for mail server authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for mail server authentication.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password for mail server authentication.</td>
</tr>
<tr>
<td>Email Address</td>
<td>The email address from which Skybox messages are sent.</td>
</tr>
<tr>
<td>Email Caption</td>
<td>The email caption from which Skybox messages are sent.</td>
</tr>
<tr>
<td>Test Message</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Events and Triggers**

The properties in the 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>Specifies whether to send Skybox events to remote logging servers.</td>
</tr>
<tr>
<td>Send System Events</td>
<td>A comma-separated list of the names or IP addresses of the remote logging servers, with the format &lt;servername&gt;[:&lt;port&gt;] or nnn.nnn.nnn[:&lt;port&gt;]. The default port is 514.</td>
</tr>
<tr>
<td>Remote Logging Server</td>
<td>The type of events to send</td>
</tr>
<tr>
<td></td>
<td>• <strong>System</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Audit log</strong>: Specifies whether to send events that go to the audit log. These are user-related events.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Activity log</strong>: Specifies whether to send activity log events. These events include many Skybox actions.</td>
</tr>
<tr>
<td>The format of the sent messages</td>
<td>Specifies whether to send messages that match the format of the Skybox Server's operating system.</td>
</tr>
<tr>
<td>Triggers</td>
<td>Controls the frequency at which overdue notifications are sent. Select a frequency and then define the schedule.</td>
</tr>
</tbody>
</table>

For additional information, see **System logs** (on page 117).

**TASK SETTINGS**

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

**Global Task Settings**

The properties in the 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><strong>Exclude Devices</strong></td>
<td>A list of devices that are not to be imported into the model. These devices are ignored whenever you run an offline file import task.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Add</strong> to add names of devices to exclude. This creates a basic exclude list.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Add &gt; Advanced Exclude</strong> to create a list of assets to exclude based on specific filters such as asset type, operating system, and features.</td>
</tr>
<tr>
<td></td>
<td>Double-click an existing entity in the list (single device or filter list) to edit it.</td>
</tr>
</tbody>
</table>
### Property Description

**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 following filters can be used in an advanced exclude list:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Name</td>
<td>Names of assets to exclude from the model (regular expression).</td>
</tr>
<tr>
<td>Network Scope</td>
<td>Networks to exclude from the model.</td>
</tr>
<tr>
<td>Asset Type</td>
<td>Types of assets to exclude from the model.</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Operating systems to exclude from the model.</td>
</tr>
<tr>
<td>OS Vendor</td>
<td>OS vendors to exclude from the model.</td>
</tr>
<tr>
<td>Features</td>
<td>Indicates that Assets with the selected features are excluded from the model.</td>
</tr>
<tr>
<td>No Services</td>
<td>Indicates that assets should only be excluded from the model if they have no services. (When this is selected, the Services filter cannot be used.)</td>
</tr>
<tr>
<td>Services</td>
<td>Indicates that assets with the specified services should be excluded from the model.</td>
</tr>
<tr>
<td>Products</td>
<td>Indicates that assets with these products should be excluded from the model.</td>
</tr>
</tbody>
</table>

### Task Alert Settings

The properties in the 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’s alert messages. When 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><strong>External Alert Source</strong></td>
<td>The alert source for which Vulnerability Definitions are displayed in the Threat Manager workspace.</td>
</tr>
<tr>
<td><strong>Threat Alert Mode</strong></td>
<td>When 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. <strong>Note</strong>: 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>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Name</td>
<td>The source name to display for custom Vulnerability Definitions.</td>
</tr>
<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 Threat Manager User’s Guide.

TICKET CONFIGURATION

The properties that you can set 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><strong>Synchronize model with tickets</strong></td>
<td></td>
</tr>
<tr>
<td>Synchronize Model with Processed 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 <strong>Fixed</strong> and changing the asset or service to reflect the <strong>selected solution</strong>. (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>
</tbody>
</table>

**Attachments**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Synchronization</td>
<td>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.</td>
</tr>
</tbody>
</table>
About ticket priority levels

When 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.

When 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 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 title of the field, type of field (String, Number, Boolean, or Date), and the ticket types to which the field applies.</td>
</tr>
</tbody>
</table>

Custom Ticket Statuses

The properties in the 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 defining custom ticket statuses, you must specify a status group value (Open, Done, or Invalid) for each custom status.

Note: Blank custom statuses are not used and do not appear in the list of statuses displayed to users.

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.</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</td>
</tr>
</tbody>
</table>
priority levels, you can disable levels 4 and 5.

**Note:** When 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.

**Ticket Phases**

**Ticket Type**
The type of tickets for which to use the phases specified in **Phase List**.
Each ticket type can have a separate phase list.

**(Phase List)**
This table is not displayed if **Ticket Type** = **Access Change**.
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 last phase (named **Verification** by default) is added automatically and cannot be deleted unless all other phases are deleted.

**Ticket CC List**

**Manage ticket cc lists automatically**
Specifies whether to add users to the cc list of tickets automatically.
If you select this option, the following users are added to the cc list:
- Ticket creator
- Ticket owner
- Rule owner
- 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 following sections:

- The Ticket phases and due dates section in the Skybox Threat Manager User’s 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.

**USER SETTINGS**

**Authentication**
The properties in the 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 an external method of authentication in addition to Skybox authentication.</td>
</tr>
</tbody>
</table>
Chapter 15 Server options

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Specifies whether authentication using LDAP is enabled. <strong>Note:</strong> Before using LDAP, set LDAP properties on the External User Management page (see page 107).</td>
</tr>
<tr>
<td>Port Number</td>
<td>The LDAP server port.</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>Configure</strong> to provide the server information.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Test</strong> to test connection to the server.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>The name or IP address of the secondary LDAP 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 Windows 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>LDAP root DN</td>
<td>The DN (distinguished name) 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 type of connection to use when connecting to the LDAP server:</td>
</tr>
<tr>
<td></td>
<td>• Secure</td>
</tr>
<tr>
<td></td>
<td>• MD5 Encryption</td>
</tr>
<tr>
<td></td>
<td>• Clear</td>
</tr>
<tr>
<td></td>
<td>• GSS</td>
</tr>
<tr>
<td></td>
<td>• LDAPS</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Specifies whether authentication using RADIUS is enabled.</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></td>
<td><strong>Note:</strong> Before using SiteMinder, set up integration with SiteMinder (see page 104).</td>
</tr>
</tbody>
</table>

Before using LDAP or RADIUS authentication, configure the primary and secondary servers.

To configure the primary and secondary servers for LDAP or RADIUS

1. Click **Configure**.
2. In the Configure Server dialog box, type the name or IP address of the server. For RADIUS, you must also 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.

Skybox version 9.0.100 103
4 If you trust the certificate, it is added to the Skybox client keystore.
5 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 the `LDAP_connection_timeout` property in `<Skybox_Home>/server/conf/sb_server.properties`

**Setting up integration with SiteMinder**

Note: Integration with SiteMinder is currently supported only when the Skybox Server is installed on a Linux machine.

To set up integration with SiteMinder

1 Install the communication agent (see page 104) on the Server machine.
2 Configure SiteMinder (see page 104) to permit communication with Skybox.
3 Create a SiteMinder properties file (see page 105). Copy the file to the `<Skybox_Home>/server/conf` directory.
4 Enable Skybox to work with SiteMinder:
   a. Select **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 following 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 user> -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 a file named sm_properties.txt, located in the <Skybox_Home>/server/conf directory. This file must have the following 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>
</tbody>
</table>
### Skybox Installation and Administration Guide

#### Key Description Mandatory

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>resource</td>
<td>The resource protected by the agent.</td>
<td>Yes</td>
</tr>
<tr>
<td>max_cookie_size</td>
<td><strong>Advanced:</strong> The memory allocated for updated cookies. The default value is 4096.</td>
<td>No</td>
</tr>
<tr>
<td>user_attrib</td>
<td><strong>Advanced:</strong> The attribute number in which to look for the user name. You might have multiple entries of <code>user_attrib</code>.</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 <code>WebAgent.conf</code> 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>
<tr>
<td>shared_secret</td>
<td>The shared secret defined on the SiteMinder Server side.</td>
<td>Yes</td>
</tr>
<tr>
<td>agent_ip</td>
<td>The IP address of the host that runs the agent.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Additional configuration properties for SiteMinder

The SiteMinder properties in `<Skybox_Home>/server/conf/sb_server.properties` are listed 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 server/conf</td>
<td><code>sm_properties.txt</code></td>
</tr>
<tr>
<td>SM_agent_name</td>
<td>The name of the SiteMinder agent utility under server/bin</td>
<td><code>smagent</code></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><code>SMSESSION</code></td>
</tr>
</tbody>
</table>
Chapter 15  Server options

Skybox version 9.0.100

| SM_cookie_max_age | The maximum age of the session cookie in seconds | 3600 |

**Testing communication**

You can test communication between SiteMinder and Skybox after you finish the setup.

**To test communication**

› On the Server machine, run SMAgent using the following command:

```
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 Disabling Inactive Users page specify how Skybox handles inactive users.

These properties are described in the following table.

<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, you must delete and disable inactive users manually (for more information, see Users (on page 55)).</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 still 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 102).

› Create a Skybox user group to correspond to the LDAP users (see page 61).

› Define the properties explained here.

The properties that you can set in the 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>
</tbody>
</table>
Property Description

Global User  
Click **Configure** to specify the global user name and password.

Default Authentication Method  
The default method to use for authenticating LDAP users who are managed externally.

**Advanced**  
The names of attributes used in user records in LDAP, used for pulling user information from the LDAP server.

*Note:* The attribute names provided are standard in LDAP and should only be changed if your organization uses other or customized attribute names.

### User Permissions

The properties in the 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><strong>Firewall Assurance, Network Assurance (Access Analyzer) &amp; Vulnerability Control Permissions</strong></td>
<td>Specifies whether Skybox limits the parts of the model that each user can view.</td>
</tr>
<tr>
<td>Permissions for Firewall Assurance, Network Assurance (Access Analyzer) &amp; Vulnerability Control</td>
<td>Specifies whether Skybox limits the phases of Access Change tickets that each user can change.</td>
</tr>
<tr>
<td>Tickets can only be edited by their owner</td>
<td>Specifies that users, even with Change Manager permissions, can only edit their own tickets.</td>
</tr>
<tr>
<td>Permissions are available for:</td>
<td></td>
</tr>
<tr>
<td>&gt; Skybox Firewall Assurance: Firewall folders</td>
<td></td>
</tr>
<tr>
<td>&gt; Skybox Network Assurance: Devices shown in the Access Analyzer</td>
<td></td>
</tr>
<tr>
<td>&gt; Skybox Vulnerability Control: Business Units and locations</td>
<td></td>
</tr>
<tr>
<td>&gt; Skybox Change Manager: Phases of Access Change tickets</td>
<td></td>
</tr>
</tbody>
</table>

When permissions are enabled, **Admins** must set permissions for each type of user and 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 change any ticket phases 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.**
VULNERABILITY CONTROL

The properties that you can set 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><strong>Unassigned Assets</strong></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 which assets are not part of any site 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>Maintain 'Unassigned Assets' Site Asset Group</td>
<td>Skybox can include a group for all assets that are not part of any other site asset group. This helps you to see which assets are not part of any site 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><strong>Standards Definition</strong></td>
<td>How data is presented in the Vulnerability Control centers.</td>
</tr>
<tr>
<td><strong>Default SLA Values for New Security Metrics</strong></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><strong>Business Asset Groups Update Warning</strong></td>
<td>Specifies how many days after the Business Asset Groups were last updated until a warning is shown in the GUI. The warning is shown on the Summary page, as well as in the Discovery Center, Analytics Center, and Remediation Center.</td>
</tr>
<tr>
<td>Warn users when Business Asset Groups have not been updated in &lt;n&gt; days</td>
<td>Display the Analytics Center pages (for backward compatibility)</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 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>Worm selection preferences</td>
<td></td>
</tr>
<tr>
<td>Maximum Worm Age</td>
<td>The maximum age of worms to be used.</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>
Chapter 16

Configuring Skybox using the properties files

This chapter describes the main Skybox properties files, which configure and fine-tune the behavior of Skybox components.

You can 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 .......................................................... 111
Collector properties file ....................................................... 111
Manager properties file ....................................................... 111
Common properties file ...................................................... 111
Port properties file ............................................................. 112

SERVER PROPERTIES FILE

The file <Skybox_Home>\server\conf\sb_server.properties contains options that control the Server’s activity.

You can modify most of the commonly used properties in this file in the GUI (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 the Manager’s activity and change the display in the Manager window.

You can modify most of the properties in this file in the GUI (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 Skybox component for which they are changed.

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: You must restart the relevant Skybox component to apply port changes.

You must 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.
Chapter 17

Managing multiple Appliances

This chapter explains how to manage multiple Skybox Appliances.

In this chapter

Viewing Appliance information ............................................. 113
Disabling tasks on the secondary Appliance Server ............... 113

VIEWING APPLIANCE INFORMATION

You can view information about the Skybox Appliances that your organization is using.

To view information about Skybox Appliances

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

When you select an Appliance in the list, the following additional information is displayed:
• Name of the model file that was loaded and the date it was loaded
• Whether tasks are enabled or disabled
• Model number of the Appliance
• Serial number of the Appliance

DISABLING TASKS ON THE SECONDARY APPLIANCE SERVER

When working 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.
When the flag is set to **false**, all invocation of task and task sequence scheduling is disabled. The scheduler is still 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 server/bin directory, run the following utility:
  - In Windows: `settaskschedulingactivation.bat`
  - In Linux: `settaskschedulingactivation.sh`

The utility takes a single argument:
- `enable`: Set the property to true
- `disable`: Set the property to false
Chapter 18

Dictionary updates

The Skybox Vulnerability Dictionary contains information about Vulnerability Definitions, worms, and IPS signatures. It is used in Skybox for Security Risk Management.

Skybox includes the most up-to-date Vulnerability Dictionary at the time of release, but new updates are issued periodically. You must 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 ........................................115
Updating the Skybox Vulnerability Dictionary ............................116

ABOUT VULNERABILITY DICTIONARY UPDATES

You obtain 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 current 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 (for example, proxy definition and local IP address) in the dictionary auto update section of <Skybox_Home>\server\conf\sb_server.properties
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’s schedule as described in the Task schedule properties topic in the Skybox Reference Guide.

Note: The task does not run on the predefined schedule until you 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 in cases where 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 Task 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

In cases where neither the Skybox Server nor the Skybox Collector can access the update server (for example, when they are protected behind a firewall and cannot access the internet), you can use the Manager or another computer to download the latest Vulnerability Dictionary and then update the Dictionary manually.

You can download the Vulnerability Dictionary from http://dictionary.skyboxsecurity.com/dictionary/9.0.0/LatestDictionary.sbd

Note: Some web browsers download the Dictionary file with the extension zip; rename 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 and select the file.
   c. Click Update Dictionary.

For additional help with manual updates, contact Skybox Support.
Chapter 19

Skybox logs

The **System** folder in the Admin tree provides the following information:

- **Activity log** (see page 117): Displays application and user events
- **Audit log** (see page 121): Displays user management and login/logout events

Other log information is available via **event logging** (see page 123) and various Skybox log files (see page 123).

**In this chapter**

- Activity log ........................................................................ 117
- Audit log ........................................................................... 121
- Event logging ..................................................................... 123
- Log files ........................................................................... 123

**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** > **Policies** > **System**.
2. Click **Activity Log**.

**Activity log messages**

The following event types can be included in the activity log:

- **Configuration Item** event types indicate 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

The following is an example of a configuration item message:

```
2015-03-18 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 indicate 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

The following is an example of a host message:

```
2015-03-16 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 indicate 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

The following is an example of a network interface message:

```
2015-03-16 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 indicate changes to networks.

• Network Zone Mapping
• Network IP Address Modification

The following is an example of a network message:

```
2015-03-16 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 indicate software update changes:

• Online-updates Check for Updates
• Online-updates Blocked
Skybox logs

- 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 indicate 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

The following is an example of a SPA message:

```
2015-03-17 11:34:46,676 INFO  SPA Analysis_Security Metric_Calculation_Started - <> Analysis - Security Metrics task started running on the Live model
```

**TAM** events indicate changes to many types of entities in the model that are not covered by the other types of events.

- 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 System Updated
- Vulnerability Definition Details User Updated
- Unhandled Vulnerability Definition More
- New Ticket
- Ticket Closed
- Ticket Reopened
- Product Details Updated
- Product Deleted
- Product Request Deleted
- New Vulnerability Notification
- Unhandled Vulnerability Notification
- New Ticket Phase
- 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
- Access Policy Section Deleted
- Access Policy Section Enabled
- Access Check Changed
- Access Check Deleted
- Access Check Enabled
- Rule Policy Changed
- Rule Policy Disabled
- Rule Check Added
- Rule Check Renamed
- Rule Check Disabled
- Configuration Policy Added
- Configuration Policy Renamed
- Configuration Policy Disabled
- 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 Disabled
- Access Check Added
- Access Check Renamed
- Access Check Disabled
- Rule Policy Deleted
- Rule Policy Renamed
- Rule Policy Enabled
- Rule Check Changed
- Rule Check Deleted
- Rule Check Enabled
- Configuration Policy Changed
- Configuration Policy Deleted
- Configuration Policy Enabled
• Configuration Check Added
• Configuration Check Renamed
• Configuration Check Disabled
• Vulnerability Occurrence Manually Added
• Vulnerability Occurrence status changed
• Exception Modified

The following is an example of a TAM message:

```
2015-03-17 11:06:22,512 INFO  TAM New_Dictionary - <> New dictionary version 75.893 , date: 3/16/15 12:00 AM loaded successfully
```

AUDIT LOG

The Audit log includes all important user management and login actions for all users, as well as messages about the creation of new tasks, and the modification or deletion of existing tasks.

To view the Audit log

1. Select **Tools > Administrative Tools > Policies > System.**
2. Click **Audit Log.**

Audit log messages

The audit log includes messages about task creation, deletion, and modification, and various system messages (for example, model loaded). Other event types that can be included in the audit log are:

- User_Management Login
- User_Management Logout
- User_Management Password_Changed
- User_Management Password_Expired
- User_Management Password_Never_Expires
- User_Management Password_Expiration_Set
- User_Management User_Renamed
- User_Management New_User
- User_Management Login_Failed
- User_Management Login_Failed_User_Doesnt_Exist
- User_Management Login_Failed_User_Is_Disabled
- User_Management User_Role_Modified
- User_Management User_Disabled
› User_Management User_Enabled
› User_Management User_Deleted
› User_Management New_User_Group
› User_Management User_Group_Deleted
› User_Management User_Group_Renamed
› User_Management User_Group_New_Member
› User_Management User_Group_Member_Removed
› User_Management User_Group_Member_Moved
› User_Management SiteMinder_Exception
› User_Management New_TMS_Permission
› User_Management New_TMS_Group_Permission
› User_Management TMS_Permission_Deleted
› User_Management TMS_Group_Permission_Deleted
› User_Management TMS_Permission_Updated
› User_Management TMS_Group_Permission_Updated
› User_Management New_VTMAS_Permission
› User_Management New_VTMAS_Group_Permission
› User_Management VTMAS_Permission_Deleted
› User_Management VTMAS_Group_Permission_Deleted
› User_Management VTMAS_Permission_Updated
› User_Management VTMAS_Group_Permission_Updated
› User_Management LDAP_Exception
› User_Management RADIUS_Exception
› User_Management SUCCESSFUL_EXTERNAL_USER_MANAGEMENT
› User_Management PROBLEMS_DURING_EXTERNAL_USER_MANAGEMENT
› User_Management EXCEPTION_OCCURRED_WHILE_FETCHING_EXTERNAL_USER_RECORD
› User_Management FAILED_TO_RESOLVE_A_ROLE_FOR_EXTERNAL_USER
› User_Management DISABLING_EXTERNAL_USER
› User_Management EXTERNAL_USER_MANAGEMENT_EXCEPTION
› User_Management User_First_Name_Modified
› User_Management User_Last_Name_Modified
› User_Management User_Email_Modified
› User_Management User_Authentication_Modified

A complete message has additional information, including a date-time stamp. The following is a sample message for user login:

```
2015-03-16 11:18:01,768 INFO  User_Management Login - 
<skyboxview@127.0.0.1:TRAY:1> User skyboxview logged in
```
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 121) for a list of these actions)
- Various actions performed by Skybox (see Activity log messages (on page 117) 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 hostname or address of the remote logging server.
   - If the logs should go to a port other than the default system UDP port (514), add a colon and the port number after the host name. For example, 192.0.2.0:8514
   - To send events to multiple remote servers, use a comma separated list.
4. Specify which events are logged to syslog or Event Viewer.

For additional information about enabling event logging, see System Events (on page 98).

LOG FILES

Skybox creates many different log files. These include:

- Startup log files (see page 123): These files can help you if you have trouble running Skybox.
- Skybox task output log files (see page 124): These files contain the output of tasks. They contain information about your organization’s network.
- Troubleshooting log files: Skybox produces various log files that Skybox’s technical support team use for troubleshooting, see Packing log files for technical support (on page 125).

Startup log files

Skybox creates log files at startup. These files contain information that can help you to troubleshoot problems running Skybox.

Server startup

When 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, which 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**

When 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`, which contains the output (for example, warning and error messages) that normally would be 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 which memory consumption statistics 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**

- **aging.log**: Includes output of Delete outdated entities tasks, which are described in the Skybox Reference Guide

  All task messages are written to the log file located 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.

- **validation.log**: Includes output of Model completion and validation tasks, which are described in the Skybox Reference Guide

  All task messages are written to the log file located 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.

- **server.log**: Includes output from all other tasks
Skybox messages

The following files are located at <Skybox_Home>\server\log unless otherwise specified.

- **activity.log**: Includes application events from Skybox Threat Manager and from the Security Metrics feature of Skybox Vulnerability Control.
- **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
- <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 the `com.skybox.view.logic.discovery.ModelsMerger.verbose_log` property in <Skybox_Home>\server\conf\sb_common.properties to `true`.

### Packing log files for technical support

Skybox produces various log files that Skybox’s 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 one copy of the ZIP file on the Server’s file system and another in a specified directory.

Pack Logs properties are described in the following table.
**Property** | **Description**
---|---
Logs from | The Skybox component for which to collect logs. **Note**: 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.

Split output into files of 5MB or less | Specifies whether to split the packed logs into separate ZIP files of 5 MB.

Add Case Number | If selected, you can add a case ID of up to 8 characters to the name of the ZIP file.

Include Latest Saved Model | 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.

Include Latest SQLX model | 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 SQLX model in the ZIP file.

Number of Days Back | This field is not displayed if **Logs from** = **Firewall Configurations**. 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.

Firewall Scope | This field is displayed only if **Logs from** = **Firewall Configurations**. The firewalls and firewall folders to include in the ZIP file.

Generations | This field is displayed only if **Logs from** = **Firewall Configurations**. The number of generations of firewall configuration files to include in the ZIP file.

Save copy to a local directory | The directory on the local machine where a copy of the packed logs is saved.

**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 71).