

CHAPTER 3

CHECK POINT SECURITY ADMINISTRATION

YOU DESERVE THE BEST SECURITY

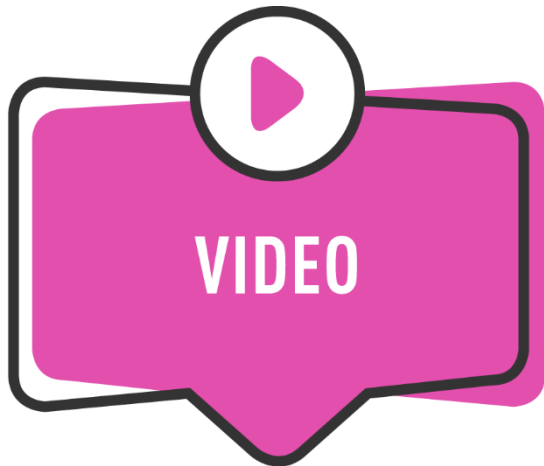
Learning Objectives

- Create SmartConsole objects that correspond to the organization's topology for use in policies and rules.
- Establish secure internal communication (SIC).
- Create secondary administrator accounts for backup and task-based management.



SmartConsole Administration Overview

- SmartConsole database requires initial setup, including:
 - Configure SmartConsole objects to represent network topology.
 - Create secondary SmartConsole administrator accounts for backup and task-based delegation.
- Security Administrators use SmartConsole to:
 - Manage licenses and service contracts.
 - Create and manage security policies.



For further learning, watch the following video:

Understanding SmartConsole

This and other videos are accessed from the online *Quantum Security Management R81.20 Administration Guide*.

SmartConsole Objects

- Objects represent topology components.

Physical Components

- Security Gateways and Management Servers
- Domain Name Servers
- Demilitarized zones
- Users



Logical Components

- Check Point and third-party services
- IP address ranges
- Third-party applications

A network topology is used to document the physical and logical structure of a network. The topology shows how various network components interconnect and how data flows.

Purpose of Objects

- Objects are used in security policies and rules to **define** and **control** network operations/

No.	Name	Source	Destination
▼ Security Gateways Access (1-2)			
1	Administrator Access to Gateways	 Admins	 Corporate-GW

Corporate-GW is an object in the Destination that represents a Security Gateway.

Admins is an object in the Source that represents administrator users in an internal group.



Some objects such as Check Point services are available by default when a site is deployed.

Deployment-specific objects such as Gateways and Management Servers must be created before they can be used.

Types of Objects

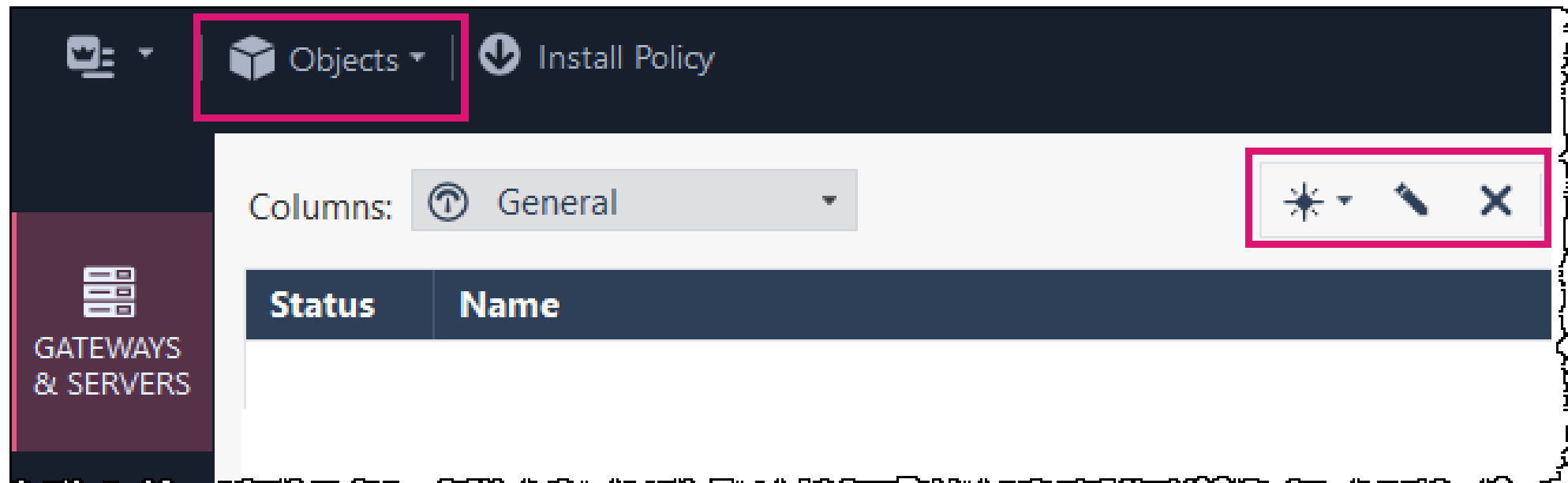
Category	Description
Network Objects	Gateways, Management Servers, hosts, networks, address ranges, dynamic objects, security zones
Services	Services, Service groups
Custom Applications/Sites	Applications, Categories, Mobile applications
VPN Communities	Site to Site or Remote Access communities
Users	Users, user groups, and user templates

Types of Objects (Continued)

Category	Description
Data Types	International Bank Account Number - IBAN, HIPAA - Medical Record Number - MRN, Source Code
Servers	Trusted Certificate Authorities, RADIUS, TACACS
Time Objects	Time, Time group
UserCheck Interactions	Message windows: Ask, Cancel, Certificate Template, Inform, and Drop
Limit	Download and upload bandwidth

Before creating objects, analyze the network topology and identify the types of objects you need.

Object Management



Exploring Existing Objects

The image shows a screenshot of the Check Point management console. On the left, a sidebar contains the text "GATEWAYS & SERVERS". The main menu bar includes "Objects" and "Install Policy". A dropdown menu is open under "Objects", listing options: "New Network...", "New Host...", "New Network Group...", "Cloud", "More object types", and "Object Explorer". A pink arrow points to the "Object Explorer" option. To the right, the "Object Explorer" window is open, displaying a tree view of object categories and a table of objects.

Object Explorer

* All -

New... X Actions Search...

Categories

- Network Objects (64)
- Services (524)
- Applications/Catego... (8322)
- VPN Communities (4)
- Data Types (62)
- Users/Identities (27)
- Servers (4)
- Time Objects (4)
- UserCheck Interactions (15)
- Limit (4)
- Updatable Objects (4)

Name	Modifier	Comments
#hashtags	System	
.corp.com	admin	
050 Plus	System	
1000keyboards	System	
1000memories	System	
100bao	System	
101 Okey Domino hakkarim.net	System	
115	System	
115-audio	System	
115-download	System	
115-upload	System	
115-video	System	

9824 items

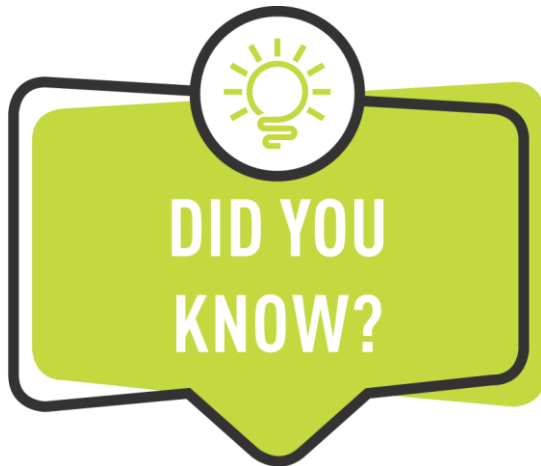
Categories

The screenshot shows the 'Object Explorer' window. On the left, a tree view shows the following categories:

- Categories
 - Network Objects (64)
 - Services (524)
 - Applications/Catego... (8322)
 - VPN Communities (4)
 - Data Types (62)
 - Users/Identities (27)
 - Servers (4)
 - Time Objects (4)

At the bottom left of the window, it says '524 items'. The main pane on the right displays a table with the following columns: Name, Port, Program Number, and ICMP Type. The table contains the following data:

Name	Port	Program Number	ICMP Type
CP_SmartPortal	4433		
CP_SSL_Network_...	444		
CPD	18191		
CPD_amon	18192		
CPM	19009		
CPMI	18190		
CrackDown	4444		
CreativePartnerClnt	455		



Check Point services are software programs that provide specific functionality. For example, the Check Point Management (CPM) service handles requests from SmartConsole and writes information to the Management database.

Check Point services are sometimes referred to as applications, daemons, and programs. See [sk97638 - Check Point Processes and Daemons](#).

Available Actions

The screenshot shows the 'Object Explorer' window with a tree view on the left and a table of objects on the right. The 'Services' category is selected, showing 524 items. The table lists various services, with 'CPM' selected. A context menu is open over 'CPM', listing actions such as View..., Edit..., Clone..., Delete, Where Used..., Copy To Clipboard, and Copy As Image.

Name	Port	Program Number	ICMP T
CP_SmartPortal	4433		
CP_SSL_Network_...	444		
CPD			
CPD_amon			
CPM			
CPMI			
CrackDown			
CreativePartnerClnt			

Create SmartConsole Objects

- Two common methods to create SmartConsole objects include:
 - Object menu on the Global toolbar
 - New menu on the Gateways & Servers toolbar
- Workflow:
 1. Specify General Properties.
 2. Initiate trusted communication.
 3. Activate available Software Blades.

Do not create two objects with the same name. A validation error occurs when you try to publish the session.

General Properties

Property	Description
Name	Enter a unique name. The name cannot include spaces or special characters except the underscore character.
IP Address	Enter an IPv6 or an IPv4 address or both (if applicable).
Dynamic IP Address	Select to assign a dynamic IP address by a dynamic host configuration protocol (DHCP) server. Only applies to Small Office Appliances.
Platform	Select the appliance model or server type from the list.
Version	Select the software release; for example, R81.20.
Operating System	Select the operating system; for example, Gaia.
Comment	Enter a description for informational purposes.

Secure Trusted Communication

Property	Description
Secure Internal Communication	Define a one-time password to initialize SIC. The password must match the password defined when the device was installed.
Trusted Communication Initiation	Click Initialize to test the SIC status. <ul style="list-style-type: none">• If the SIC status is Unknown, there is no connection between the Gateway and Management Server.• If the SIC status is No Communication, an error message appears.

Software Blades (Features)

Blade Category	Description
Network Security (Gateway)	Includes: <ul style="list-style-type: none">• Access Control• Advanced Networking• Infinity Services
Threat Prevention (Gateway)	Includes: <ul style="list-style-type: none">• Autonomous Threat Prevention• Custom Threat Prevention
Management (Management Server)	Includes: <ul style="list-style-type: none">• Network Policy Management• Endpoint Policy Management• Logging & Status• User Directory• Provisioning• Compliance• SmartEvent

Create Security Gateway Object

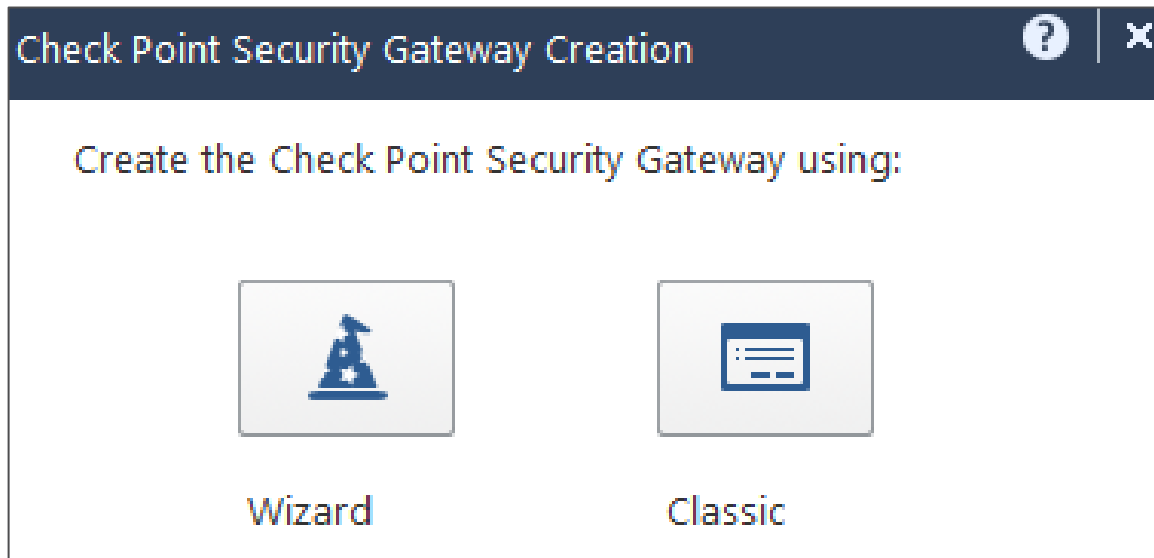
A screenshot of the Check Point management console interface. The 'Objects' menu is open, showing options like 'New Network...', 'New Host...', and 'New Gateway...'. A pink arrow points to the 'Objects' menu. The 'New Gateway...' option is highlighted, and a sub-menu is visible with options like 'New Network...', 'New Host...', 'Group', 'Address Range', and 'New Security Zone...'. The background shows a table of objects with columns for Name, IP, Version, and Active Bl.

Name	IP	Version	Active Bl
BranchOffice	198.51.100.7	R81.20	
Remote-5-gw	192.0.26.1	R81	
RemoteBranchGw	198.51.100.120	R80.40	

A screenshot of the Check Point management console interface showing the 'New Gateway...' sub-menu. A pink arrow points to the 'New menu'. The sub-menu options include 'Gateway...', 'Cluster', 'VSX', and 'More'. The background shows a table of objects with columns for Status, Name, IP, and Version.

Status	Name	IP	Version
✓	BranchOffice	198.51.100.7	R81.20
✓	Corporate-Cluster	17.23.5.1	R81.20
-	Corporate-Cluster-member-A	17.23.5.2	R81.20
-	Corporate-Cluster-member-B	17.23.5.3	R81.20

Gateway Creation Mode - Gateways Only



- Wizard - Lets you quickly create the object with basic properties.
- Classic - Opens a Properties window for manual configuration.

Check Point Gateway Installation Wizard

Check Point Gateway Installation Wizard

General Properties
Specify the Gateway name, platform and IP address.

General Properties

- Trusted Communication
- Blade Activation
- End

Gateway name:

Gateway platform:


Gateway IP address:


Static IP address:

IPv4:

IPv6:

Dynamic IP address (e.g. assigned by DHCP server)





Follow the
onscreen
instructions.

Classic Mode - Manual Configuration

Check Point Gateway

- General Properties
- Network Management
- NAT
 - HTTPS Inspection
 - HTTP/HTTPS Proxy
- ICAP Server
- Platform Portal
- Mail Transfer Agent
- Logs
 - Fetch Policy
 - Optimizations
 - Hit Count
- Other

Machine

Name: Color:

IPv4 Address: Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication:

Platform

Hardware: Version: OS:

Network Security (1) Threat Prevention (Custom) Management (0)

Create Check Point Host Object

The screenshot shows the 'Check Point Host' configuration window. On the left is a navigation pane with 'General Properties' selected. The main area is divided into 'Machine' and 'Platform' sections. The 'Machine' section includes fields for Name, IPv4 Address, IPv6 Address, and Comment. The 'Platform' section includes fields for Hardware, Version, and OS. At the bottom, there are tabs for 'Network Security (0)', 'Threat Prevention (Custom)', and 'Management (0)'.

Machine

Name: Color: ■ Black ▾

IPv4 Address: Resolve from Name Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Uninitialized Communication...

Platform

Hardware: Open server ▾ Version: R81.20 ▾ OS: Gaia ▾ Get

Network Security (0) Threat Prevention (Custom) Management (0)

New
Check
Point Host

Edit Objects

The screenshot shows the Check Point management console interface. The 'Objects' menu is highlighted in the top navigation bar. A table of network objects is displayed, with columns for Status, Name, IP, Version, Active Blades, Hardware, CPU Usage, Recommended Updates, and Recommended. A context menu is open over the 'Corporate-GW' object, showing options like Scripts, Actions, Monitor, View..., Edit..., Clone..., Delete, and Where Used... The 'Edit...' option is highlighted in blue. A red arrow points to the 'Edit...' option with the text 'Right-click or double-click'.

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommen.
✓	BranchOffice	198.51.100.7	R81.20	[Icons]	3000 Appliances	9%	2	
✓	Corporate-Cluster	17.23.5.1	R81.20	[Icons]	26000 Appliances	11%	3	
-	Corporate-Cluster-member-A	17.23.5.2	R81.20	[Icons]	26000 Appliances			
-	Corporate-Cluster-member-B	17.23.5.3	R81.20	[Icons]	26000 Appliances			
✓	Corporate-GW	192.0.2.100	R81.20	[Icons]	23000 Appliances	24%	2	
✓	BranchGw	192.0.2.100	R81.10	[Icons]	5000 Appliances	17%	1	
✓	CenterGw	192.16.26.100	R81.20	[Icons]	23000 Appliances	9%	2	
✓	BranchGw	192.0.2.200	R81	[Icons]	15000 Appliances	18%	3	
✓	BranchGw	10.0.168.103	R81.20	[Icons]	Open server	23%	2	N/A
✓	BranchGw	192.16.26.7	R81.20	[Icons]	23000 Appliances	14%	2	
✓	BranchGw	192.0.22.1	R80.40	[Icons]	1590 Appliances	11%	2	
✓	BranchGw	192.0.23.1	R80.40	[Icons]	1550 Appliances	4%	3	
✓	BranchGw	192.0.24.1	R80.40	[Icons]	5000 Appliances	6%	1	
✓	BranchGw	192.0.25.1	R80.40	[Icons]	5000 Appliances	24%	2	
✓	BranchGw	192.0.26.1	R81	[Icons]	5000 Appliances	16%	2	
✓	RemoteBranchGw	198.51.100.120	R80.40	[Icons]	Open server	9%	2	
✓	ThreatEmulationDevice	192.0.111.13	R81	[Icons]	TE Appliances	4%	2	


™

SMARTCONSOLE ADMINISTRATORS AND PERMISSIONS

CPCConfig Administrator

The screenshot displays the 'Administrator' configuration window for a user named 'admin'. The interface includes a search, help, and close icon in the top right corner. Below the user name, there is a prompt to 'Enter Object Comment'. A left-hand navigation pane shows 'General' as the active tab, with 'Additional Info' below it. The main configuration area is divided into three sections: 'Authentication', 'Permissions', and 'Expiration'. Under 'Authentication', the 'Authentication Method' is set to 'OS Password'. The 'Certificate Information' section shows a 'Certificate is not defined' status with a 'Create' button. Under 'Permissions', the 'Permission Profile' is set to 'Super User'. Under 'Expiration', the 'Expire At' option is selected with a date of '31-Dec-30'.

Administrator

 **admin**
Enter Object Comment

«

General

Additional Info



Authentication

Authentication Method: OS Password

Certificate Information:


Certificate is not defined

Permissions

Permission Profile:  Super User 

Expiration

Never

Expire At: 31-Dec-30 

- Created when the Primary Security Management Server is configured.
- Assigned Super User Permissions.

Additional Administrators

- Created for task-based delegation, including:
 - Auditing
 - Session management
 - System monitoring and logging

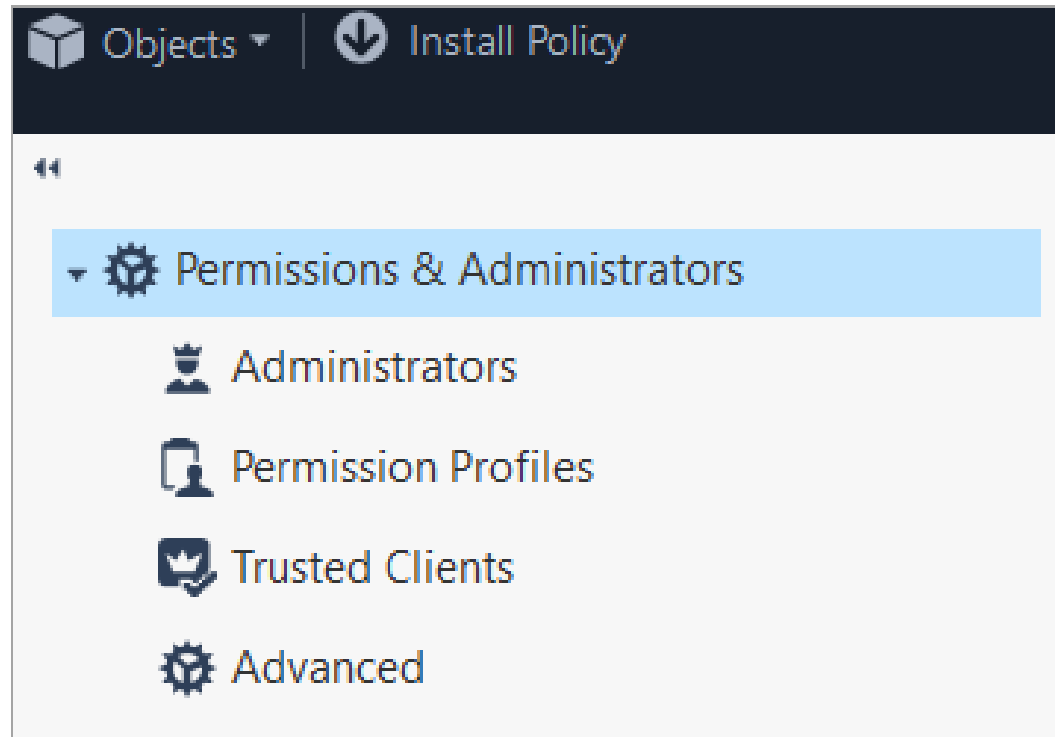


Permission Profiles

Property	Description
Super User	Full Read/Write permissions, including management of administrator and sessions.
Read Write All	Full Read and Write permissions.
Read Only All	Full Read Permissions. No Write permissions.

Predefined, default permission profiles cannot be edited or deleted but can be cloned. The clone can be edited and deleted.


Permissions and Administrator Management



From Manage & Settings view.

Create Administrator Account

New Administrator

 * Enter Object Name
Enter Object Comment

General
Additional Info


Authentication

Authentication Method: Check Point Password

Password is not defined * Set New Password...


Certificate Information:
 Certificate is not defined Create

Permissions

Permission Profile: * No item selected. 

Expiration

Never

Expire At: 03-Feb-25 

From Manage & Settings view.

General Account Properties

Property	Description
Name	Unique name for the administrator (case-sensitive).
Expiration Date	Specific date or Never. After account expiration, the administrator cannot log in to SmartConsole (or SmartConsole clients such as SmartEvent).
Profile	Predefined set of permissions assigned to individual administrators. Tip: To add a profile while creating the new account, click New.
Authentication Method	How account is authenticated; for example: <ul style="list-style-type: none">• SecurID - Use number displayed on the Security Dynamics SecurID card.• Check Point Password - Use Gateway internal password.• OS Password - Use System Management Server operating server (Gaia) password.• Identity Provider Administrator Group - Use SAML authentication (R81.20 and higher).• RADIUS - Use RADIUS server.• TACACS - Forward to TACACS server for authentication.• API - Generate an API key to authenticate to the management API.• Undefined – No authentication method configured.



Users with an undefined authentication method can not log in to SmartConsole.

Access is denied or authentication is based on a certificate as defined in the Admin Certificates tab.

Creating Permission Profiles

New Profile

Enter Object Name

Enter Object Comment

Overview

Gateways

Access Control

Threat Prevention

Others

Monitoring and Logging

Events and Reports

Management

Endpoint

Permissions

Read/Write All

Auditor (Read Only All)

Customized

Add Tag

OK Cancel

See steps in Student Guide.



™

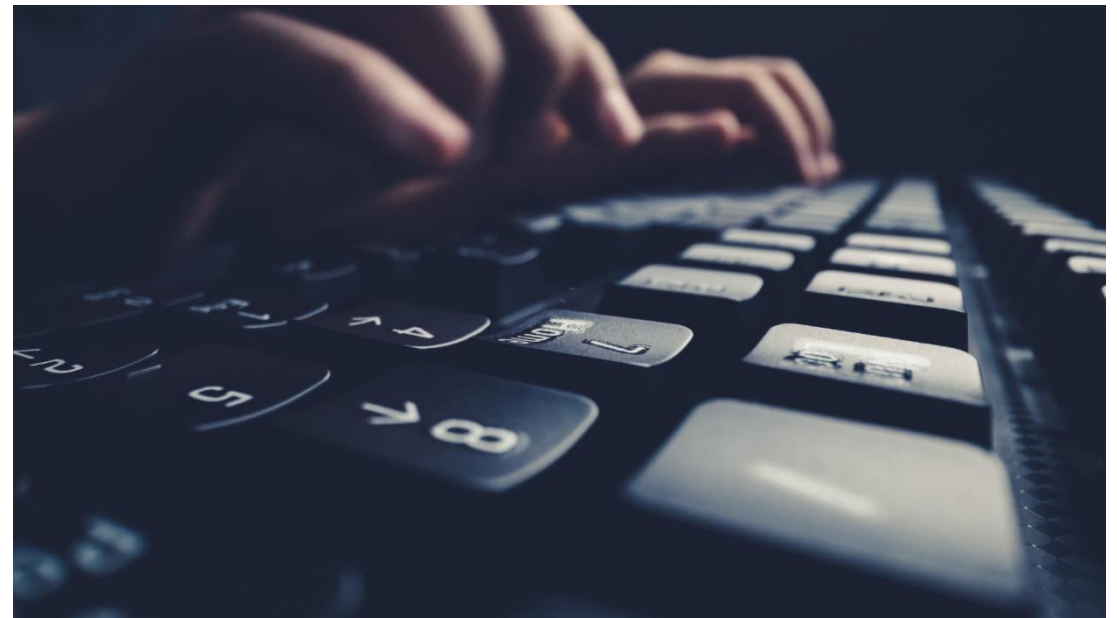
ADMINISTRATOR COLLABORATION

Manage Sessions Permission

- Publish and discard their own sessions.
- See sessions opened by other administrators, the number of the locks they have made.
- Disconnect and discard the private sessions of other administrators.
- Take over sessions created by applications, for example sessions created by the API command line tool.
- Take over the private sessions of other administrators.
- Publish and disconnect the private sessions of other administrators. The action applies to both SmartConsole sessions and command line API sessions.



Administrators working with multiple sessions can open multiple additional private sessions without publishing changes made in the current private session.



Concurrent Administration



- Multiple administrators work in read-write mode on the same security policy without impacting the other's work.
- Lock objects being managed to avoid overwrites or conflicts.
- Administrator profiles determine exact administrator privileges.

Concurrent Policy Installation

- One administrator or more can run different policy installation tasks on multiple Gateways at the same time.
- Five is the maximum number of policy installation tasks run at the same time. Anything above five is queued.
- When installing Access Control and Threat Prevention for the first time on a Gateway, Threat Prevention is queued until Access Control is installed.

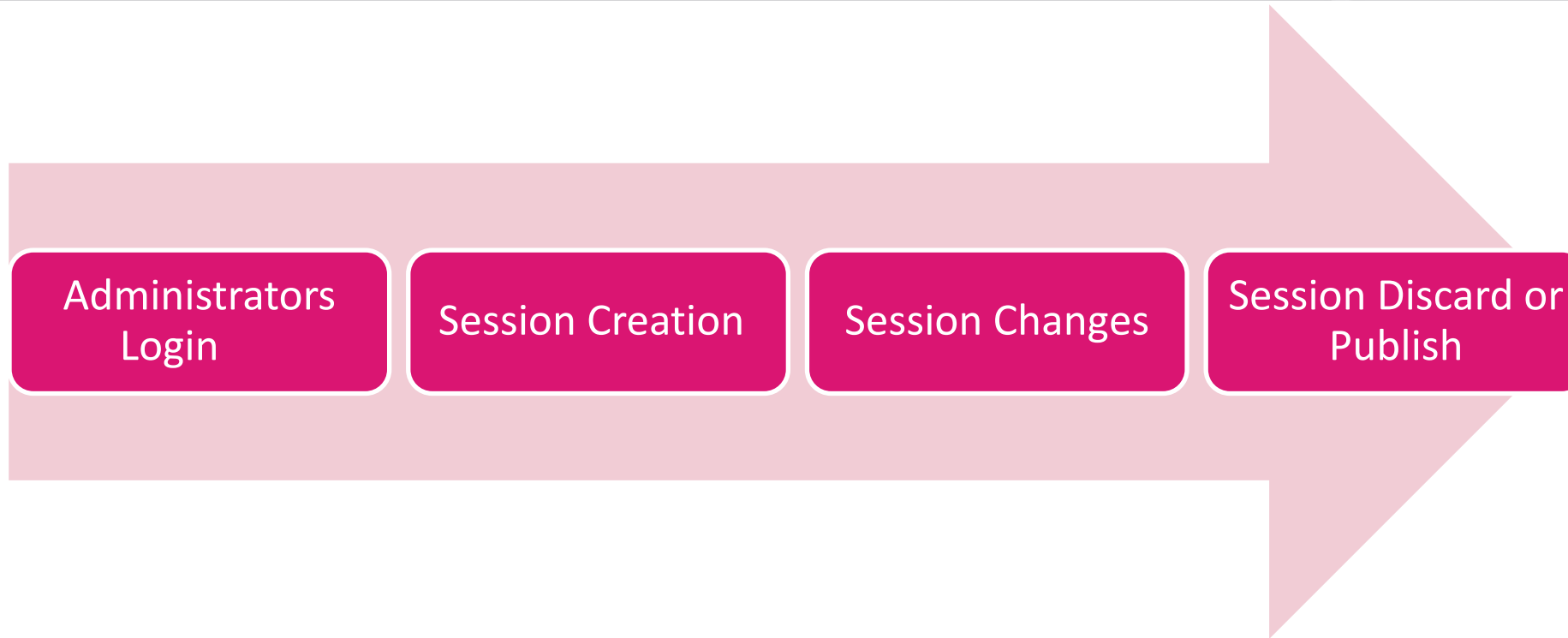
Supported:

- Access Control
- Threat Prevention

Not Supported

- Desktop
- QoS Closed

Session Workflow for Administrators







If you log out of SmartConsole and you did not discard or publish, you will be asked if you want to keep your changes.



If an admin logs out or loses connectivity before discarding or publishing the session, changes are preserved and are present when the admin logs in again or if the session is taken over by another admin.

Session Management



- ▾  Sessions
-  View Sessions
-  Revisions
-  Advanced

View Sessions

Sessions Actions ▾ Y

Name	Administrator	Workflow...	Connected...	Connection Mode	Application	Locks
(Current Ses...	admin	Open	23.101.188.233	Read Write	SmartConsole	0
(Unnamed)	sessionmanager@m...	Open	127.0.0.1	Read Write	Management API	0

(Current Session)

SmartConsole	Connected	Administrator:	admin
Number of Locks:	0	Connected from:	23.101.188.233
Number of Changes:	0		
Login:	04-Feb-23 12:50 PM		

See which administrator accounts are connected to the Security Management Server.

Revisions

Publish Time	Name	Publis...	Description
21-Nov-22 2:37 AM		Saul	Set rules in Corporate_Policy
21-Nov-22 2:37 AM		admin	Add rules in NAT Policy on Package "Bra
21-Nov-22 2:37 AM		admin	Add rules in NAT Policy on Package "Co
21-Nov-22 2:37 AM		admin	Add rules in HTTPS Policy
21-Nov-22 2:36 AM		admin	Add rules in HTTPS Policy
21-Nov-22 2:36 AM	Add Policy Package	admin	Add Branch_Office_Policy
21-Nov-22 2:36 AM	Add Policy Package	admin	Add Corporate_Policy
21-Nov-22 2:34 AM	Add Objects	admin	Add Objects

With R80 and higher, revisions are built-into the architecture.

Each publish operation creates a new revision, which contains only the changes from the previous revisions.

Revisions Options

Option	Description
Main Window	Displays the following: <ul style="list-style-type: none">• Publish Time - Date and time when the administrator published the session.• Name - Name of the database version assigned during the session.• Publisher - ID of the administrator that published the changes.• Changes - Number of changes published.• Description - Explanation of changes.
Edit	Edit Description.
View	Launch SmartConsole in a read-only mode and view a selected revision.
Revert	Revert to a selected rulebase. This action reverts the rulebase structure but not the objects used in the rulebase.
Purge	Permanently delete all data for the selected revision and all revisions prior to it.



Revert and Purge cannot be reversed.

Revisions Limitations

- Database Revision revert operation is not supported on a Backup Security Management Server.
- Reverting to a previous revision is an irreversible operation. Newer revisions than the target revision are lost.
- Changes apply to objects only and not to the file system.
- Tasks, SIC, and Licenses are not reverted.
- The revert action disconnects all other connected users and discards their private sessions.

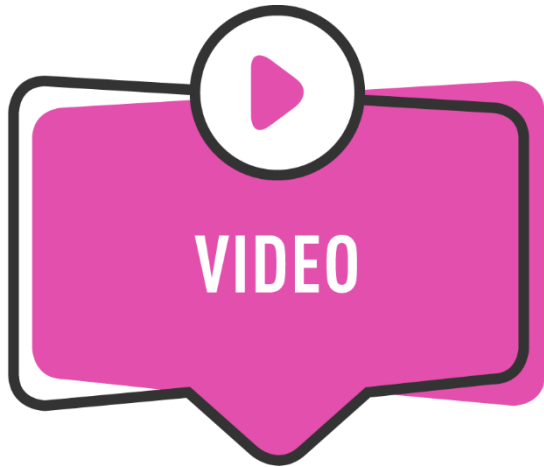
Revision is **not** supported in these scenarios:

- If SmartConsole and the Security Management Server are connected through a proxy server, the GUI for this feature is not supported. In this case, use the applicable API command.
- A Security Management Server or a Check Point object was created or deleted after the target revision date.
- The corresponding revision of the IPS or Application Control component was purged.

Best Practices

- Update the IPS and Application Control signatures and install the policy after the revert. Install policy if changes to log destinations are applied.
- If you need a full environment restore to a certain point in time, use Restore Backup.
- Purge irrelevant revisions. Too many revisions can create a heavy load on the server, which can cause disk and performance issues.





For further learning, watch the following video:

Database Revisions

This video is accessed from the online *Quantum Security Management R81.20 Administration Guide*.

Advanced - Sessions Settings

Session Settings

Session management

- Each administrator can manage a single SmartConsole session at a time
- Each administrator can manage multiple SmartConsole sessions at the same time

Session name and description

- Generate session name (on publish)

+ [administrator name] + @ + [date]

admin@04-Feb-23

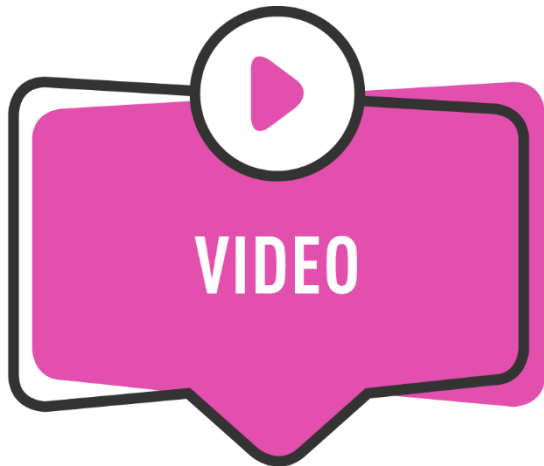
- All sessions must have a description

- Session management
- Session name and description

SmartWorkflow Overview

- With R81.20, administrators can define an Approval Cycle for Sessions (SmartWorkflow and Identity Provider).
- This ensures configuration changes are reviewed and approved by authorized administrators before the changes are published.





For further learning, watch the following video:

Approval Cycle for Sessions (SmartWorkflow and Identity Provider)

This video is accessed from the online *Quantum Security Management R81.20 Administration Guide*.

SmartWorkflow Configuration Workflow - Steps 1 and 2

Profile

Read Write All Approver

Used in SmartWorkflow, for approving other administrators' sessions.

- Overview
- Gateways
- Access Control
- Threat Prevention
- Others
- Monitoring and Logging
- Events and Reports
- Management**
- Endpoint

Management Permissions

- Manage Administrators ⓘ
- Manage Sessions
- High-Availability Operations
- Management API Login
- Cloud Management Extension (CME) API
- Publish sessions without an approval ⓘ
- Approve / reject other sessions
- Manage integration with Cloud Services

[Add Tag](#)

OK Cancel

Profile

Read Write All Submitter

Used in SmartWorkflow, allows only to submit changes for an approval, without the optio...

- Overview
- Gateways
- Access Control
- Threat Prevention
- Others
- Monitoring and Logging
- Events and Reports
- Management**
- Endpoint

Management Permissions

- Manage Administrators ⓘ
- Manage Sessions
- High-Availability Operations
- Management API Login
- Cloud Management Extension (CME) API
- Publish sessions without an approval ⓘ
- Approve / reject other sessions
- Manage integration with Cloud Services

[Add Tag](#)

OK Cancel

SmartWorkflow Configuration Workflow – Steps 3 and 4

Administrator

John Junior - Submitter
Enter Object Comment

General
Additional Info

Authentication

Authentication Method: Check Point Password
Password is defined
Certificate Information: Certificate is not defined

Permissions

Permission Profile: Read Write All Submitter

Expiration

Never
Expire At: 02-Feb-25

Add Tag

OK Cancel

Administrator

Jane Senior - Approver
Enter Object Comment

General
Additional Info

Authentication

Authentication Method: Check Point Password
Password is defined
Certificate Information: Certificate is not defined

Permissions

Permission Profile: Read Write All Approver

Expiration

Never
Expire At: 02-Feb-25

Add Tag

OK Cancel

Review Questions

1. Give at least one example of a physical component that network objects represent.
2. Give at least one example of a logical component that network objects represent.
3. What Permissions Profile allows unrestricted permissions?

Lab 3A

Establishing Secure Internal Communication



Lab 3B

Managing Administrator Access

