Skybox

Change Manager Help

9.0.800
Proprietary and Confidential to Skybox Security. © 2019 Skybox Security, Inc. All rights reserved.

Due to continued product development, the information contained in this document may change without notice. The information and intellectual property contained herein are confidential and remain the exclusive intellectual property of Skybox Security. If you find any problems in the documentation, please report them to us in writing. Skybox Security does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the prior written permission of Skybox Security.

Skybox®, Skybox® Security, Skybox Firewall Assurance, Skybox Network Assurance, Skybox Vulnerability Control, Skybox Threat Manager, Skybox Change Manager, Skybox Appliance 5500/6000/7000/8000/8050, and the Skybox Security logo are either registered trademarks or trademarks of Skybox Security, Inc., in the United States and/or other countries. All other trademarks are the property of their respective owners.

Contact information

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

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

Skybox Change Manager 9.0 Help ................................................................. 4
Technical support ..................................................................................... 6
Overview of Skybox Change Manager ...................................................... 7
How Change Manager works ................................................................. 7

Getting started with Skybox Change Manager ......................................... 8
Before you begin .................................................................................. 9
Prerequisites ...................................................................................... 9
Logging in to Skybox Change Manager .................................................. 9
Changing the regional settings ............................................................ 10
Navigating Skybox Change Manager .................................................... 11
What kind of requests can you make via Change Manager? ................... 12
Viewing tickets .................................................................................. 13
Working with tickets ......................................................................... 14
Default workflow ............................................................................. 14
Creating a ticket ............................................................................... 14
Technical Details phase ................................................................... 17
Risk Assessment phase ................................................................... 19
Implementation Details phase ............................................................ 21
Verification ....................................................................................... 24
Recertification tickets ....................................................................... 25
Cloning a ticket ................................................................................. 26

Using Skybox Change Manager ................................................................. 27
Change management ........................................................................ 28
Users and their responsibilities .......................................................... 28
Typical flow of a change request ........................................................ 29
Submitting change requests ............................................................... 30
Processing technical details .............................................................. 42
Assessing risk ............................................................................... 44
Implementation phase ....................................................................... 46
Verifying a request ........................................................................ 47
Additional workflow actions ............................................................... 48
Rule recertification .......................................................................... 49
Change implementation ....................................................................... 50
Viewing a specific set of change requests ............................................. 50
Assigning change requests ............................................................... 50
Implementing change requests .......................................................... 51
Exporting information from Change Manager ................................... 56
Skybox Change Manager 9.0
Help

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

This help is specifically for Skybox Change Manager users. Additional help for Change Manager, including how to set up Change Manager, is in the general Skybox documentation.

**Technical support**

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

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

When you open a case, you need:

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

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

Change Manager ends risky changes with network-aware planning and risk assessment that keep your network secure and in continuous compliance with policies. Change Manager incorporates customizable workflows and provides comprehensive management of rule lifecycles to automate change processes.

- Fully automates firewall change management workflows, improving communication and efficiency across security teams
- Validates proposed firewall changes by checking for policy violations, security gaps and vulnerabilities that could be exposed by the change
- Ensures that changes are made as intended and do not introduce new risk
- Customizes and simplifies workflows to reduce change management time by 80 percent
- Establishes end-to-end rule life cycle management for secure infrastructure and optimized firewalls

HOW CHANGE MANAGER WORKS

The following figure is an overview of how the Change Manager process works.
Getting started with Skybox Change Manager

This part provides background information about what Skybox Change Manager does and how it works, and explains how to get started using it. It is intended for use with the demo model only.
Chapter 1

Before you begin

This chapter contains introductory information about working with Skybox.

In this chapter

Prerequisites ........................................................................ 9
Logging in to Skybox Change Manager ............................... 9
Changing the regional settings ........................................... 10

PREREQUISITES

To work with Skybox Change Manager, you need:

- A valid Skybox account
  - For information about registration as a Skybox user, see the User management section in the Skybox Change Manager User Guide
- A browser:
  - Microsoft Internet Explorer 9 or higher
    - Note: Microsoft Edge is not supported.
  - Google Chrome
  - Mozilla Firefox

LOGGING IN TO SKYBOX CHANGE MANAGER

Note: Skybox Change Manager sessions have an automatic expiration. If your session is idle for 30 minutes, you must log in again.

To log in to Skybox Change Manager

1  Verify that the Skybox Server is running.
2  Open the login page of the web interface using the following URL, where <server> is the full path name or IP address of the Skybox Server machine:
   - https://<server>:8443/skybox/
3 Type your Skybox user name and password.

If you were not assigned a user name and password by a Skybox administrator, use the user name `skyboxview` with the password `skyboxview`.

CHANGING THE REGIONAL SETTINGS

The region sets the date and time formats, currency, and other settings that vary between countries.

To change the regional settings

1 Click your user name at the top of the screen, and select **Regional Settings**.
2 Select the desired setting from the list. The region sets the date and time formats, currency, and other settings that vary between countries.
Chapter 2

Navigating Skybox Change Manager

Navigate in Skybox Change Manager using the menu and the history in the control panel.

**Menu**

- **Search**: Enables you to search for a text string in all fields of all tickets
- **Home**: The main page of Change Planning
- **Create New Ticket**: Enables you to create a new ticket
- **My Assigned Tickets**: Displays all the tickets that are assigned to you (the logged-in user)
- **My Requested Tickets**: Displays all the open tickets that you (the logged-in user) created
- **Pending Implementation**: Displays ready-for-implementation change requests grouped by firewall rather than by ticket
- **Closed Tickets**: Displays all the closed tickets
- **Choose Analysis**: Enables you to select a ticket analysis (that is, a set of tickets to view) from Skybox

**History**

The History pane lists the pages that were most recently visited in Change Manager. Mouse over an entry to see additional information about that entry in a tooltip.
Chapter 3

What kind of requests can you make via Change Manager?

You can use Skybox Change Manager to create tickets requesting firewall changes. After a user creates a ticket with a requested change, Skybox analyzes the original (user-created) change request and might split it into several action items (named derived change requests). For example, a request to open access in the network from point A to point B might involve adding or changing access rules in all the firewalls on the way from point A to point B. Each change is listed as a separate change request.

Change Manager supports the following change requests:

- **Access Update**: Access is required between 2 points. You do not need to know the firewalls that are involved or what the rules say.
- **Add Rule**: A specific rule is missing from a firewall
- **Modify Rules**: Access rules must be changed (for example, a new destination or service must be added to the access rules)
- **Deactivate Rules**: Access rules must be disabled or deleted
- **Modify Object**: A firewall object must be changed
- **Recertify Rule**: Enables recertifying (authorizing) that access rules in your organization continue to be required

Note: **Web Ticket Requestors**, whose primary task in Change Manager is to create tickets for specific requests, might be limited in the change requests that they can create.
Chapter 4

Viewing tickets

You can view tickets from locations in Change Manager that include:

- **My Requested Tickets**: Lists all the tickets that 'I' created
- **My Assigned Tickets**: Lists all open tickets that are assigned to 'me'
- **Closed Tickets**
- **Search**: Lists tickets that match the search string
- **History pane**

**Web Ticket Requestors**

**Web Ticket Requestors** can always see the general information about tickets that they created, but they can only see the phase information of their tickets when those tickets are in the 1st or last phase.

*To view a ticket that you requested*

1. Click **My Requested Tickets**.
2. Click the link in the ticket named **Remove access from partner to web servers**.
3. The top pane of the ticket shows the ticket general information. It also contains the toolbar for general changes to the ticket.

Below the metadata there is a tab for each phase of the ticket. The tab for the current phase is bolded; this tab is open by default.

This ticket is in the **Request** phase. In the Change Requests pane, you can see the requested change for this ticket.

**Request** is the 1st phase. After a ticket is promoted, the information about the previous phases is visible in their tabs.
Chapter 5

Working with tickets

Tickets go through various phases, which are often managed by different users. Also, many organizations have different workflows for different ticket types. Each workflow has different phases, different due dates, and usually applies to different firewalls. Each workflow can be assigned to a different set of users.

This chapter walks you through the phases of a typical ticket for a typical organization, using the workflow in the Skybox demo model.

In this chapter

- Default workflow ................................................................. 14
- Creating a ticket ................................................................. 14
- Technical Details phase ....................................................... 17
- Risk Assessment phase ........................................................ 19
- Implementation Details phase .............................................. 21
- Verification ........................................................................ 24
- Recertification tickets .......................................................... 25
- Cloning a ticket .................................................................. 26

DEFAULT WORKFLOW

1  **Request**: A user opens a ticket to request access.

2  **Technical Details**: A technical reviewer looks at the original change request and makes sure that it is complete and valid. If the requested access is permitted, the request is marked as unnecessary and the ticket can be closed.

3  **Risk Assessment**: For each request, security analysts can see all the exposed vulnerability occurrences and policy violations that would be caused by implementing the request. They then assign a risk level to the ticket, approve the risk, and add any other necessary information.

4  **Implementation Details**: Firewall administrators implement the requested changes on the firewalls and mark the requests as implemented. After all the requests are implemented, an administrator promotes the ticket.

5  **Verification**: Tickets in this phase wait for Skybox to verify that they are implemented correctly. After that, their **Requestors** review and usually close them.

CREATING A TICKET

**Request** is the 1st phase of a ticket when using the default workflow.
To create a ticket

1. Click **Create New Ticket**.

   Note: Clicking the arrow in the **Create New Ticket** icon enables you to select a different workflow for your ticket. However, this is not necessary for the tutorial.

2. Some fields are displayed twice (for example, **Title** and **Description**) and are always available in the top pane. These fields can be modified.

3. In the **Title** field, type *Open access from partner to FTP server.* This ticket is a request for access between 2 points.

4. In the **Description** field, type *Partner2 access to the FTP server.*

5. Click **Save**.

   The ticket is saved; it now has a ticket ID and fields in the top pane are filled. If you navigate from the ticket, you can find it in the History pane or from **My Requested Tickets**.

6. In the Change Requests panel, click **Access Update**.
In this dialog box, you specify the source, destination, and services for the request either by typing specific IP addresses and ports or by selecting objects.

7 Define the source:

Note: You can select the source, destination, and services from the list of objects that belong to a firewall or from a repository of objects that is managed by the organization. Requestors are usually guided to work with the repository; technical users might want to see the firewall objects or enter IP addresses. This tutorial uses the repository.

a. In the **Source** area, next to **Addresses**, click [ ].

![Object Finder](image)

b. In the **Search** field, type **Partner** and then click **Find**.

Partner objects are listed in the **Matching Objects** table.

c. Make sure that **Repository Objects** is selected above this table.

d. Double-click **Partner2** to move it to the **Selected Objects** table.

e. Click **OK**.

8 Define the destination:

a. In the **Destination** field, click [ ].

b. In the **Search** field, type **ftp** and then click **Find**.

c. Double-click **FTP Servers** to move it to the **Selected Objects** table.

d. Click **OK**.

9 Define the service:

a. In the **Services & Applications** field, click [ ].

b. In the **Search** field, type **ftp*** and then click **Find**.

c. Select **ftp** to move it to the **Selected Objects** table.
d. Click **OK**.

10 Click **OK**.

11 Click **Save**.

12 Look in the Change Requests pane to see how the finished request looks.

13 Look at the **Change Required** column. This column tells you whether the changes that you are requesting are required. If all the changes are labeled as unnecessary, you can reject the ticket.

14 Click **Promote**.

15 In the pop-up asking whether to approve the risk of all policy violations, click **No**.

   **Note:** This pop-up is displayed only because you are running the tutorial as an administrator (skyboxview).

16 In the **Promote** dialog box you are asked to select the owner for the next phase, even though there is a default owner for each phase. This is useful if, for example, you know that the ticket belongs to a specific user. For the tutorial, this is not necessary; use the default owner.

17 Click **OK**.

The ticket moves to the **Technical Details** phase.

**TECHNICAL DETAILS PHASE**

**Technical Details** is the 2nd phase of a ticket when using the default workflow. In this phase, technical users review the request and verify that all details are defined correctly and that the firewalls are correctly identified.

Users can create tickets without creating formal change requests; they type a description of what they want and promote the ticket to the **Technical Details** phase. When this happens, the person handling the tickets in this phase must formalize the change requests (by adding the necessary source-destination-service combinations) before continuing with the review.

**To review the technical details of a ticket**

1. In a regular workflow (that is, not a tutorial), the users working on the ticket in each phase are different. After a ticket that you created is promoted, you cannot see the ticket. In this tutorial, use the History pane to select and open the ticket; it is the most recent item.

   The Original Change Requests area shows the change request as it appeared in the **Request** tab.

2. Look in the **Change Required** column. If the value in this column is **No**, all the requested access exists; you can reject the ticket.

   Rejected tickets are assigned a closure reason and an optional comment, and then sent back to their **Requestors** to be closed.
3 Look at the Derived Change Request area.

The original request was divided into several requests, each request on a different firewall. Because Access Update change requests are not firewall specific, Change Manager identifies the relevant firewalls for the request. Relevant firewalls are those that reside between the source and destination. The change details are translated from repository objects to IP address ranges and ports. Information is also added about where in the ACL the new rules are to be added. This makes it easier for the firewall administrators to update the firewalls.

4 Check the **Change Required** column of the derived change requests; you can see that all 3 changes are required.

5 At this point, review the derived change requests to see if they make sense based on the original change request. For example, by checking that the firewalls listed in the derived change requests are those that you expect for this request. You can edit the original change request or any of the derived change requests.

6 Click **Promote**.

7 Click **OK** to move the ticket to the default owner of the **Risk Assessment** phase.

**Viewing the routes that a change request might take**

By default, the identification of the relevant firewalls in the route for Access Update change requests is based on checking the source and destination in the firewall interfaces and routing rules, and examining if the firewall could filter such traffic between 2 different interfaces.

However, if your organization works in network mode, Skybox access analysis identifies the path between source and destination. The firewalls on this path are the relevant firewalls. This methodology is more accurate and can consider Network Address Translation along the path.
If you work in network mode, while reviewing the change requests you can view a graphical representation of the identified routes (by clicking Routes in the Technical Details phase). The display includes the routers and other gateways, showing both the traffic details (including any NAT translation) and the change request details. For the request in this tutorial, you see the following.

![Image of graphical representation of routes]

**RISK ASSESSMENT PHASE**

*Risk Assessment* is the 3rd phase of a ticket when using the default workflow. Use this phase to review the risks of the change requests.

*To assess the risk of a ticket*

1. Use the History pane to select and open the ticket.
2. In the Risks pane, make sure that the View is Original Change Requests.

The *Original Change Requests* view shows whether the original request is:

- Compliant with the organization’s Access Policies
- Secure (there are no vulnerability occurrences that would be exposed by granting this access)

This request is neither compliant nor secure.

3. Switch to the *Derived Change Requests* view.

This view displays the compliance and security of each derived change request.
4 Select the 1st request and look at the 2 tables below it.

The **Compliance: Policy Violations** table shows all the violations that this change will cause—they all have medium severity.

The **Security: Vulnerability Definitions with Exposed Assets** table shows Vulnerability Definitions that will be exposed by this change.

5 For the 1st Vulnerability Definition in the list, click the link in the **Solutions** column.

The dialog box that opens shows the list of solutions that are available for this Vulnerability Definition; several possibilities are available.

Close the dialog box when you finish looking at the possible solutions.

6 For this tutorial, although the request is not fully compliant with the organization’s Access Policy, it has been decided that it is necessary and must be approved. For each derived change request, click **Approve** to approve the risk.

Use temporary approval if the request itself is temporary or to grant temporary approval and then review the request. For this tutorial, you do not need to change anything.
7 Add a comment (perhaps the reason why the approval is only temporary) and click **OK**.

Note that the time frame for temporary approval of a request depends on the severity of its violations. High severity violations are approved for less time than medium severity violations.

8 Look at the Risk Assessment pane. The overall risk of the ticket is defined in this pane. You can add additional details of risk assessment if they will be helpful to users in the next phases or to the **Requestor** in their final review of the change.

9 **Promote** the ticket to the Implementation Details phase.

**IMPLEMENTATION DETAILS PHASE**

**Implementation Details** is the 4th phase of a ticket when using the default workflow. This phase manages the implementation of the requested changes. The following users work in this phase:

- Firewall administrators, who are responsible for implementing the changes on the firewalls

  There is a separate view, **Pending Implementation**, where firewall administrators can see the change requests on a per-firewall basis rather than per ticket, because it is easier for them to work that way.

- Users who are monitoring the ticket

**To implement the changes via Pending Implementation**

1 In the control panel, click **Pending Implementation**.

Make sure that you are looking at the **Not Implemented** tab, and that the view is **All**. This view shows all change requests in the Implementation Details phase that were not yet implemented. The changes are sorted by date and then by management server (or firewall if there is no management server), so that the first changes are those that are most urgent, but all the changes for each management server or firewall are together so that the administrator can apply them all together.
2. Click in the row of the change request of your ticket that is for **dev FW** and select **Assign > Assign to Me** above the table.

   ![Change Request Table]

   - You can see the changes that need to be made.

3. Add a comment.

4. View additional information about the change request by clicking the link in the **ID** column.

   ![Detail View]

   - View the background of the change request by clicking the link in the **Ticket ID** column. This opens the ticket in a separate window.

   ![Ticket Background]

   - Close the dialog box.
7 View a change request in command format by putting your cursor in the row of the request and clicking **Implement** (on the toolbar).

For this and other firewalls for which automatic implementation is supported, a list of all the changes that can be implemented on the relevant management server is displayed.

Clicking **Implement Changes** in this dialog box sends these changes to the firewall to be implemented.

For firewalls where automatic implementation is not yet supported, you see the change in a command format to help you to implement the changes on the firewall. For most firewalls, a generic representation of the firewall command is displayed; for Cisco firewalls, a Cisco-format command is displayed.

8 Click **Implement Changes** and add a comment for the implementer.

9 Click **OK**.

You get a message that the implementation will be done in the background. When implementation is complete, the status of the change request is updated.

**Note:** Implementation for this request fails because there is no actual connection to the firewall in the demo model.

10 Look at the pending implementation list again and find the change request from this ticket for **prod FW**.
With your cursor in the row of this change request, click **Mark as Implemented**.

Add a comment and click **OK**.

This change request is now implemented and deleted from the pending implementation list.

**To monitor the change request implementation**

1. Use the History pane to select and open the ticket.
2. In the Implementation List pane, there is a single change request that is marked as implemented (checkmark in the **Status** field).

3. In the Implementation Details pane, there is room to add a target date (for implementation) and additional implementation details for the users who implement the changes.

4. In a real scenario, you wait until all the change requests are marked as implemented before promoting the ticket, but for this tutorial, promote the ticket to the **Verification** phase. Note that the status of the ticket changes to **Resolved**.

**VERIFICATION**

**Verification** is the 5th and final phase of a ticket when using the default workflow.

Tickets can be promoted to the **Verification** phase manually (as was done in the previous step of the tutorial) or automatically. If all the change requests of a ticket are implemented, the status of the ticket is changed to **Verified**, and the ticket is sent back to its original **Requestor**, who receives a notification about the change.

The **Requestor**’s job in this phase is to review the ticket, make sure that the requests are implemented as expected, and close the ticket. If the **Requestor** sees a problem (for example, if not all the derived requests are implemented), they can demote it and explain the problem.

**Note**: In this tutorial, you close the ticket that you created as if the access that you requested was granted.
**To close a ticket**

1. Use the History pane to select and open the ticket.

   The original change request was not verified by Skybox—when Skybox checked for the requested access, it was not found. In an actual scenario, after all the changes are implemented on the firewalls, the change request is automatically marked as **Verified**.

2. On the toolbar at the top of the ticket, click **Close**.

3. In the **Select the Closure Reason** field, select **Fixed** and click **OK**.

   Note: If tickets are closed in earlier phases, additional closure reasons are available.

**To view closed tickets**

- In the control panel, select **Closed Tickets**. You can see the ticket that you just closed.

If you closed a ticket by accident, you can reopen it from here.

**RECERTIFICATION TICKETS**

A recertification ticket contains requests that access rules be recertified. You can open these tickets both from Firewall Assurance and from within Change Manager, but they are managed in Change Manager. Recertification tickets have a different workflow than other tickets, usually with fewer phases.
**To view a recertification ticket**

1. In the control panel, click **My Requested Tickets**.
2. Click the link to the 1st ticket that has **Recertification** in the **Workflow** column.

The ticket has only 3 phases. The **Recertification Request** phase enables you to view all the violations and vulnerability occurrences for the access rule, to help you to decide the risk of recertifying the rule.

Note that each rule is marked as either certified or rejected, except the last rule.

3. Select the last rule and click **Certify**.
   In the Certify Rules dialog box you can change the business attributes for the rule.

4. Click **OK**.

5. **Promote** the ticket to the next phase: **Recertification Review**. This phase is usually used by technical reviewers.

6. Promote the ticket to the **Verification** phase.

When the ticket is verified, each rule recertification status is changed as specified. For certified rules, their most recent certification date is set to the current date. The administrator can decide whether to create tickets for modification or deactivation of the rejected rules.

**CLONING A TICKET**

If you need 2 very similar requests or there is a request that is similar to the request that you need, you can open the ticket and click **Clone**. This creates a copy of the ticket where you can make all the necessary changes, save the ticket, and promote it to the next phase.

Regardless of the phase of the original ticket, the cloned ticket is always opened in the **Request** phase.
Using Skybox Change Manager

This part explains how to work with Skybox Change Manager.
Chapter 6

Change management

Change Manager provides a complete and centralized change workflow so that you can:

› Identify the firewalls that need changing
› Plan and optimize the details of access rule changes
› Assess security risks
› Verify that appropriate access was granted

In this chapter

Users and their responsibilities ............................................. 28
Typical flow of a change request ........................................... 29
Submitting change requests ................................................. 30
Processing technical details .................................................. 42
Assessing risk..................................................................... 44
Implementation phase ......................................................... 46
Verifying a request.............................................................. 47
Additional workflow actions .................................................. 48

USERS AND THEIR RESPONSIBILITIES

This section explains the user roles in Skybox Change Manager and the most common actions for each user.

Requestors

Requestors are users who submit requests for granting connectivity. The following actions are available:

› Create tickets: Submit requests for connectivity
› Find a ticket by ID: View a specific ticket for follow up
› View my requests: View a list of the tickets that the Requestor created
› View my tickets: View a list of the tickets that the Requestor owns
› Verify the tickets that the Requestor created at the end of the cycle

Analysts

Analysts are users who process tickets. The following actions are available:

› View tickets by phase or by assignee/owner: This list represents the tickets owned or opened by the analyst (or their group)
› View change requests by firewall or firewall management system (in the implementation phase)
Process tickets and promote them to the next phase in the life cycle

Note: In some cases, analysts can view the change requests that relate to their own firewalls only; change requests for other firewalls are obfuscated. In this case, each analyst reviews their own change requests. After each change request is reviewed by its owner, the ticket is promoted automatically.

Find a ticket by ID: View a specific ticket for follow up

**Workflow supervisors**

The following actions are available to workflow supervisors:

- View tickets that have been in the system for some time and do not seem to be progressing (including overdue tickets)
- Update ticket due dates, change ticket priority
- View tickets by phase: For each phase, make sure that there are no bottlenecks, that content is coherent, and so on
- Find a ticket by ID: View a specific ticket to resolve a problem with requests

**TYPICAL FLOW OF A CHANGE REQUEST**

This is a typical workflow for change assurance management. Each step represents a phase in the life cycle of a Skybox Change Manager ticket. For a typical workflow of a recertification request, see Rule recertification (on page 49).

1. **Request**: A user in your organization submits a change request in the form of a ticket.
   
   The request can be a general request for access, a source-destination-port request, or a request to add or modify specific access rules or objects on a specific firewall or firewall cluster.

   Note: When firewalls are clustered, the cluster name is displayed instead of the names of the individual firewalls. The tooltip for the cluster provides the names of the individual members.

2. **Technical details:**
   
   - General requests are refined to include IP addresses and ports, and the relevant firewalls and clusters. They might be subdivided to several requests—usually one per firewall.
   
   - Specific requests are checked for validity and sometimes refined (if Skybox finds a more efficient way to grant access). For example, a request to add a new rule might be refined into a request to modify an existing (similar) rule.
   
   - Each request is checked to see whether the requested access is already permitted. If it is, the request is marked as **Unnecessary**.
   
   - For zone-based or interface-based firewalls, the zone or interface information is included when calculating Access Update and Add Rule change requests. This information is available in the Additional Details column.
The firewall administrator reviews the derived requests to make sure that they are complete and in line with your policy. The derived requests can be edited, or additional requests can be added to the ticket. If all the requests are marked as unnecessary, the ticket will be rejected.

3 Risk assessment: Skybox checks whether each derived request is compliant and secure.

- Compliant: The request does not cause any access policy violations.
- Secure: There are no vulnerability occurrences that would be exposed by granting this access.

For each request, security analysts can see all the policy violations and exposed vulnerability occurrences. They then assign a risk level to the ticket and add any other necessary information.

Skybox shows whether the firewall for each derived request already provides connectivity for the request.

If the request involves multiple firewalls and some show no connectivity, changes must be made to the access rules of the firewalls that show no connectivity. If all firewalls show connectivity, all the permissions necessary for the request (that is, the access rules) exist, and the ticket can be rejected.

4 Implementation details: Firewall administrators plan and implement the firewall changes. For some firewall types (for example, Check Point) implementation may be done automatically.

5 Verification: Skybox verifies that the change requests are fulfilled and marks the ticket as verified. If the requests are not fulfilled, Skybox reopens the ticket.

After the ticket is verified, its owner closes it (usually, this is the Requestor who created the ticket).

Note: The preceding explanation is for the standard workflow using the default phases. Admins can delete phases, edit their content, or add more phases. They can also create additional workflows with different sets of phases for different Business Units or distinctive processes. For information about customizing phases and creating workflows, see the Customizing Ticket phases and workflows section in the Skybox Change Manager User Guide.

SUBMITTING CHANGE REQUESTS

In Skybox Change Manager, you submit a change request by opening a ticket. The minimum required information is a title, priority, and free-form description of the request. You can make the request more specific by creating a formal request to:

- Add, modify, activate, or deactivate an access rule
- Add specific access (source, destination, and service)
- Modify a firewall object

In some workflows, you can add or change the business attributes of an access rule, including the rule owner and the owner email address.
To open a ticket

1 In the control panel, click **Create New Ticket**.

   If you have multiple workflows and no default workflow, you must select a default workflow or a workflow for this ticket. See **Selecting a workflow** (on page 32).

2 Provide the basic request information (title, priority, and free-form description).

   This information can be edited in later phases.

3 If you have no other information to add, skip to step **10**.

4 If **View Rules** is displayed, use it to view the rules in any firewall:
   a. Select the firewall.
   b. Provide a search string (use “*” as the search string to view all the rules).

5 Add requests to the ticket:

   Note: **Web Ticket Requestors** might be limited in the requests that they are permitted to add.

   - **Request specific access** (on page 32) between a source and a destination
   - **Add an access rule** (on page 35)
   - **Modify access rules** (on page 38)
   - **Deactivate or enable access rules** (on page 39)
   - **Modify firewall objects** (on page 40)
   - Add multiple requests for specific access by **uploading a file** (on page 34).

   Alternatively, you can add a **custom change request** (see page 41) of a type created specifically for your organization.

6 Click **Save**.

   Note: For non-recertification tickets, Skybox checks whether the changes are required—if the access already exists, you can **reject** the ticket at this point; there is no need for it.

7 Click **Attachments** to add an attachment (or view the existing attachments).
8 (Optional) Click Add Comment to add additional information to the ticket.

9 Click Promote.

10 To change the owner for the next phase, click (next to the suggested owner’s name) and select a different owner.

11 Click OK.

The ticket is promoted to the Technical Details phase.

Selecting a workflow

Skybox supports multiple workflows for tickets—different ticket types can have different sets of phases, different due date calculations, and different users. When you submit a change request for the 1st time, you might find that you have multiple workflows that you can use. You must select a workflow to continue submitting the change request. You can either select a workflow only for the current ticket or select a default workflow. Until you select a default workflow, you must select a workflow for each new change request. However, even if you select a default workflow, you can select a different workflow when necessary.

To select a workflow when there is no default

1 (If you have not already done so, click Create New Ticket in the control panel.)

2 Look at the list of available workflows.

3 Select the workflow to use for the current ticket.

4 To select a default workflow, select the workflow that is used most often and click Set Default.

5 Click OK.

To select a workflow when a default exists

1 In the control panel, click the arrow next to Create New Ticket.

2 Click Choose Workflow, select the workflow you want, and click OK.

Requesting specific access

If you know the source, destination, and desired ports, you can submit a change request for specific access. After you promote the ticket, Skybox:

› Checks the Skybox model
› Identifies the firewalls and access rules that must be changed to permit access
› Derives specific change requests from the original request for the identified firewalls and access rules
To request specific access between a source and a destination

1. Click **Access Update**.
2. Fill in the fields. The fields are described in the following table.
3. Click **OK**.

**Access update properties**

The access update properties available for Skybox Change Manager requests are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Addresses         | • For **Requestors** (if there is a repository): Applications that represent the assets of the source. Click ⬤ to search for specific application objects.  
                      • For other users: The original representation of the source addresses in firewall objects. If there is a repository, application objects are also listed. Click ⬤ to search for specific objects (see page 37). |
| Type IP Addresses | A comma-separated list of source IP addresses for which access is requested to be added or blocked.  
                      • Separate the values of a range with a hyphen. |
| Users             | The users for whom access is needed. Possible values:  
                      • Any  
                      • Unknown User  
                      • Known User  
                      • Specific users or user groups (select **Specific** and then type in the user and group names) |
| **Destination**   |                                                                                                                                              |
| Addresses         | • For **Requestors** (if there is a repository): Applications that represent the assets of the destination. Click ⬤ to search for specific application objects.  
                      • For other users: The original representation of the destination addresses in firewall objects. If there is a repository, application objects are also listed. Click ⬤ to search for specific objects (see page 37). |
| Type IP Addresses | A comma-separated list of destination IP addresses for which access is requested to be added or blocked.  
                      • Separate the values of a range with a hyphen. |
| Services & Applications | • For **Requestors** (if there is a repository): Objects that represent the services (ports) used for the access. Click ⬤ to search for specific service objects.  
                      • For other users: The original representation of the ports in firewall objects. If there is a repository, service objects are also listed. Click ⬤ to search for specific objects (see page 37). |
| Type Port         | The services (ports) for which access is requested to be added or blocked.                                                                  |
**Property** | **Description**
---|---
Use application default ports as services | If an application is selected, Skybox sets the service to be the default service for that application. You can select a different service.

**Additional fields**

| Property | Description |
---|---|
Rule Logging | Specifies whether changes to the relevant access rules should be logged in the firewall. |
Comment | A comment to add to the change request. |
Expiration Date | The expiration date of the access rule. |

**Uploading a file with multiple requests**

If your organization has configured this, you can create an Excel or CSV file that contains the information for multiple Access Update change requests and then upload the file directly to a Change Manager ticket.

For Change Manager to use the change requests in your file, both the file and the data must obey certain rules. For example, Change Manager looks for each part of the change request in columns of specific names. You must format the data correctly.

If your organization has created a template file, you can download it to use for creating your change requests.

*To download the template file*

1. In a new ticket, click **Upload**.
2. Click the link in the **Template** field to download the template file.

After filling in the change requests and saving the file, use the following directions to upload it to a Change Manager ticket.

*To upload a file of access update change requests to Change Manager*

1. Open a new ticket.
2. Click **Upload**.
3. Next to the **File** field, click ![image].
4. Navigate to the file and click **Open**.

   *Note: Change Manager requires that the file include the fields that were configured, so you must use the template and only enter information in that format. Otherwise, the file cannot be uploaded.*

5. After the file is previewed a dialog box appears. You can see all the change requests in the file.

   If Change Manager detected an error or missing value in any field of a change request, there is an X in the problematic field and in the **Valid** field of that request. Change requests that are not valid are not added to the ticket.

6. You can make changes to a change request by selecting it and clicking **Edit**; you can delete a change request from the list by selecting it and clicking **Remove**.

7. When you are finished, click **OK**.

   The valid change requests are added to the ticket.
Adding an access rule

You can use Skybox Change Manager to request that a specific access rule be added to a specific firewall.

To request a new access rule on a firewall
1. Click **Add Rule**.
2. Fill in the fields, as specified in **Access rule properties** (on page 35).
3. Click **OK**.
4. (Optional) Set the rule’s **business attributes** (on page 38).

Positioning of new access rules

The first time that a ticket is saved or promoted, Change Manager checks the requests to see if they are necessary or if their coverage already exists. For necessary rules, Change Manager then checks the requested rule against existing rules in the ACL to suggest where in the list to add the new rule. For new rules that are partially or completely blocked by existing rules, Change Manager suggests adding the new rule before the 1st blocking rule. All other rules can be added at the end of the list.

Access rule properties

The properties of access rules available for Skybox Change Manager requests are described in the following table. Some properties (for example, **Create After**) are not available for all request types.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>The firewall or cluster to which to add the rule.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the access rule.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Addresses</td>
<td>• For <strong>Requestors</strong> (if there is a repository): Objects that represent the assets of the source. Click ![search icon] to search for specific application objects.</td>
</tr>
<tr>
<td></td>
<td>• For other users: The original representation of the source addresses in firewall objects. If there is a repository, application objects are also listed. Click ![search icon] to <strong>search for specific objects</strong> (see page 37).</td>
</tr>
<tr>
<td>Type IP Addresses</td>
<td>A comma-separated list of source IP addresses for this rule (the permitted source addresses for a packet).</td>
</tr>
<tr>
<td></td>
<td>• Separate the values of a range with a hyphen.</td>
</tr>
<tr>
<td>Negate</td>
<td>Specifies whether to use all valid sources (IP addresses or objects) except those selected, select <strong>NOT</strong>.</td>
</tr>
<tr>
<td>Users</td>
<td>The users that the request is for. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• Any (default)</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Known User</td>
</tr>
<tr>
<td></td>
<td>• Specific users or user groups (Select <strong>Specific</strong> and then type in the user and group names)</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Destination Addresses** | • For **Requestors** (if there is a repository): Objects that represent the assets of the destination. Click ⬤ to search for specific application objects.  
  • For other users: The original representation of the destination addresses in firewall objects. If there is a repository, application objects are also listed. Click ⬤ to search for specific objects (see page 37). |
| **Type IP Addresses**     | A comma-separated list of destination IP addresses for this rule (the permitted destination addresses for a packet).                                                                                       |
|                           |  • Separate the values of a range with a hyphen.                                                                                                                                                    |
|                           |  • To permit all destination addresses except those selected, select NOT.                                                                                                                                  |
| **Negate**                | Specifies whether to use all valid destinations (IP addresses or objects) except those selected.                                                                                                            |
| **Services & Applications**| • For **Requestors** (if there is a repository): Objects that represent the services (ports) used for the access.                                                                                     |
|                           |  • For other users: The original representation of the ports in firewall objects. If there is a repository, service objects are also listed. Click ⬤ to search for specific objects (see page 37). |
| **Type Ports**            | The services (ports) for this rule (the permitted services for a packet).                                                                                                                              |
| **Negate**                | Specifies whether to use all valid services (ports or objects) except those selected.                                                                                                                   |
| **Rule Group**            | The rule group to which to add this access rule upon creation.                                                                                                                                           |
|                           | **Note**: This information is not added to the access rule.                                                                                                                                              |
| **NAT**                   |                                                                                                                                                                                                          |
| **Hide Source Behind Gateway** | Specifies whether source networks are hidden behind the gateway IP address (they are translated to the IP address of the gateway or firewall).                                                                  |
| **Source Addresses**      | A comma-separated list of source NAT IP addresses for this rule (the permitted source addresses for a packet).                                                                                         |
|                           |  • Separate the values of a range with a hyphen.                                                                                                                                                       |
|                           |  • To permit all source addresses except those selected, select NOT.                                                                                                                                   |
| **Objects**               | The original representation of the source NAT addresses in firewall objects. Click ⬤ to search for specific objects (see page 37).                                                                          |
Chapter 6  Using Skybox Change Manager

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Addresses | A comma-separated list of destination NAT IP addresses for this rule (the permitted destination addresses for a packet).  
  - Separate the values of a range with a hyphen.  
  - To permit all destination addresses except those selected, select NOT. |
| Objects | The original representation of the destination NAT addresses in firewall objects. Click to search for specific objects (see page 37). |
| Services | Ports | The service NATs (ports) for this rule (the permitted services for a packet). |
| Services | Objects | The original representation of the service NATs in firewall objects. Click to search for specific objects (see page 37). |
| Additional Fields | Rule Logging | Specifies whether changes to this rule should be logged in the firewall. |
| Additional Fields | Comment | A comment or additional information about the change request. |
| Additional Fields | Create After | Information about where to create the rule for the user who makes the actual change on the firewall.  
  **Note:** This information is not added to the access rule. |
| Additional Fields | Expiration Date | The expiration date of the access rule. |
| Additional Fields | VPN | Specifies the VPN over which to send data. |

**Object finder**

To find an object using the Object Finder dialog box

1. Select the firewall, firewall cluster, or management system in which to search for the object.  
  **Note:** In many situations, this field is read-only.

2. In the Search field, type a string.  
   You can use the characters ? and * for standard pattern matching; type * to display all rules.

3. Click .  
   The objects that meet the search requirements are listed in the Matching Objects box. If there is a repository, there are separate tabs for firewall objects, repository objects, and all objects.

4. Select desired objects from each tab and click to move them to the Selected Objects box. Click OK.

5. If a firewall object that you need does not exist, use the following instructions to open a request to create it.
To create a request for a new firewall object from within the Object Finder

1 Click **New Object**.
2 Provide the necessary information about the new object, according to the following table.
3 Click **OK**.
   - A change request for the new object is created.
   - The new object is added to the set of searchable objects for the firewall or management system for which it was created. If the new object is used in additional change requests, it appears as a link to its change request.

The properties of a new object are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the new object.</td>
</tr>
<tr>
<td>Type (read-only)</td>
<td>The type of the object (network or service).</td>
</tr>
<tr>
<td>Value</td>
<td>The value of the new object. For a network object, this is the IP addresses or IP address ranges; for a service object, it is the ports or port ranges.</td>
</tr>
<tr>
<td>Members</td>
<td>For group objects, the members of the group, consisting of either existing objects or new objects. You can only add one layer of members.</td>
</tr>
<tr>
<td>Comment</td>
<td>Any information about this object for the firewall administrator.</td>
</tr>
</tbody>
</table>

Setting business attributes for an access rule

You can set the business attributes of an access rule for which there is a change request.

**To set rule attributes**

1 In the list of change requests, select the change request with the desired access rule.
2 Click **Set Attributes**.
3 Make the necessary changes and click **OK**.

Modifying access rules

You can use Skybox Change Manager to request the following modifications to specific access rules:

- Adding or removing specific access from the rule
- Changing the services and applications to which the rule applies
- Changing the rule owner
- Changing the position of the rule in the policy
- Changing whether the rule is logged in the firewall

Note: Each change requires a separate change request.
To request that specific access rules be modified

1. Click **Modify Rules**.
2. In the Modify Rules – New Change Request dialog box, click to select the access rules to change.
3. In the Select Access Rules dialog box, select the desired firewall or cluster.
4. In the **Search** field, type a string that is part of the access rules that you want to modify.
   
   You can use the characters ? and * for standard pattern matching; type * to display all rules.
5. Click .
   The access rules that match the search criteria are displayed.
6. Select the rules to modify and click the arrow to move them to the Selected Access Rules box.
7. Click **OK**.
8. In the **Modification Details** pane:
   a. Select the field to modify.
   b. Make the required changes, either manually or by clicking to search for specific objects (see page 37).

   Note: Selecting **Rule Logging** toggles the rule logging of the selected rules; you do not have to make any additional changes.

   Note: Unless you selected **Users** or **# (Rule Position)**, you can negate the value of the selected field.
9. Click **OK**.
10. If necessary, update the rule’s **business attributes** (on page 38).

**Deactivating and enabling access rules**

You can use Skybox Change Manager to request that specific access rules be deactivated (disabled or deleted) to block access or cleanup unnecessary rules. You can also request that specific disabled rules be activated (enabled).

To request that specific access rules be deactivated

1. Click **Deactivate Rules**.
2. In the Deactivate Rules dialog box:
   a. Select the firewall.
   b. In the **Search** field, type a string to use in identifying the access rules to be deactivated.
      
      Type * to display all rules.
   c. Click .
      
      The access rules that match the search criteria are displayed.
   d. Select the rules that you want to deactivate and click the arrow to move them to the Selected Access Rules box.
e. To delete the rules rather than disable them, select **Delete Rules** in the **Action Required** field.

f. Click **OK**.

*To request that specific access rules be activated (enabled)*

1. Click **Activate Rules**.

2. In the Activate Rules dialog box:
   a. Select the firewall.
   b. In the **Search** field, type a string to use in identifying the access rules to be deactivated.
      Type * to display all rules.
   c. Click.
      The access rules that match the search criteria are displayed.
   d. Select the rules that you want to activate and click the arrow to move them to the Selected Access Rules box.
   e. Click **OK**.

**Modifying firewall objects**

You can use Skybox Change Manager to request that specific firewall objects be modified. You do this by adding or deleting entities or objects from the selected object.

*To request changes to firewall objects*

1. Click **Modify Object**.

2. Select the object to modify:
   a. In the Selected Object area, click the **Browse** button to open the Object Finder.
   b. Click the **Browse** button next to the **Firewalls/Management Server** field.
   c. Select the firewall management systems or individual firewalls to which the object is relevant, and click the arrow to move them to the right-hand field.
   d. In the **Search** field, type a string.
   e. You can use the characters ? and * for standard pattern matching; type * to display all objects for the selected firewalls.
   f. Click.
   g. The objects that match the search criteria are displayed.
   h. Select the object to modify and click the arrow to move it to the **Selected Object** box.
   i. Click **OK**.
3 Define the properties of the object that you want to change in the Modification Details pane. The pane is filtered according to the type of the selected object; you can only enter entities or select objects to add or delete that match the object type.
   a. Use the **Name** field to change the name of the object.
   b. In the Modification Details pane, type entities or **select objects** (see page 37) add to or delete from this object.
   c. Add a comment.

4 Click **OK**.

**Custom change requests**

In addition to the regular change request types provided by Skybox, administrators might have created custom change request types that you can use to enter requests.

*To make a custom change request*

1 Click **More** and then select the change request type.

   The New Change Request dialog box appears.

2 Select whether the change request relates to a firewall or management server, or to access rules.

3 Click the **Browse** button and select the relevant firewall or management server, or the relevant access rules.

4 Fill in the values of the fields, as you would for any change request.

   Mandatory fields are marked with an asterisk.

   - In the **Change Details** field, provide a description of the requested change and any other necessary information.
   - Add an expiration date.
   - Add additional comments.

5 Click **OK**.

**Adding business information to an access rule**

You can add business information about the access rule to a change request in the **Request** and **Technical Details** phases.

To add this information, select the change request in the ticket and click **Set Attributes**.

You can add the following information:

- **Rule Owner:** The owner of the access rule
- **Owner Email:** The rule owner email address
- **Next Review Date:** The date when the access rule should be reviewed
- **Business Function:** The business function of the access rule
- **Comment:** A comment about the rule
- **(Optional) Custom Attribute fields:** If custom business attributes were defined, you can add their information here
PROCESSING TECHNICAL DETAILS

Technical users review new tickets that are in the Technical Details phase.

The 1st job in this phase is to make sure that there are formal change requests in the ticket. If the original request was added as a free-text description only, users in this phase must formalize it to create change requests (on page 42).

After the ticket contains formal change requests, Skybox checks these requests against the model. The results of the checking process are derived change requests, which are listed underneath the list of original requests.

These derived change requests need to be reviewed to make sure that they are correct and necessary (on page 42).

Reviewing tickets that have no formal change requests

To review a new ticket that does not include any formal change requests

1. Open the ticket.
   The Technical Details tab is displayed.
2. In the ticket details at the top of the page, examine the Title and Description to understand the requested access.
3. Add requests to the ticket:
   - Request specific access (on page 32) between a source and a destination
   - Add an access rule (on page 35)
   - Modify access rules (on page 38)
   - Deactivate an access rule (on page 39)
   - Modify firewall objects (on page 40)
   - Multiple requests for specific access (by uploading a file (on page 34))
   Alternatively, you can add a custom change request (see page 41) of a type created specifically for your organization.
4. Save the ticket.

Reviewing the derived change requests

The main task in this phase is reviewing and updating the derived change requests:

- Check whether the changes are necessary. If the requested access exists, the changes are unnecessary. If all the derived change requests are unnecessary, you can close (reject) the ticket.
- Access Update change requests are not firewall-specific. When Change Manager derives requests from them, it might miss a firewall or suggest changing the wrong firewall because of inaccurate or incomplete routing rules on the firewalls. Users in this phase must validate that the breakdown is correct and fix it.

To review the derived change requests of a new ticket

1. Open the ticket.
   The Technical Details tab is displayed.
2 Look at the Original Change Requests panel. If none of the requests are required (that is, all the Change Required values are No), all the requested access exists. Click Reject to send the ticket back to the requester for closure.

3 Look at the Derived Change Requests panel. Check whether the derived change requests suggested by Skybox cover all the necessary firewalls, make sense, and are in line with your firewall policy.

Note: If some of the derived change requests in the ticket are obfuscated, they are for firewalls owned by other users. In this case, mark your change requests as Reviewed (select a change request and click Review).

If the derived change requests are not what you expected, edit the original change request or add additional requests. You can delete derived change requests by selecting them and clicking Remove.

4 Derived change requests that are unnecessary have linked explanations as to why they are unnecessary. Click the link to see the existing rules that cover this request.

5 To add additional firewalls to or delete unnecessary firewalls from the selected derived request, click Firewalls and add or remove the relevant firewalls. Skybox creates the corresponding derived change requests for these firewalls.

6 If the ticket is overdue, revise the due date for the current phase. The due dates for future phases are revised accordingly.

7 Click Promote.

To change the owner for the next phase, click (next to the suggested owner’s name) and select a different owner.

Note: If you do not have permissions for all the change requests, there is a Review button instead of Promote.
8 Click **OK**.

- For tickets with a single owner, the ticket is promoted to the next phase (usually **Risk Assessment**).
- For tickets with multiple owners, the ticket is only promoted after all the owners have reviewed their change requests.

### ASSESSING RISK

In the **Risk Assessment** phase, security analysts review the tickets to check whether the requested access is justified in terms of risk.

The risk of the requested changes to your organization is displayed in the **Risk Assessment** tab. For each change request there is a list of:

- All the Access Policy and Rule Policy violations that the requested change would cause
- All the vulnerability occurrences to which the requested change would expose your organization

**Note:** Skybox does not calculate risk for change requests that add Deny rules. These requests are considered both compliant and secure.

Analysts reviewing tickets in the **Risk Assessment** phase:

1. Check the due date of the ticket. If it is overdue or seems unreachable, revise the due date for the current phase (and Skybox modifies subsequent due dates).
2. Check whether each request is compliant with your organization’s Access Policy and Rule Policy and view the violations if it is not.
3. Check whether each request exposes your organization’s network to any Vulnerability Definitions and view the exposed Vulnerability Definitions.
4. Based on the 2 previous steps, determine the overall risk of the ticket.
5. If there are policy violations, decide whether to approve them, and whether to limit your approval until a specific expiration date. After the ticket is verified, these changes are no longer displayed as violations in Change Manager or Firewall Assurance until their expiration date is reached.
6. If the risk continues to be very high, decide whether to demote the ticket to a previous phase (or to the **Requestor**) with an explanation. Otherwise, promote the request to the next phase.

**To assess the risk of a ticket**

1. Select a ticket (in the **Risk Assessment** phase).

   The **Risk Assessment** tab is displayed.

   In the Risks pane, the list of original change requests shows whether each change request is compliant with your organization’s Access Policy and Rule Policy, and secure from Vulnerability Definitions.
2 After you look at the overall risk of each original change request, change the view to **Derived Change Requests**.

3 Review each change request that is not compliant.

   a. With the request selected in the table, look at the Compliance: Policy Violations table. Each violation shows the policy type and the part of the affected policy that would be violated if this request is implemented. Because violations might exist for other reasons also, violations that are only a result of the request are marked as new.

   Note: If you are working with recertification requests, all the policy violations and vulnerability occurrences for the access rule are listed, to help you to determine the risk of recertifying the rule.

   ![Compliance: Policy Violations Table](image)

   b. If you decide that the risk of the change request is acceptable (at least temporarily), click **Approve**.

   c. In the Approve Request dialog box, select either **Approve Until** or **Approve with No Expiration**. If you select **Approve Until**, an expiration date is displayed. This date is determined by the highest severity of all the violations. Higher severities have closer expiration dates. (You can change the expiration date.)

   Note: For recertification requests, Skybox uses the expiration date as the date on which the access rule must be reviewed again.

   For each violation, an exception is created (but not yet activated). The exception expires on the specified date. After the ticket is verified, the exceptions are activated, and the violations are not visible again in either Change Manager or Firewall Assurance until after the expiration date.

4 Review each change request that is not secure. With the request selected in the table, look at the **Security: Vulnerability Definitions with Exposed Assets** table. The network will be exposed to these Vulnerability Definitions if the change request is implemented. Vulnerability Definitions that were not exposed before and are only exposed due to the change request, are marked as new.

   ![Security: Vulnerability Definitions with Exposed Assets Table](image)

   - You can check the available solutions for each exposed Vulnerability Definition by clicking the link in the **Solutions** column.

5 Based on your review, specify the risk of the ticket:

   a. Assign a risk value: **High**, **Medium**, or **Low**.

   b. In the **Assessment Details** box, type your assessment of the risk. This can include separate risks for each request.

   Note: This assessment is added to the **Comment** field of any exceptions that are created.
6 If the risk is reasonable in your opinion, or if a supervising manager gave clearance (outside Skybox) for the request, **Promote** the ticket to the next phase (usually **Implementation Details**). You can add an attachment or a **Risk Justification** comment.

*Reasonable* risk usually means that the request is acceptable and valid/legitimate.

If the risk is too high, demote the ticket to a previous phase for additional review and update of the requests or back to the **Requestor** to revise the requests. Make sure to add a comment explaining the problem.

Note: If you do not have permissions for all the change requests, there is a **Review** button instead of **Promote**. After all the change requests in the ticket are reviewed by their owners, it is promoted automatically.

7 If there are no approved change requests when you promote the ticket, you are asked whether to approve the change requests as part of the promotion. The effects of approval are the same as those explained in step 3.

**IMPLEMENTATION PHASE**

The **Implementation Details** tab includes a list of changes to be made on the firewalls. Use this tab to track and comment on tickets, and for tickets that require urgent implementation. We recommend that the actual implementation be done via the **Pending Implementation** view, where change requests are grouped by firewalls, in a way that is suitable for the firewall administrators that implement the changes.

The tasks in this phase are often split between the following users:

› Firewall administrators, who implement the changes on the firewalls
› Users who oversee the tickets

Users in this phase:

1 Check whether the ticket is overdue, and whether the current phase due date can be met. If necessary, revise the due date of the current phase. Due dates of subsequent phases are revised accordingly.
   • Make the necessary changes on the firewalls.

   For information about the **Pending Implementation** view, see Change implementation (on page 50).

2 Promote the ticket to the **Verification** phase, so that Skybox can reanalyze the connectivity of the change request based on the updated firewalls.

*To implement the change requests in a ticket*

1 Select a ticket in Implementation Details phase.

2 To view a preview of implementation changes for selected not-yet-implemented change requests in a separate window, select the change requests and click **Implementation Preview**.

Note: If you do not have permissions for all the change requests, you only see the requests that you own.
3 (Optional) Set a target date for the implementation and add details. Some organizations require a target date.

4 For firewall administrators (do one of the following):
   - Switch to the Pending Implementation view and implement the change requests (on page 51) for the firewall.
   - Select the changes to implement in this ticket and click Implement Change Requests.

   Note: Even if you are using automatic implementation, you must perform this step.

5 Tickets whose change requests are all marked as implemented are promoted automatically and are no longer visible in Pending Implementation. If the ticket was not promoted, promote it manually to the final phase (usually named Verification or Pending Closure). (When you promote a ticket, its change requests are marked as implemented.)

By default, tickets are sent to their Requestors for verification. After the Requestor reviews the ticket, they usually close it.

   Note: After a ticket is promoted to the verification phase, the existing requests can no longer be changed, even if the ticket is later demoted to earlier phases. If you need to make additional changes, you can add new requests to the ticket or create a new ticket.

**VERIFYING A REQUEST**

After the firewall changes are implemented, Skybox rechecks the change requests the next time firewall data is imported. An Analysis – Change Requests task, scheduled to run after the import cycle, checks the requests.

- If all the change requests are implemented (that is, there is access between the source and destination over the specified port), Skybox changes the status of the ticket to Verified, and the ticket is sent back to its original Requestor, who usually closes it.

  If notifications are set up for Access Change tickets, then the owner receives a notification about the change in the ticket status.

- If there are unimplemented change requests, Skybox reopens the ticket. Usually, the Requestor then checks the ticket and closes it.

  Optionally, workflow supervisors can review the tickets in this phase and decide to close the verified tickets or add additional suggestions to reopened tickets.

**Rejected tickets**

A ticket that is rejected for any reason is given a status of Rejected and returned to its Requestor. It should usually be closed, but the Requestor can reopen it and fix the properties.
To close a ticket

1. Select the ticket.
2. Click Close.
3. Add a comment to the ticket before you close it.
4. Click OK.

ADDITIONAL WORKFLOW ACTIONS

In addition to handling existing tickets in a specific phase, you can use Skybox Change Manager to:

- Request recertification of an access rule, if this action is enabled
- Clone a ticket—create a new ticket based on an existing ticket
  The new ticket does not have the history or attachments of the original ticket, but all other fields are the same. You must make at least one change in the new ticket before you can save it.
- Reassign a ticket to a different user
- Revise the due date of the current phase (Skybox revises the due dates of subsequent phases)
- Add a comment to a ticket
- Add attachments to a ticket and view the existing attachments
- View the history (change log) of a ticket
- Change the status of open tickets (if this option is enabled)
  Open tickets have a status of New, In Progress, Reopened, or any custom status whose status group value is Open.
- Reject a ticket

Note: Requestors can only manage the 1st and last phases of the tickets.
Chapter 7

Rule recertification

Rule recertification tickets are opened by users in Skybox Firewall Assurance or Skybox Network Assurance, or automatically for access rules that are scheduled to be reviewed in the near future (via rule recertification ticket policies). Each recertification ticket includes at least 1 access rule.

After recertification tickets are opened, they are handled in Change Manager. They generally go through a different workflow than other tickets, with fewer steps.

**Typical rule recertification workflow**

1. In the request (1st) phase of rule recertification tickets, review the requests and determine the access rules to certify and those to reject (not recertify). You can view all the violations and vulnerability occurrences for each access rule to help you to decide the risk of recertifying it. You can also add or update business attributes (for example, rule owner and email) in the access rules, and you can update the next review date.

   After determining whether to certify or reject each rule, promote the ticket to the next phase.

2. In the assessment (2nd) phase, review and modify the decisions made in the 1st phase (which rules to certify or reject), by someone who is a higher security authority.

   The ticket cannot be promoted until all the access rules are marked as either certified or rejected.

3. In the verification (final) phase, close the ticket. After the ticket is closed, the changes are applied to the access rules, including the change to their status and any changed business attributes.

4. If any access rules were rejected rather than recertified, we recommend that you open tickets on those access rules to disable or modify them as needed.
Chapter 8

Change implementation

For firewall administrators who must implement change requests, it is helpful to view the requests grouped by firewalls. To do this, use the **Pending Implementation** view, which lists all change requests from tickets in the implementation phase.

When you work in the **Pending Implementation** view, you can:

- View a list of change requests that are ready to be implemented
- Assign change requests to specific users or user groups (for implementation)
- Mark change requests as implemented (or not implemented)
- Automatically implement change requests for Check Point, Palo Alto Panorama, and Fortinet FortiManager devices
- View each change request in command format (the format used on the firewall itself)
  
You can select multiple change requests to view their commands together.

- Add comments to change requests

In this chapter

**Viewing a specific set of change requests** .................................................. 50
**Assigning change requests** ................................................................. 50
**Implementing change requests** ............................................................. 51

**VIEWING A SPECIFIC SET OF CHANGE REQUESTS**

The default display in the **Pending Implementation** view shows all change requests that are not yet implemented. Use the **View** field to display a different set of change requests.

**ASSIGNING CHANGE REQUESTS**

You can assign change requests to yourself or to another user.
To assign change requests to yourself, select the change requests and click **Assign to Me**.

To assign change requests to a specific user, select the change requests and click **Assign**; select the user.

In both cases, you must add a comment to the change request.

**IMPLEMENTING CHANGE REQUESTS**

You can implement change requests in the **Pending Implementation** view in either of 2 ways:

- **View the change requests in command format** (see page 51) and then **mark them as implemented** (see page 52) in Skybox
  
  This format can help you to understand the changes that you need to make. It saves time because you can copy and paste relevant parts of the command text directly. Sometimes, these are generic representations. For many request types on Cisco devices, a representation of the command is displayed in Cisco format.

- **Automatically** (see page 53)

**Viewing change requests in command format**

For devices on which automatic implementation is not supported, you can view the change requests in command format.

- Select change requests from the list and click **Implement**.
A separate window shows the commands to use on the firewall for each selected change request.

Sometimes, these are generic representations. For the following changes on Cisco devices, a representation of the command is displayed in Cisco format:

- Add Rule
- Modify Rule
- Deactivate Rule
- Add Object
- Modify Object

You can copy the commands in this window directly to the CLI, but they might need editing to make them completely compatible with the command format used on the firewalls.

**Marking change requests as implemented**

After you finish manually implementing a change request on the firewall or firewall server, select the change request and click **Mark as Implemented**. Add any relevant information to the change request as a comment.

**Note:** Use **Mark as Not Implemented** if a change request was mistakenly marked as implemented.
When all the change requests for a specific ticket are marked as implemented, the ticket is promoted to the **Verification** phase and its change requests are no longer visible in **Pending Implementation**.

**Automatic implementation**

Change Manager provides the option of automatically implementing some change requests directly to Check Point, Palo Alto Panorama, and Fortinet FortiManager devices.

**Supported device types and versions**

The following table lists the tested versions of each supported device type, and other relevant information.

<table>
<thead>
<tr>
<th>Device type</th>
<th>Version</th>
<th>Additional information</th>
<th>Add Rule</th>
<th>Add Object</th>
<th>Modify Rule</th>
<th>Modify Object</th>
<th>Delete/Disable Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point CPMI</td>
<td>R77</td>
<td>• Expiration dates are not supported in Add Rule. • Modify Rule is not supported.</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R80, R80.10</td>
<td>• Modify Rule is supported from R80.10 and higher. • Layered policies are not supported.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Check Point Security Management</td>
<td></td>
<td>• Layered policies are not supported.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco ASA</td>
<td>9.3(2), 9.9(2)</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Firepower</td>
<td>6.2.3, 6.3</td>
<td>You must implement the Add Object and Add Rule change requests at the same time.</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet FortiManager</td>
<td>5.2, 5.4, 5.6</td>
<td>The policy must be installed on a VDOM.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Palo Alto Panorama</td>
<td>PA OS 7.1, PA OS 8.0</td>
<td>An administrator can define whether the new rules are added as Pre Rules or Post Rules (in Tools &gt; Options &gt; Server Options)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: For best results, it is recommended to use these versions.
Supported change request types

The following change request types can be automatically implemented on all supported devices unless noted otherwise in the preceding section (on page 53).

› Add Rule
Support is available for: expiration dates, comments, networks, hosts, ranges, and TCP, UDP, and ICMP services.

› Add Object
Support is available for source, destination, service, and object comments.

› Modify Rule
Support is available for: Allow rules, Deny rules, source, destination, and service.

Global rules cannot be modified.

› Modify Object (Fortinet FortiManager only)
For details, see Implementation of Modify Object change requests (on page 54).

Change request types that are not supported for automatic implementation

The following change requests can only be implemented manually:

› Change requests with NAT
› Change requests that include negated source, destination, or service values
› Change requests that include users and applications
› Modify Object (except in Fortinet FortiManager)
› Deactivate Rule (except in Check Point R80)

Implementation of Modify Object change requests

Automatic implementation of Modify Object change requests is supported only for Fortinet FortiManager.

The following changes are supported per object type.

› For single objects (hosts, networks, IP address ranges, services):
  • Add / remove / replace values in the object

› For object groups (groups of hosts, networks, IP address ranges or services):
  • Add / remove objects (single or lists)

Note: Nested objects (in sub-groups) are not removed.
The following actions are not supported:

- Object renaming
- Changes to global objects

**Implementing the change requests**

Changes are calculated and implemented on the active policy only. After the changes are made and saved, the policy must be installed (activated) manually.

During automatic implementation:

- If the same field of a rule is modified in 2 separate requests, a collection task must be run before implementing the 2nd request.
- A collection task must be run before using a new object in a ticket.

**To implement change requests**

1. Select the relevant change requests in the list and click **Implement**.

   A list of changes to be implemented appears. Usually, in addition to the change requests that you suggested, there are additional change requests in this list. For example, if you select an Add Rule change request, all the Add Object change requests that are necessary for the Add Rule are in the list and are also selected. There may be other change requests for the same management server.

   If you selected any change requests that cannot be implemented automatically, they are listed in a pop-up message.

2. Review the list and select any other change requests that should also be implemented. You can also clear any change requests that you do not want to implement now.

3. Click **Implement Changes**.

4. Add an implementation comment and click **OK**.

   Change Manager performs implementation in the background and the status of each change request is updated appropriately. On success, requests are marked as implemented and shown in the Implemented tab. Failed requests remain in the pending list and you can view their failure reason.

**What happens to change requests that are successfully implemented?**

Whenever possible, Change Manager adds each new rule to the policy before the first rule that blocks its traffic (as calculated in the Skybox Access Analyzer). If this is not possible, the rule is added as the last rule in the policy. In this case, an **Admin** must open the policy on the management server and reposition each new rule.

An **Admin** must also install the policy (that is, activate it).
Chapter 9

Exporting information from Change Manager

You can export tables from Change Manager to CSV files, whether the table is inside a ticket or takes up the entire workspace. To export a table, click 

**Exporting workspace tables**

For workspace tables, Skybox uses the following naming convention, where the view can be any of those in the control pane or a selected analysis:

> `<view name>_<timestamp>.csv`

**Exporting tables within tickets**

Skybox uses the following naming convention:

> `<panel name>_<phase name>_phase_Ticket_<ticket#>_<timestamp>.csv`

In the **Risk Assessment** phase, the tables depend on which change request is selected and Skybox uses the following convention:

> `<panel name>_<request>_<phase name>_phase_Ticket_<ticket#>_<timestamp>.csv`