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=22926
For additional technical information, visit the Check Point Support Center
(http://supportcenter.checkpoint.com).
For more about this release, see the R76 home page

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 January 2013</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 R76 Administration Guide).
# Contents

Important Information ................................................................. 3  
SmartWorkflow Overview .................................................................. 5  
  Why is Change Management Important? ..................................... 5  
  Terms and Concepts .................................................................... 5  
  Key Features ............................................................................... 6  
  How SmartWorkflow Works ....................................................... 6  
    SmartWorkflow Environment ..................................................... 6  
    Task Flow ................................................................................. 6  
Working with the SmartWorkflow GUI ........................................ 8  
  SmartWorkflow Session Information ......................................... 8  
  SmartWorkflow Toolbar ................................................................ 8  
  SmartWorkflow Session Management Window ......................... 9  
Configuring SmartWorkflow ........................................................ 11  
  Assigning Permissions .............................................................. 11  
    Defining Permissions for Security Management Server .......... 11  
    Defining Permissions for Multi-Domain Security Management . 11  
  Enabling the SmartWorkflow Blade .......................................... 12  
  Configuring SmartWorkflow Properties ................................... 12  
Working with Sessions ................................................................. 14  
  Starting a New Session ............................................................. 14  
  Continuing a Session in Progress .............................................. 14  
  Working Without a SmartWorkflow Session ............................ 15  
  Viewing Sessions ....................................................................... 15  
  Submitting Sessions for Approval ........................................... 15  
  Discarding Session Changes .................................................... 15  
Managing and Approving Sessions ............................................... 16  
  Security Configuration Change Summary Report ..................... 16  
  Viewing a Submitted Session .................................................... 17  
  Comparing Policies ................................................................... 18  
  Comparing Submitted Sessions ................................................ 18  
  Approving Sessions ................................................................... 18  
  Requesting Repairs to Sessions ............................................... 19  
  Repairing Sessions ................................................................... 19  
  Installing the Security Policy .................................................... 20  
Auditing Changes with SmartView Tracker .................................. 21  
  Viewing Session Activity in SmartView Tracker ...................... 21  
  Auditing Objects and Rules in SmartView Tracker ................... 21  
  Creating Custom SmartView Tracker Queries ......................... 21  
Index ............................................................................................. 23
Chapter 1

SmartWorkflow Overview

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

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.

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 in SmartDashboard and works with SmartView Tracker, SmartReporter, and other consoles. In a Multi-Domain Security Management environment, SmartWorkflow works with the global SmartDashboard and a Domain Management Server SmartDashboard.

To see SmartWorkflow Session Information:

Open the SmartWorkflow tab in the bottom pane of the Software Blade tab.

Alternatively, you can click the Launch Menu button on the main SmartDashboard toolbar > SmartWorkflow > Show SmartWorkflow Pane.

**Task Flow**

SmartWorkflow is flexible, with options for session management and role segregation features. You configure if SmartWorkflow works with sessions only, sessions and roles, without sessions or roles.
Task Flow for Sessions and Role Segregation

Sessions and role segregation use the full change management functionality in SmartWorkflow.

1. A SmartWorkflow administrator opens a new session to modify the security and network environment.
2. The administrator configures the security policy and network settings.
3. The administrator submits the completed session for approval.
4. A manager reviews the proposed modifications and 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 changes and resubmits the session for approval.
6. On approval, the administrator installs the policy for all approved sessions.

All sessions must be approved before you can install a policy.

Task Flow Sessions Without Role Segregation

You can configure SmartWorkflow to work with sessions, without requiring manager approval before policy install. Full tracking and auditing is available.

1. The administrator opens a new session, and makes the changes.
2. The administrator submits the session.
3. SmartWorkflow automatically approves it.
4. The administrator installs the policy.

Task Flow Without Sessions or Role Segregation

You can 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 is in the background. SmartView Tracker and audit trail are still available.

1. The administrator changes the security policy and network configuration settings in SmartDashboard.
2. The administrator installs policies.
Chapter 2

Working with the SmartWorkflow GUI

In This Chapter

- SmartWorkflow Session Information 8
- SmartWorkflow Toolbar 8
- SmartWorkflow Session Management Window 9

SmartWorkflow Session Information

When you open the SmartWorkflow tab, you see **SmartWorkflow Session Information**. It shows detailed and comparative information:

- **List of Changes**: Rules and objects added, changed or deleted during the session.
- **Change Details**: Data for the selected item in the List of Changes: property name, newest value and last value for changed objects, rule changes (click **Show Changes**).

SmartWorkflow Toolbar

The SmartWorkflow Session Information toolbar shows the available commands.

The options you see depend on the SmartWorkflow mode that has been configured:

- **Track changes without sessions** - When SmartWorkflow was enabled, the **Use SmartWorkflow for visual change tracking** option was selected. This allows policy installation without approval.
- **Track changes with sessions** - When SmartWorkflow was enabled, the **Use SmartWorkflow to track, review, and require approval for changes** option was selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Visible in Track Changes Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit for Approval</td>
<td>Opens the <strong>Submit Session</strong> window.</td>
<td>With sessions</td>
</tr>
<tr>
<td>Discard Changes</td>
<td>Deletes all changes made in the current session.</td>
<td>With sessions</td>
</tr>
</tbody>
</table>
Working with the SmartWorkflow GUI

Option | Description | Visible in Track Changes Mode
--- | --- | ---
Show Report | Shows a summary of the changes made in the current session. | With sessions
Show Audit Logs | Opens SmartView Tracker, to the Records with Session predefined query. | Without sessions
Manage Sessions | Opens the SmartWorkflow Session Management window. | With sessions
Highlight Changes | Turns on and off the highlighting of objects changed during a session. | Without sessions
Settings | Opens Global Properties > SmartWorkflow. | Without sessions

The main SmartDashboard toolbar also has buttons that let you move chronologically between the different objects that have been changed or added.

All of the options on the toolbar can also be accessed from the SmartWorkflow menu (Launch Menu > SmartWorkflow).

**SmartWorkflow Session Management Window**

The Session Management window displays all sessions submitted, approved, or in progress, for which a policy is not yet installed. The Session Management window is not available if sessions are disabled.

**To see the session status:**
1. Click Manage Sessions in the SmartWorkflow toolbar.
2. Place the mouse pointer on the icons in the Status column to see the session status values.

**Session status:**

<table>
<thead>
<tr>
<th>Session Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Progress</td>
<td>Session is in progress.</td>
</tr>
<tr>
<td>Waiting for Approval</td>
<td>Session was submitted for approval.</td>
</tr>
<tr>
<td>Not Approved</td>
<td>Session is not approved and the manager requested repairs.</td>
</tr>
<tr>
<td>Repaired</td>
<td>Session was changed. It must be submitted for approval again.</td>
</tr>
<tr>
<td>Approved</td>
<td>Session has approval.</td>
</tr>
</tbody>
</table>

Other data:
- **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**: Last note associated with a session.
- **Notes History**: All notes associated with a session.

The action buttons are available for the selected session, if it is in a certain state. This table shows when the buttons are available.
<table>
<thead>
<tr>
<th>Action</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>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>View Session</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Compare</td>
<td></td>
<td></td>
<td>Available if two sessions are selected, and they are both in one of these states.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Note</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Repair</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repair</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Continue Session in progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continue Without Session</td>
<td></td>
<td></td>
<td>Available if there is no session In Progress. Not available for Multi-Domain Security Management Global SmartDashboard.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open New Session</td>
<td></td>
<td></td>
<td>Available if no session is in progress.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3

Configuring SmartWorkflow

In This Chapter

Assigning Permissions 11
Enabling the SmartWorkflow Blade 12
Configuring SmartWorkflow Properties 12

Before you can use SmartWorkflow, you set it up. You assign administrators and managers, decide on deployment mode, enable it as a Software Blade, and configure its properties for your environment.

Assigning Permissions

In a full change management scenario with Role Segregation, only managers are authorized to:

- approve sessions
- enable or disable SmartWorkflow
- configure SmartWorkflow properties

In Multi-Domain Security Management, only Multi-Domain Security Management and Domain Superusers have these permissions.

Define users and assign their permissions before you enable SmartWorkflow. This is necessary to prevent SmartWorkflow from enforcing Role Segregation before you assign manager permissions.

Defining Permissions for Security Management Server

When you configure permissions, make sure to give Manager permissions to people who should actually have auditing authority. It is best if Managers are not Administrators.

To configure permission profiles 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. Select the Allow access via as required for your environment.
5. Select Read/Write All for managers and administrators.
6. For Managers only, select Manage Administrators.

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 Domain Superuser or Multi-Domain Security Management Superuser for managers.
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 to work with it. After SmartWorkflow is enabled, SmartWorkflow is 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

Configure SmartWorkflow properties in SmartDashboard. In a Multi-Domain Security Management environment, do these configuration steps for each Domain Management Server.

To configure SmartWorkflow properties:
1. In SmartDashboard, click Edit Global Properties.
2. In the **Global Properties** window, open **SmartWorkflow**.

   ![SmartWorkflow Administration Guide R76](image)

   - To disable highlighting changes made in sessions, clear **Highlight changes**.
   - To work without sessions, clear **Work with sessions**.
   - To work without role segregation, clear **Require session approval**.

3. Select **Administrators can only view their submitted sessions** to let administrators view only their own sessions. Managers can view all sessions.

4. If you enable role segregation:
   a) To make sure managers cannot approve their own sessions, select **Managers cannot approve their submitted sessions**.
   b) To let administrators install policy if the manager is not available and it must be done, select **Administrators can install unapproved policies using a password in an emergency**. Enter the emergency password.

   The session remains unapproved after the policy installation. Enter and confirm the emergency password in the designated fields.
Chapter 4

Working with Sessions

In This Chapter
- Starting a New Session 14
- Continuing a Session in Progress 14
- Working Without a SmartWorkflow Session 15
- Viewing Sessions 15
- Submitting Sessions for Approval 15
- Discarding Session Changes 15

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.

### 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**.
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 (such as 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. Do 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 changed objects in the Network Objects tree and rule bases.

To enable highlighting:
1. In the SmartWorkflow tab, click Settings.
   Global Properties window > SmartWorkflow opens.
2. Select Highlight Session Changes.

After you make the first changes, the top of SmartDashboard shows Previous and Next buttons. You can navigate easily to see the changes you made.

Submitting Sessions for Approval

When you complete all the changes you want to make in a session, submit the session for approval by an authorized manager.

To submit a session for approval:
1. In SmartWorkflow Session Information, click Submit for Approval.
2. Enter a note to the manager.
   Optional: click Send email notification and enter an email address. This could be a way to get the manager's attention faster, or acknowledgment to someone else that the task is done.
3. Click Submit.
   The session 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, the email message opens in your email client.
   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 changes made during a session:
Click Discard Changes. This action reverts SmartDashboard to its state at the beginning of the session.
Chapter 5

Managing and Approving Sessions

In This Chapter

Security Configuration Change Summary Report 16
Viewing a Submitted Session 17
Comparing Policies 17
Comparing Submitted Sessions 18
Approving Sessions 18
Requesting Repairs to Sessions 19
Repairing Sessions 19
Installing the Security Policy 19

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.

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 you install the security policy, compare the changes with the installed policy. You can compare policies from the Install Policy window or 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 Install Policy:**
1. In the Install Policy window, select one Installation Target.
2. Click Compare Policies.
   A comparative report opens. Compare the current session policy with all the targets you want to review.

**To compare policies from Database Revision Control:**
1. In the Database Revision Control window:
   - To compare the current state with an earlier revision, select one revision.
   - To compare two database Revisions with each other, hold down the Control key and select two revisions.
2. Click Action > Compare Policies.

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 is shown.

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, you can install the security policy in SmartDashboard.

To install the security policy:

1. In the Sessions Management window, select **Continue without a session**.
   
   You enter SmartDashboard and most options are read/write blocked except for Install Policy and SmartWorkflow session management.

2. Click **Install Policy**.

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 21).
Chapter 6

Auditing Changes with SmartView Tracker

In This Chapter

- Viewing Session Activity in SmartView Tracker 21
- Auditing Objects and Rules in SmartView Tracker 21
- Creating Custom SmartView Tracker Queries 21

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.

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

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 • 18
Assigning Permissions • 11
Auditing Changes with SmartView Tracker • 21
Auditing Objects and Rules in SmartView Tracker • 21

C
Comparing Policies • 18
Comparing Submitted Sessions • 18
Configuring SmartWorkflow • 11
Configuring SmartWorkflow Properties • 12
Continuing a Session in Progress • 14
Creating Custom SmartView Tracker Queries • 21

D
Defining Permissions for Multi-Domain Security Management • 11
Defining Permissions for Security Management Server • 11
Discarding Session Changes • 15

E
Enabling the SmartWorkflow Blade • 12

H
How SmartWorkflow Works • 6

I
Important Information • 3
Installing the Security Policy • 20

K
Key Features • 6

M
Managing and Approving Sessions • 16

R
Repairing Sessions • 19
Requesting Repairs to Sessions • 19

S
Security Configuration Change Summary Report • 16
SmartWorkflow Environment • 6
SmartWorkflow Overview • 5
SmartWorkflow Session Information • 8
SmartWorkflow Session Management Window • 9
SmartWorkflow Toolbar • 8
Starting a New Session • 14
Submitting Sessions for Approval • 15

T
Task Flow • 6

Terms and Concepts • 5

V
Viewing a Submitted Session • 17
Viewing Session Activity in SmartView Tracker • 21
Viewing Sessions • 15

W
Why is Change Management Important? • 5
Working with Sessions • 14
Working with the SmartWorkflow GUI • 8
Working Without a SmartWorkflow Session • 15