Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=13959
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R75.40 home page (http://supportcontent.checkpoint.com/solutions?id=sk67581).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 May 2012</td>
<td>Updated permission options</td>
</tr>
<tr>
<td>16 April 2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SmartWorkflow R75.40 Administration Guide).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td><strong>SmartWorkflow Overview</strong></td>
<td>5</td>
</tr>
<tr>
<td>Why is Change Management Important?</td>
<td>5</td>
</tr>
<tr>
<td>Terms and Concepts</td>
<td>5</td>
</tr>
<tr>
<td>Key Features</td>
<td>6</td>
</tr>
<tr>
<td>How SmartWorkflow Works</td>
<td>6</td>
</tr>
<tr>
<td>SmartWorkflow Environment</td>
<td>6</td>
</tr>
<tr>
<td>Task Flow</td>
<td>7</td>
</tr>
<tr>
<td><strong>Working with the SmartWorkflow GUI</strong></td>
<td>9</td>
</tr>
<tr>
<td>The SmartWorkflow Toolbar</td>
<td>9</td>
</tr>
<tr>
<td>The SmartWorkflow Session Management Window</td>
<td>10</td>
</tr>
<tr>
<td>The SmartWorkflow Session Information Pane</td>
<td>11</td>
</tr>
<tr>
<td><strong>Configuring SmartWorkflow</strong></td>
<td>12</td>
</tr>
<tr>
<td>Assigning Permissions</td>
<td>12</td>
</tr>
<tr>
<td>Defining Permissions for Security Management Server</td>
<td>12</td>
</tr>
<tr>
<td>Defining Permissions for Multi-Domain Security Management</td>
<td>13</td>
</tr>
<tr>
<td>Enabling the SmartWorkflow Blade</td>
<td>13</td>
</tr>
<tr>
<td>Configuring SmartWorkflow Properties</td>
<td>14</td>
</tr>
<tr>
<td><strong>Working with Sessions</strong></td>
<td>15</td>
</tr>
<tr>
<td>Starting a New Session</td>
<td>15</td>
</tr>
<tr>
<td>Continuing a Session in Progress</td>
<td>15</td>
</tr>
<tr>
<td>Working Without a SmartWorkflow Session</td>
<td>16</td>
</tr>
<tr>
<td>Viewing Sessions</td>
<td>16</td>
</tr>
<tr>
<td>Moving Between Changed Rules and Objects</td>
<td>17</td>
</tr>
<tr>
<td>The Session Information Pane</td>
<td>17</td>
</tr>
<tr>
<td>Submitting Sessions for Approval</td>
<td>17</td>
</tr>
<tr>
<td>Discarding Session Changes</td>
<td>17</td>
</tr>
<tr>
<td><strong>Managing and Approving Sessions</strong></td>
<td>18</td>
</tr>
<tr>
<td>Reviewing Sessions</td>
<td>18</td>
</tr>
<tr>
<td>Security Configuration Change Summary Report</td>
<td>18</td>
</tr>
<tr>
<td>Viewing a Submitted Session</td>
<td>19</td>
</tr>
<tr>
<td>Comparing Policies</td>
<td>19</td>
</tr>
<tr>
<td>Comparing Submitted Sessions</td>
<td>21</td>
</tr>
<tr>
<td>Approving Sessions</td>
<td>21</td>
</tr>
<tr>
<td>Requesting Repairs to Sessions</td>
<td>21</td>
</tr>
<tr>
<td>Repairing Sessions</td>
<td>22</td>
</tr>
<tr>
<td>Installing the Security Policy</td>
<td>22</td>
</tr>
<tr>
<td><strong>Auditing Changes with SmartView Tracker</strong></td>
<td>23</td>
</tr>
<tr>
<td>Viewing Session Activity in SmartView Tracker</td>
<td>23</td>
</tr>
<tr>
<td>Auditing Objects and Rules in SmartView Tracker</td>
<td>24</td>
</tr>
<tr>
<td>Creating Custom SmartView Tracker Queries</td>
<td>24</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>25</td>
</tr>
</tbody>
</table>
Chapter 1

SmartWorkflow Overview

SmartWorkflow Blade is a security policy change management solution that tracks proposed changes to the Check Point network security environment, and ensures appropriate management review and approval prior to implementation.

In This Chapter

Why is Change Management Important? 5
Terms and Concepts 5
Key Features 6
How SmartWorkflow Works 6

Why is Change Management Important?

Managing network operations while accurately and efficiently implementing security policies is a complex process. Security and system administrators find it increasingly difficult to ensure that all security gateways, network components and other system settings are properly configured and conform to organization security policies.

As enterprises evolve and incorporate technological innovations, network and security environments have become increasingly complex and difficult to manage. Typically, teams of engineers and administrators are required to manage configuration settings, such as:

- Security Policies and the Rule Base
- Network Objects
- Network Services
- Resources
- Users, administrators, and groups
- VPN Communities
- Servers and OPSEC Applications

An effective enterprise security policy change management solution is also essential to ensure compliance with increasingly stringent corporate governance standards and regulatory reporting requirements.

Terms and Concepts

This section defines several SmartWorkflow terms and concepts.

- **Session**: A set of additions and modifications to the network security environment performed using SmartDashboard. Each session is identified by a unique name and session ID.
- **Administrator**: A system or security administrator responsible for maintaining the network and security environment using SmartDashboard or Multi-Domain Security Management.
- **Manager**: The individual responsible for approving all modifications made by administrators and for enabling and configuring SmartWorkflow.
- **Role Segregation**: Role segregation ensures that changes made by administrators are approved by authorized managers and that only managers can enable, disable and configure SmartWorkflow.
Key Features

- SmartWorkflow Sessions allow administrators to work with discrete sets of additions and modifications to the security and network environment. The use of sessions is optional.
- Comprehensive audit trail features allow users to track and analyze changes to the security and network environment:
  - New and modified objects are highlighted in the SmartDashboard object tree and in the Rule Base.
  - Session Information Windows display specific changes and provide justification for these actions.
  - Audit logs provide detailed information regarding all changes and can be viewed using SmartView Tracker.
  - The Security Policy Change Summary report summarizes changes made during the current session. It includes detailed before and after comparisons.

How SmartWorkflow Works

This section presents a brief overview of the SmartWorkflow environment and task flow.

SmartWorkflow Environment

SmartWorkflow is integrated into SmartDashboard. In a Multi-Domain Security Management environment, SmartWorkflow works with both the global SmartDashboard and a Domain Management Server SmartDashboard.

The Session Information pane typically appears below the data pane associated with the selected tab, although some tabs may cover it. Changed items are highlighted in the navigation tree and in the data pane.

All SmartWorkflow tasks are available on the toolbar.
**Task Flow**

SmartWorkflow is very flexible, providing options for session management and/or role segregation features.

**Task Flow Using Sessions and Role Segregation**

Using sessions and role segregation together utilizes the full change management functionality incorporated into SmartWorkflow.

1. An administrator opens a new session to modify the security and/or network environment using SmartDashboard.
2. The administrator configures security policy and network settings in SmartDashboard.
3. The administrator submits the completed session for approval.
4. A manager reviews the proposed modifications and either approves the session or returns it to the administrator with a request for repairs to the proposed changes.
5. If a session is returned for repair, the administrator makes the requested changes and resubmits the session for approval.
6. Upon approval, the administrator installs the policy for all approved sessions. All sessions must be approved before you can install a policy.

To configure SmartWorkflow to work with sessions and Role Segregation, refer to Configuring SmartWorkflow (see "Configuring SmartWorkflow Properties" on page 14).

**Task Flow Using Sessions Without Role Segregation**

You can configure SmartWorkflow to work with sessions, but without requiring manager approval before installing the resulting policy. Full tracking and audit trail functionality is available in this scenario.

1. An administrator opens a new session to modify the security and/or network environment using SmartDashboard.
2. The administrator configures security policy and network settings in SmartDashboard.
3. When finished, the administrator submits the completed session and SmartWorkflow automatically approves it.
4. The administrator installs the policy for all approved sessions. All sessions must be approved before you can install a policy.
To configure SmartWorkflow to work with sessions but without Role Segregation, refer to Configuring SmartWorkflow.

**Task Flow Without Using Sessions and Role Segregation**

You can also configure SmartWorkflow to work without explicit sessions and without Role Segregation. Using this option, SmartDashboard functions as if SmartWorkflow is not enabled but an automatic session exists in the background. However, the full SmartView Tracker and audit trail functionality is still available.

1. The administrator modifies the security policy and network configuration settings in SmartDashboard.
2. The administrator installs policies as required without any intermediate steps.
Chapter 2

Working with the SmartWorkflow GUI

In This Chapter

The SmartWorkflow Toolbar 9
The SmartWorkflow Session Management Window 10
The SmartWorkflow Session Information Pane 11

The SmartWorkflow Toolbar

You can perform SmartWorkflow tasks using the SmartWorkflow toolbar or the menu, which appears next to the standard SmartDashboard toolbars. You can freely reposition the toolbar.

The functions of the menu options and toolbar buttons are summarized in the following table:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Forward/Back</td>
<td>Moves chronologically between the different changed objects.</td>
</tr>
<tr>
<td></td>
<td>Show Session Information</td>
<td>Displays or hides the SmartWorkflow Session Information pane.</td>
</tr>
<tr>
<td></td>
<td>Submit for Approval</td>
<td>Opens the Submit Session for Approval window.</td>
</tr>
<tr>
<td></td>
<td>Discard Session Changes</td>
<td>Discards all changes made in the current session.</td>
</tr>
<tr>
<td></td>
<td>Show Change Summary Report</td>
<td>Displays a summary of the changes made in the current session.</td>
</tr>
<tr>
<td></td>
<td>Start New Session</td>
<td>Opens the New Session window. This option is only available when there is no session currently in progress.</td>
</tr>
<tr>
<td></td>
<td>Manage Sessions</td>
<td>Opens the SmartWorkflow Session Management window.</td>
</tr>
<tr>
<td></td>
<td>Highlight Changes</td>
<td>Turns on and off the highlighting of objects changed during a session.</td>
</tr>
<tr>
<td></td>
<td>Online Help</td>
<td>Opens the online help.</td>
</tr>
</tbody>
</table>
### The SmartWorkflow Session Management Window

The **Session Management** window displays all sessions submitted, approved, or in progress, for which a policy has not yet been installed. The Session Management window is not available if sessions are disabled. The following information appears:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in progress</td>
<td>Session is currently in progress.</td>
</tr>
<tr>
<td></td>
<td>Awaiting Approval</td>
<td>Session was submitted for approval.</td>
</tr>
<tr>
<td></td>
<td>Not Approved</td>
<td>The session is not approved and the manager has requested repairs.</td>
</tr>
<tr>
<td></td>
<td>Repaired</td>
<td>Indicates that the original session has been repaired (modified). The <strong>Notes</strong> column displays the session ID for the session in which the repair took place.</td>
</tr>
<tr>
<td></td>
<td>Approved</td>
<td>Indicates that a session has been approved.</td>
</tr>
</tbody>
</table>

- **ID**: Unique session ID assigned to a session.
- **Name**: Session name.
- **Submitted By**: Administrator who submitted a session for approval.
- **Submitted At**: Date and time that a session was submitted for approval.
- **Notes**: Displays the last note associated with a session.
- **Notes History**: All notes associated with a session.

The lower section contains buttons representing tasks that can be performed on the selected session. The following table lists the tasks that are available based on the session status.

<table>
<thead>
<tr>
<th>Task Name</th>
<th>In Progress</th>
<th>Awaiting Approval</th>
<th>Not Approved</th>
<th>Repaired</th>
<th>Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Changes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View Session</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Compare</td>
<td>No</td>
<td>Available when selecting two sessions from the list (as long as one of them is not in progress).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Note</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Approve</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Request Repair</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Repair</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Continue Session in progress</td>
<td>Available upon logon if there is a session in progress.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Help</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Continue Without Session</td>
<td>No</td>
<td>Available if there is no session in progress. Not available for Multi-Domain Security Management Global SmartDashboard.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open New Session</td>
<td>No</td>
<td>Available if no session is in progress.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The SmartWorkflow Session Information Pane

The SmartWorkflow Session Information pane displays detailed and comparative information, consisting of three sections:

- **Session Information** pane: Displays general information about the session, notes that have been added to the session and buttons that enable you to work with the session. You can perform the following actions directly from this pane.
  - Submit the current session for approval.
  - Discard all changes made during the current session.
  - Display the Security Configuration Change Summary Report.
  - Display the audit logs in SmartView Tracker.

- **List of Changes** pane: Displays all rules and objects that have been added, changed or deleted during the current session.

- **Change Details** pane: Displays details and comparative data for the selected item in the List of Changes pane. This pane displays the property name, current value and previous value for changed objects and provides a **Show Changes** button to display details of changes to rules.
Chapter 3

Configuring SmartWorkflow

This section presents the procedures for the initial setup for SmartWorkflow, including the following tasks, which should be performed in sequence:

- Assigning permissions for administrators and managers in the Security Management Server and Multi-Domain Security Management environments. You should define your initial users and assign permissions before enabling SmartWorkflow.
- Enabling the SmartWorkflow Blade globally for each Security Management server or Domain Management Server and choosing whether or not to utilize sessions.
- Starting SmartDashboard for the first time.
- Performing the initial SmartWorkflow configuration.

In This Chapter

Assigning Permissions 12
Enabling the SmartWorkflow Blade 13
Configuring SmartWorkflow Properties 14

Assigning Permissions

In a full change management scenario, with Role Segregation enabled, only managers are authorized to approve sessions, enable or disable SmartWorkflow, and configure SmartWorkflow itself. You can choose to disable Role Segregation.

When working with Multi-Domain Security Management, only Multi-Domain Security Management and Domain Superusers are authorized to approve sessions, enable, disable, and configure SmartWorkflow.

You should always define your initial set of users and assign their permissions before enabling SmartWorkflow. This is necessary to prevent SmartWorkflow from enforcing Role Segregation before you assign manager permissions.

Defining Permissions for Security Management Server

To configure permission profiles for administrators and managers in a Security Management Server environment:

1. In SmartDashboard, select Manage > Permissions Profiles.
2. Select an existing profile or click New to create a new profile.
3. Enter a name for the permission profile.
4. Configure the Allow access via parameter as required for your environment.
5. Enable Read/Write All for both managers and administrators.
6. For Managers only, enable the Manage Administrators option.

Note: We strongly recommend not to enable the Manage Administrators option for ordinary administrators, because this action allows administrators to change the SmartWorkflow configuration or to disable it entirely.

You can disable Role Segregation on the Global Properties > SmartWorkflow page without allowing administrators to configure or disable SmartWorkflow.
Defining Permissions for Multi-Domain Security Management

To configure manager permissions for Multi-Domain Security Management:

1. In the SmartDomain Manager, click **Administrators** on the Selection Bar.
2. In the **Domains per Administrator** pane, double-click an existing user or right-click the **Multi-Domain Security Management** icon and choose **New Administrator**.
3. In the **Edit Administrator** window, select either **Domain Superuser** or **Multi-Domain Security Management Superuser** for managers. Select any other permission for administrators as required.
4. Define other user properties as required.

Enabling the SmartWorkflow Blade

You must enable SmartWorkflow in SmartDashboard for each Security Management server or Domain Management Server before you can begin working with it. After SmartWorkflow is enabled, the SmartWorkflow toolbar and menus are available when you re-open SmartDashboard.

After you enable SmartWorkflow, you have a 45-day trial license.

To enable SmartWorkflow:

1. In SmartDashboard, double-click an **active** Security Management server or Domain Management Server object and select **General Properties**. The Security Management server can be primary or secondary but it must have an IP address identical to the server you are connected to.
2. In the **Software Blades** section, select the **Management** tab and then select **Workflow**. The **SmartWorkflow Configuration Wizard** opens.
3. Select a mode of working with SmartWorkflow.
   - **Use SmartWorkflow for visual change tracking** - Lets you track changes to the policy without sessions. You can install the policy without an approval process.
   - **Use SmartWorkflow to track, review and require approval for changes** - Lets you track changes to the policy with sessions. This enforces policy installation only with approval by a manager. Without approval, the policy cannot be installed.
4. Save the configuration.
To disable SmartWorkflow:
1. In SmartDashboard, double-click a Security Management server or Domain Management Server object and select General Properties.
2. In the Software Blades section, select the Management tab and clear Workflow.
3. Save the configuration.

Configuring SmartWorkflow Properties

You must now configure SmartWorkflow properties in SmartDashboard. In a Multi-Domain Security Management environment, you perform these configuration steps for each Domain Management Server.

To configure SmartWorkflow properties:
1. In SmartDashboard, select Policy > Global Properties.
2. On the Global Properties window, select SmartWorkflow from the navigation tree.

3. Sessions are enabled by default. If you choose NOT to work with sessions, clear the Work with sessions option. In this case, all other options are disabled.

4. Select Administrators can only view their submitted sessions to allow administrators to view only their own sessions. Managers can view all sessions.

5. Role Segregation is enabled by default. If you choose NOT to use Role Segregation, clear the Require session approval option. If you enable Role Segregation, configure the following:
   a) Enable Managers cannot approve their submitted sessions if you do not want to allow managers to approve their own sessions.
   b) Enable Administrators can install unapproved policies using a password in an emergency to grant administrators the ability to install a policy for an unapproved session, in emergency situations, by entering a password. The session remains unapproved after the policy installation. Enter and confirm the emergency password in the designated fields.
Chapter 4

Working with Sessions

When working in SmartDashboard with sessions enabled, you must either open a new session or continue a session in progress in order to modify rules or objects. A session in progress is the last session not yet submitted for approval. You can, however, use SmartDashboard in the read-only mode (no modifications allowed) without opening a session.

Note - There can only be one session in progress at any time. The option to start a new session is not available if a session is in progress.

In This Chapter

Starting a New Session 15
Continuing a Session in Progress 15
Working Without a SmartWorkflow Session 16
Viewing Sessions 16
Submitting Sessions for Approval 17
Discarding Session Changes 17

Starting a New Session

You can only start a new session if there is no session currently in progress.

To start a new session:

1. From the Session Management window, click Open New Session or select Open New Session from the SmartWorkflow menu or toolbar.
2. Enter a unique, descriptive Name for the session.
3. In the Notes area, type a comment or any additional information you may have regarding the session. This field is optional.
4. The new session opens.

Note - If the SmartWorkflow Session Information pane is not visible, click the Show Information Pane icon on the toolbar.

Continuing a Session in Progress

If you close SmartDashboard while working on a SmartWorkflow session, the next time you log in to SmartDashboard, you continue working with the session in progress.

Note - You cannot continue without a session in the Multi-Domain Security Management Global SmartDashboard.

To continue a session in progress:

1. In the Session Management window, click Continue Session in progress. The Session in progress window appears.
2. To add a note, click Add and enter the note text.
3. Click OK. The SmartDashboard login process completes and you can continue working in the session in progress.
Working Without a SmartWorkflow Session

You can open SmartDashboard without a SmartWorkflow session (read/write blocked) to perform session management tasks (approving or disapproving sessions, adding notes to sessions or installing policies).

To work in SmartDashboard without a session temporarily:

1. In the Session Management window, click Continue Without Session and confirm the message.
2. Perform your tasks.

Note - While working without a SmartWorkflow session, you cannot make any changes to objects, rules or any other element.

Viewing Sessions

SmartWorkflow highlights modified objects in the navigation tree and the Rule Base panes. This feature provides a visual road map to identify modified objects. Highlighting is enabled by default.

To enable highlighting, click the icon in the SmartWorkflow toolbar or select Highlight Session Changes from the SmartWorkflow menu. To disable highlighting, repeat this procedure.

Navigation tree objects

Rule Base objects
**Moving Between Changed Rules and Objects**

To scroll through changes made during the current session, click the **Go to Previous Change** or **Go to Next Change** arrow toolbar icons, which are listed in chronological order. The numbers appearing between the arrows, for example 3/4, refer to the currently displayed item out of the total number of items.

**The Session Information Pane**

You can always view details of changes in the Change Information pane. If the Change Information pane is not visible, click the icon in the SmartWorkflow toolbar.

**Submitting Sessions for Approval**

Once you have completed all changes you want to make in the current session, you then submit the session for approval by an authorized manager.

**To submit a session for approval:**

1. Perform one of the following steps:
   - From the SmartWorkflow menu, select **Submit Session for Approval**.
   - Click the **Submit Session for Approval** icon on the SmartWorkflow toolbar.
   - Click **Submit for Approval** in the Session Information pane.
2. If you want to add a note regarding the approval request, enter the text in the designated area.
3. If you want to send a notification regarding the approval request by email:
   a) Select **Send email notification to**.
   b) Enter the email address in the designated field.
   c) If you want to attach the summary report to the email, select **Attach change summary report**.
4. Click **Submit**.
   The session's status changes from **In progress** to **Waiting for approval** (or **Approved** if the Require session approval feature is disabled). If you selected the email notification option, an email message opens in your email client, displaying your note and an attachment containing the Change Summary report (if you selected those options).
   If the Role Segregation feature is disabled, the session is automatically approved and you can install the policy immediately.

**Discarding Session Changes**

You can always undo all changes made during the current SmartWorkflow session.

**To discard all changes made during the current session**, click the toolbar icon or select **Discard Session Changes** from the SmartWorkflow menu. This action reverts SmartDashboard to its state at the beginning of the session.
Chapter 5

Managing and Approving Sessions

This section presents the procedures for reviewing and approving repairs to sessions. If Role Segregation is disabled the approval procedures are not necessary, however the review and audit options are fully functional.

All options for session management and session review are contained in the Session Management window.

In This Chapter

| Reviewing Sessions | 18 |
| Approving Sessions | 21 |
| Requesting Repairs to Sessions | 21 |
| Repairing Sessions | 22 |
| Installing the Security Policy | 22 |

Reviewing Sessions

The following tools are available for reviewing submitted sessions:

**Security Configuration Change Summary Report**

The Security Configuration Change Summary Report presents a comprehensive picture of all changes that were made during the selected session. You can print, save or send an email containing the report. In addition, you can approve or request repairs to the selected session directly from the report window.

The Security Configuration Change Summary Report is divided into several sections, according to the types of changes made. The initial section presents a summary of each changed item with a link to the details. The details include the type of change, who performed the change and when.
To display the Security Configuration Change Summary Report, click Review Changes in the Session Management window.

Viewing a Submitted Session
To view a submitted session, click the View Session button in the Session Management window. You will be viewing the session in Read-only mode.

Comparing Policies
Before approving a session and installing the security policy, it is recommended that you compare the current changes with the currently installed policy. You can compare policies by clicking the Compare Policies button in either the Install Policy window or the Compare Versions button in the Database Revision Control window.

Compare Policies compares the current state, which includes all pending sessions regardless of their status, with the state immediately following the last Policy installation.

To Compare Policies from the Install Policy window:
1. Select Policy > Install.
2. In the Install Policy window, select an Installation Target for comparing the current and previously installed policies.
3. Click Compare Policies. A comparative report is displayed.
Repeat steps two and three for each Installation Target whose policies you want to review.

To compare policies using the Database Revision Control window:

1. Click the Database Revision Control icon on the SmartDashboard toolbar. The Database Revision Control window opens.

2. Select a revision and perform any of the following tasks:
   - To compare the current state with an earlier revision, select any specific revision.
   - To compare two database Revisions with each other, hold down the Control key and select two revisions.

3. Click Compare Versions.

Repeat steps two and three for each report that you want to view.
Comparing Submitted Sessions

You can compare two submitted sessions appearing in the SmartWorkflow Session Management window. You cannot, however, compare a session that has not yet been submitted (in the "in progress" state).

To compare two sessions:
1. In the Session Management window, select two sessions to compare.
2. Click Compare. A comparative report displays.

Approving Sessions

All sessions must be approved before they can be installed on a management server. Typically, managers approve sessions created by administrators. In a Multi-Domain Security Management environment, Multi-Domain Security Management superusers and Domain Superusers can approve sessions. You can also configure SmartWorkflow to automatically approve submitted sessions without approval.

Managers must approve sessions in the order that they were submitted. For example, if session 1 and session 2 are both awaiting approval, session 1 must be approved before you can approve session 2. This restriction also applies to sessions that have been repaired.

To approve a session:
1. In the Session Management window, click Approve.
2. If you choose to add comments, enter text in the Notes field.
3. If you choose to send a notification by email:
   a) Select Send email notification to.
   b) Enter the email address in the designated field.
   c) If you wish to attach the summary report to the email, select Attach change summary report.
4. Click Approve. The session status changes to Approved.

If you selected the email notification option, an email message opens in your email client containing any notes you entered and, optionally, an attachment containing the change summary report.

Requesting Repairs to Sessions

Managers can request modifications (repairs) be made to a submitted session before approval. Essentially, this means that the manager disapproves the session and returns it to the submitting administrator for action.

To request that a repair be made to a session:
1. In the Session Management window, click Request Repair.
2. Enter a Note describing the repairs to be made to the Note field.
3. If you choose to send a notification by email:
   a) Select Send email notification to.
   b) Enter the email address in the designated field.
   c) If you wish to attach the summary report to the email, select Attach change summary report.
4. Click Add Note.
5. Click Request Repair.

The session status changes from "Awaiting Approval" to Waiting for Repair”. If you selected the email notification option, an email message opens in your email client displaying the note you inserted and, optionally, an attachment containing the change summary report.
Repairing Sessions

When a session is returned for repair, the submitting administrator makes the requested repairs in SmartDashboard and then resubmits the session for approval.

The repair process actually creates a new session, with its own ID, to record the actual change. The original session status is updated to **Repaired** and a note is inserted stating "Repaired by session <session ID>".

For example, if the submitting administrator receives a request to repair session 2, named "Adding new network objects", he makes the requested repairs. These repairs create a new session 5 named "Repairing Session 2". The original session (ID 2) is updated to the **Repaired** status and the Notes column in the **Session Management** window indicates that it was "Repaired by Session 5".

**To repair a session:**
1. In the **Session Management** window, click **Repair**.
2. Add a **Note** describing the repairs made in the **Note** field.
3. If you choose to send a notification by email:
   a) Select the **Send email notification to**.
   b) Enter the email address in the designated field.
   c) If you want to attach the summary report to the email, select **Attach change summary report**.
4. Click **Add Note**.
5. Click **Repair**.

   The original session status is updated to Repaired and the "Repair" session status is updated to In Process. If you selected the email notification option, an email message opens in your email client displaying the note you inserted and optionally, an attachment containing the change summary report.
6. Later on, submit the repaired session for approval as usual.

   If you selected the email notification option, an email message opens in your email application displaying the note you inserted and optionally, an attachment containing the change summary report.

Installing the Security Policy

After all sessions have been approved, install the security policy in SmartDashboard according to normal procedures.

When you install a policy, you are presented with the option to retain session information for those sessions included in the policy install. By default, session information is deleted from the database once the policy is installed. Actions performed in deleted sessions are always available for audit using SmartView Tracker. Refer to Auditing Changes with SmartView Tracker (on page 23).
Chapter 6

Auditing Changes with SmartView Tracker

Actions performed using SmartWorkflow are recorded in the audit logs and can be viewed using SmartView Tracker. Actions are logged in real time when saved in SmartDashboard. You can view the logs at any time, whether or not the session has been approved or the policy has been installed.

In This Chapter

Viewing Session Activity in SmartView Tracker 23
Auditing Objects and Rules in SmartView Tracker 24
Creating Custom SmartView Tracker Queries 24

Viewing Session Activity in SmartView Tracker

To view session activity in SmartView Tracker:

1. In the Session Management window, select a session and then click View Session. An instance of SmartDashboard opens showing the selected session.

2. In the Session Information pane, click Show Audit Logs. SmartView Tracker opens, displaying the log entries for the selected session.

3. To view details of a log entry, double-click it. The Record Details window opens. Click More Information to display all of the log information for this entry.
Auditing Objects and Rules in SmartView Tracker

To view changes to objects or rules:

- Right-click on an object in SmartDashboard or an object/rule in the List of Changes that appears in the Session Information pane and select Audit Trail. SmartView Tracker opens with all audit logs for the specific object shown in the Records pane.

To see the changes made to a specific rule:

- Right-click on the rule number. You will see all changes to the specific rule package.

The records include the following categories of information: the date and time when changes were made, the application used to make the changes, the type of operation performed, the type and specific name of the object, the changes made, and the administrator who performed the changes.

Creating Custom SmartView Tracker Queries

You can create your own queries and filters with SmartView Tracker to audit changes to your security and network environment. Feel free to experiment using all of the advanced features available with this powerful tool. For detailed information regarding the use of SmartView tracker, refer to the SmartView Tracker online help.

To open SmartView Tracker directly from SmartDashboard, select SmartView Tracker from the Window menu.
Index

A
Approving Sessions • 21
Assigning Permissions • 12
Auditing Changes with SmartView Tracker • 23
Auditing Objects and Rules in SmartView Tracker • 24

C
Comparing Policies • 19
Comparing Submitted Sessions • 21
Configuring SmartWorkflow • 12
Configuring SmartWorkflow Properties • 14
Continuing a Session in Progress • 15
Creating Custom SmartView Tracker Queries • 24

D
Defining Permissions for Multi-Domain Security Management • 13
Defining Permissions for Security Management Server • 12
Discarding Session Changes • 17

E
Enabling the SmartWorkflow Blade • 13

H
How SmartWorkflow Works • 6

I
Important Information • 3
Installing the Security Policy • 22

K
Key Features • 6

M
Managing and Approving Sessions • 18
Moving Between Changed Rules and Objects • 17

R
Repairing Sessions • 22
Requesting Repairs to Sessions • 21
Reviewing Sessions • 18

S
Security Configuration Change Summary Report • 18
SmartWorkflow Environment • 6
SmartWorkflow Overview • 5
Starting a New Session • 15
Submitting Sessions for Approval • 17

T
Task Flow • 7
Terms and Concepts • 5

The Session Information Pane • 17
The SmartWorkflow Session Information Pane • 11
The SmartWorkflow Session Management Window • 10
The SmartWorkflow Toolbar • 9

V
Viewing a Submitted Session • 19
Viewing Session Activity in SmartView Tracker • 23
Viewing Sessions • 16

W
Why is Change Management Important? • 5
Working with Sessions • 15
Working with the SmartWorkflow GUI • 9
Working Without a SmartWorkflow Session • 16