Welcome to SmartConsole Online Help



Offline Version of this Help
For offline viewing, download the complete help in TGZ format.
If you're viewing the offline version, and wish to see the latest online version, click here.



Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Gateways & Servers

What can I do here?

Use the **Gateways & Servers** view to:

- Create or delete servers and gateways.
- Edit properties of servers and gateways.
- Run scripts on servers and gateways.
- Run actions on servers and gateways.
- Generate a report of session changes.
- See summary, task, and error validation messages.
- View license details on the **Summary** tab in the bottom section (see *"Licenses" on page 16*).
- Manage licenses on the **Licenses** tab in the bottom section (see *"Licenses" on page 16*).
- Monitor device status (see *"Monitoring Device Status" below*).

Getting Here - SmartConsole > Gateways & Servers
Or:
SmartConsole for Multi-Domain Server > Gateways & Servers

Monitoring Device Status

The Gateways & Servers view in SmartConsole contains 6 views of the status of the Security Management Server and all the devices it manages.

- **General** - Provides general information about all devices.
- **Health** - Provides information about the health or operational status of each device.
- **Traffic** - Provides information about the volume of network traffic which passes through a specific device
- **Access Control** - Provides information about the Access Control blades and Identity Awareness information for each device.
- **Threat Prevention** - Provides information about the Threat Prevention blades and policy for each device.
- **Management** - Provides information about the management blades for each device.

- **Licenses** - Provides information about the licenses of the device and Software Blades enabled on the device.

The **General** view is the default view. To change the view, go to the top-left corner of the **Gateways & Servers** view > **Columns**, and from the drop-down menu, select the required view.

Device Status

The status updates of a Security Gateway reflect the status of the Software Blades. For example, if statuses of all the **Software Blades** are **OK**, except for the SmartEvent blade, which has a **Problem** status, the overall status is **Problem**.

Status Icon	Description
OK	The Security Gateway and all its Software Blades work properly.
Attention	At least one Software Blade has a minor issue, but the Security Gateway works.
Problem	At least one Software Blade reported a malfunction, or an enabled Software Blade is not installed.
Waiting	SmartView Monitor waits for the Security Management Server to send data from Security Gateways.
Disconnected	Cannot reach the Security Gateway.
Untrusted	Cannot make Secure Internal Communication between the Security Management Server and the Security Gateway.

Managing Gateways

A Security Gateway enforces Security Policies configured on the Security Management Server.

Creating a New Security Gateway

A Security Gateway enforces Security Policies configured on the Security Management Server.

To install Security Policies on the Security Gateways, configure the gateway objects in SmartConsole.

To define a new Security Gateway object:

1. From the navigation toolbar, select **Gateways & Servers**.
2. Click **New**, and select **Gateway**.

   The **Check Point Security Gateway Creation** window opens.
3. Click **Classic Mode**.

   The Check Point **Gateway** properties window opens and shows the **General Properties** screen.
4. Enter the host **Name** and the **IPv4 Address** or **IPv6 Address**.
5. Click **Communication**.

   The **Trusted Communication** window opens.
6. Select a **Platform**.
7. In the **Authentication** section, enter and confirm the **One-time password**.

   If you selected **Small Office Appliance** platform, make sure **Initiate trusted communication automatically when the Gateway connects to the Security Management Server for the first time** is selected.
8. Click **Initialize** to establish trusted communication with the gateway see *"Secure Internal Communication (SIC)" on the next page*.

   If trust fails to establish, Click **OK** to continue configuring the gateway.
9. Click **OK**.
10. The **Get Topology Results** window that opens, shows interfaces successfully configured on the gateway.
11. Click **Close**.
12. In the **Platform** section, select the **Hardware**, the **Version**, and the **OS**.

    If trust is established between the server and the gateway, click **Get** to automatically retrieve the information from the gateway.
13. Select the Software Blades to enable on the Security Gateway.

    For some of the Software Blades a first-time setup wizard will open. You can run the wizard now or later. For more on the setup wizards, see the relevant Administration Guide.

Manually Updating the Gateway Topology

As the network changes, you must update the gateway topology.

To update the gateway topology:

1. In SmartConsole, click **Gateways & Servers**.
2. Double-click the gateway object.

   The gateway property window opens.
3. Click **Network Management**.
4. Click **Get Interfaces**.

   A warning window asks if you want to overwrite the existing Topology and Anti-spoofing settings.
5. Click **Yes**.
6. The **Get Topology Results** window opens.
7. Click **Accept**.
8. Click **OK**.

Secure Internal Communication (SIC)

Check Point platforms and products authenticate each other through one of these Secure Internal Communication (SIC) methods:

- Certificates.
- Standards-based TLS for the creation of secure channels.
- 3DES or AES128 for encryption.

  Gateways above R71 use AES128 for SIC. If one of the gateways is below R71, the gateways use 3DES.

SIC creates trusted connections between gateways, management servers and other Check Point components. Trust is required to install polices on gateways and to send logs between gateways and management servers.

Initializing Trust

To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.

Note - Make sure the clocks of the gateway and Security Management Server are synchronized, before you initialize trust between them. This is necessary for SIC to succeed. To set the time settings of the gateway and Security Management Server, go to the **Gaia Portal** > **System Management** > **Time**.

To initialize Trust:

1. In SmartConsole, open the gateway network object.
2. In the **General Properties** page of the gateway, Click **Communication**.
3. In the **Communication** window, enter the **Activation Key** that you created during installation of the gateway.
4. Click **Initialize**.

   The ICA signs and issues a certificate to the gateway.

   Trust state is **Initialized but not trusted**. The Internal Certificate Authority (ICA) issues a certificate for the gateway, but does not yet deliver it.

   The two communicating peers authenticate over SSL with the shared Activation Key. The certificate is downloaded securely and stored on the gateway. The Activation Key is deleted.

   The gateway can communicate with Check Point hosts that have a security certificate signed by the same ICA.

SIC Status

After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

- **Communicating** - The secure communication is established.
- **Unknown** - There is no connection between the gateway and Security Management Server.
- **Not Communicating** - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.

Trust State

If the Trust State is compromised (keys were leaked, certificates were lost) or objects changed (user leaves, open server upgraded to appliance), reset the Trust State. When you reset Trust, the SIC certificate is revoked.

The Certificate Revocation List (CRL) is updated for the serial number of the revoked certificate. The ICA signs the updated CRL and issues it to all gateways during the next SIC connection. If two gateways have different CRLs, they cannot authenticate.

1. In SmartConsole, open the **General Properties** window of the gateway.
2. Click **Communication**.
3. In the **Trusted Communication** window that opens, click **Reset**.
4. Install Policy on the gateways.

This deploys the updated CRL to all gateways. If you do not have a Rule Base (and therefore cannot install a policy), you can reset Trust on the gateways.

Important - Before a new trust can be established in SmartConsole, make sure the same one-time activation password is configured on the gateway.

To establish a new trust state for a gateway:

1. Open the command line interface on the gateway.
2. Enter: **cpconfig**
3. Enter the number for **Secure Internal Communication** and press Enter.
4. Enter **y** to confirm.
5. Enter and confirm the activation key.
6. When done, enter the number for **Exit**.
7. Wait for Check Point processes to stop and automatically restart.

In SmartConsole:

1. In the **General Properties** window of the gateway, Click **Communication**.
2. In the **Trusted Communication** window, enter the one-time password (activation key) that you entered on the gateway.
3. Click **Initialize**.
4. Wait for the **Certificate State** field to show **Trust established**.
5. Click **OK**.

Troubleshooting SIC

If SIC fails to Initialize:

1. Make sure there is connectivity between the gateway and Security Management Server.
2. Make sure that the Security Management Server and the gateway use the same SIC activation key (one-time password).
3. If the Security Management Server is behind a gateway, make sure there are rules that allow connections between the Security Management Server and the remote gateway. Make sure Anti-spoofing settings are correct.
4. Make sure the name and the IP address of the Security Management Server are in the `/etc/hosts` file on the gateway.

If the IP address of the Security Management Server mapped through static NAT by its local gateway, add the public IP address of the Security Management Server to the `/etc/hosts` file on the remote gateway. Make sure the IP address resolves to the server's hostname.

5. Make sure the date and the time settings of the operating systems are correct. If the Security Management Server and remote the gateway reside in different time zones, the remote gateway may have to wait for the certificate to become valid.
6. Remove the Security Policy on the gateway to let all the traffic through: In the command line interface of the gateway, type: `fw unloadlocal`
7. Try to establish SIC again.

Remote User access to resources and Mobile Access

If you install a certificate on a gateway that has the Mobile Access Software Blade already enabled, you must install the policy again. Otherwise, remote users will not be able to reach network resources.

Understanding the Check Point Internal Certificate Authority (ICA)

The ICA (Internal Certificate Authority) is created on the Security Management Server when you configure it for the first time. The ICA issues certificates for authentication:

- **Secure Internal Communication (SIC)** - Authenticates communication between Security Management Servers, and between gateways and Security Management Servers.
- **VPN certificates for gateways** - Authentication between members of the VPN community, to create the VPN tunnel.
- **Users** - For strong methods to authenticate user access according to authorization and permissions.

ICA Clients

In most cases, certificates are handled as part of the object configuration. To control the ICA and certificates in a more granular manner, you can use one of these ICA clients:

- The *Check Point configuration utility* - This is the `cpconfig` CLI utility. One of the options creates the ICA, which issues a SIC certificate for the Security Management Server.
- *SmartConsole* - SIC certificates for Security Gateways and administrators, VPN certificates, and user certificates.
- *ICA Management tool* - VPN certificates for users and advanced ICA operations.

See audit logs of the ICA in SmartConsole **Logs & Monitor** > **New Tab** > **Open Audit Logs View**.

SIC Certificate Management

Manage SIC certificates in the

- **Communication** tab of the gateway properties window.
- ICA Management Tool.

Certificates have these configurable attributes:

Attributes	Default	Comments
validity	5 years	
key size	2048 bits	
KeyUsage	5	Digital Signature and Key encipherment
ExtendedKeyUsage	0 (no KeyUsage)	VPN certificates only

To learn more about key size values, see RSA key lengths.

Run One Time Script

What can I do here?

Use this window to manually enter and run a command line script on the selected GaiaSecurity Gateways. This feature is useful for scripts that you do not need to run more than one time. It also lets you run Gaia Clish and other commands directly from SmartConsole.

Getting Here - Gateways & Servers > Scripts > One Time Script

Understanding One-Time Scripts

When you specify a script:

- By default, the maximum size of a script is 8 KB.
- The output from the script shows in the **Tasks** tab at the bottom of the **Gateways & Servers** view.
- The **Run One Time Script** window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell.

Note - SmartConsole limits the length of a script's output. For more information, see sk181529.

Running a one-time script

Step	Instructions
1	Right-click the Security Gateway.
2	Select **Scripts > Run One Time Script**.
3	The **Run One Time Script** window opens. You can: ■ Enter the command in the **Script Body** text box and specify script arguments, or ■ Load the complete command from a text file **Notes:** • By default, the maximum size of a script is 8 kilobytes. • This value can be changed in SmartConsole > **Main application menu > Global properties > Advanced > Configure > Central Device Management > device_settings_max_script_length_in_KB**.
4	Click **Run**. The output from the script shows in the **Tasks** tab > **Results** column. ■ Double-click the task to view the output in a larger window. ■ You can also right-click the task and select **View**, then **Copy to Clipboard** **Notes:** • The **Run One Time Script** window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell. • If the Security Gateways are not part of a Cloning Group, you can run a script on multiple Security Gateways at the same time.

One Time Script Options

Script Body - Enter the script commands.

Load from File - Load a prepared script.

Comment - Enter a text comment (optional).

Run - Click to run the script that you entered.

Note - The ~ character is not supported in scripts for security reasons.

Run Repository Script

What can I do here?

Use this window to select a script to run on the selected Security Gateway.

Getting Here - Gateways & Servers > Scripts > Script Repository > Run button

Running Repository Scripts

You can run a predefined script from the script repository.

To run a script from the repository:

Step	Description
1	In the **Gateways & Servers** view, right-click the Security Gateways or Security Management Servers on which you want to run scripts.
2	Select **Scripts** > **Scripts Repository**. The **Scripts Repository** window opens.
3	Do one of these steps: ■ Select an existing script from the list, enter **Arguments** if needed, and click **Run**. ■ Click **New** to create a new script for the repository, or load it from a text file. Click **OK**.

The output from the script shows in the **Tasks** tab at the bottom of the **Gateways & Servers** view.

Notes:

- The **Scripts Repository** window does not support interactive or continuous scripts. To run interactive or continuous scripts, open a command shell.
- You can run the script on multiple Security Gateways or Security Management Servers at the same time.
- For a cluster object, the script will run automatically on all cluster members.
- The ~ character is not supported in scripts for security reasons.

Script Repository

What can I do here?

Use this window to add new scripts, edit existing ones, or delete scripts no longer in use.

Getting Here - SmartConsole > Gateways & Servers > Scripts > Script Repository
Or:
SmartConsole > Gateways & Servers > right-click an object > Scripts > Script Repository

Managing Repository Scripts

You can create new scripts, edit or delete scripts from the script repository.

To manage scripts:

1. Right-click the Security Gateway.
2. Select **Scripts > Manage Script Repository**
3. The **Script Repository** window opens

Note: You can also run and manage scripts by clicking **Scripts** in the Gateways view.

New Repository Script

What can I do here?

Use this window to:

- Create a new script
- Load a prepared script from file
- Edit an existing script

Getting Here - SmartConsole > Gateways & Servers > Scripts > Scripts Repository > New

Running scripts

The scripts repository lets you do many Gaia management and provisioning tasks directly from SmartConsole.

You can manually enter and run a command line script on the selected Gaia Security Gateways. This feature is useful for scripts that you do not need to run more than one time. It also lets you run Gaia Clish and other commands directly from SmartConsole.

Note - The ~ character is not supported in scripts for security reasons.

SmartConsole Actions

For the selected gateway, the Actions in the gateway view let you:

Action	Description
Monitor Info	Show monitoring information
System Backup	Create a system backup, not a snapshot image
System Restore	Restore the system from a backup file
Open Shell	Open a command line on the gateway
Support	Open a new service request

System Backup

What can I do here?

Use this window to back up the system of the selected device.

Getting Here - SmartConsole > Gateways & Servers > Select a Security Gateway > Actions > System Backup

Understanding the Fields

The backup location can be on the local gateway or a remote server. If the location is a remote server, enter the:

- IP address
- Transfer protocol
- Authentication credentials - username and password
- Path to a backup directory. The path must start and end with (/).

  For example: `/ftproot/backup/`

  Or just (/) for the root directory of the server.

The status of the Backup operation shows in **Tasks**.

When the task is complete, double-click the entry to see the file path and name of the backup file.

Note: This name is necessary to do a system restore.

To backup multiple Security Gateways, select them in the Gateways view and click **Actions > System Backup**.

System Restore

What can I do here?

Use this window to restore the system of the selected device.

Getting Here - SmartConsole > Gateways & Servers > Select a Security Gateway > Actions > System Restore

Understanding the Fields

- **Server**

  Select the server with the backup file.

- **Protocol**

  Select the transfer protocol

- **Username** and **Password**

  Enter authentication credentials

- **Path**

  The path to a backup directory and filename.

  The path must start and end with (/).

  For example: `/ftproot/backup/`

  Or just (/) for the root directory of the server.

  The file will be named according to this convention:

  `backup_<name of gateway object>_<date of backup>.tgz`

  If you cannot find the name of the file in **Tasks**, or did not save the file name after completing the backup process:

  1. Right-click the Security Gateway.
  2. Select **Actions > Open Shell**.
  3. On the gateway, run the Gaia Clish command: `show backup logs`.

4. Find the name of the compressed backup file.

   The file will be named according to this convention:

   `backup_<name of gateway object>_<date of backup>.tgz`

Open Shell

What can I do here?

Use this window to open a command line on the selected Security Gateway

Getting Here - SmartConsole > Gateways & Servers > Select a Security Gateway > Actions > Open Shell

Install Hotfix/Jumbo

What can I do here?

Use this window to install a recommended Jumbo Hotfix Accumulator or install a specific Hotfix.

For more information, see the *R81.10 Security Management Administration Guide*>Managing Gateways > Central Deployment of Hotfixes and Version Upgrades.

Getting Here - SmartConsole > Gateways & Servers > Select a Security Gateway > Actions > Install Hotfix/Jumbo

Version Upgrade

Use this window to perform a version upgrade.

For more information, see the *R81.10 Security Management Administration Guide* > Managing Gateways > Central Deployment of Hotfixes and Version Upgrades.

Getting Here - SmartConsole > Gateways & Servers > Select a Security Gateway > Actions > Version Upgrade

License Report

What can I do here?

Use this window to view a license report.

Getting Here - Gateways & Servers > Right-click gateway or server object > Actions > License Report

Device & License Information

What can I do here?

Use this window to monitor the selected gateway.

Getting Here - SmartConsole > Gateways & Servers > Monitor button

Available Monitoring Information

The monitoring information window has these panes:

Pane	Description
Device Status	Shows system information and network activity.
License Status	The blades the device can enable according to the licensing agreement.
System Counters	Shows system counters such as counters for content inspection and Threat Emulation history.
Traffic	Shows traffic, for example the top services or destinations.

Licenses

What can I do here?

Use this window to view the status of Gateway and Management Server licenses.

Getting Here - Gateways & Servers > Licenses tab

Starting from R81, you can add or remove licenses manually in SmartConsole.

Adding and removing a license

Step	Instructions
1	In SmartConsole, from the left navigation panel, click **Gateways & Servers**.
2	In the top pane, select the object of the applicable Management Server or Security Gateway.
3	In the bottom pane, click the **Licenses** tab.

Step	Instructions
4	Add or remove a license: ■ To add a license from a license file: a. Click **Add** and select **License File**. b. Browse for the license file. c. Select the license file. d. Click **Open**. ■ To add a license from a license string: a. Click **Add** and select **License String**. b. Paste the license string. c. Click **OK**. ■ To remove a license: a. Select the license in the leftmost column. b. Click **Remove**.

Note - To add or remove licenses on the **Licenses** tab, an administrator must have the **Run One Time Script** permission selected in their profile. To assign this permission, in SmartConsole, go to **Manage & Settings** > **Permissions & Administrators** > **Permission Profiles**. Open the relevant permission profile, go to **Gateways** > **Scripts**, and select **Run One-Time Scripts**.

You can see these columns with license information:

Column	Description
IP Address	The IP address, for which this license was generated.
Expiration Date	Date when the Check Point support contract expires.
CK	Unique Certificate Key of the license instance.
SKU	Catalog ID from the Check Point User Center.

Note - SmartConsole R81 and higher does not support viewing a license of Quantum Spark appliances with Gaia Embedded OS (in the "Gateways & Servers" view, select the Security Gateway object > in the bottom pane, click the "Licenses" tab).
Workaround: Use SmartUpdate to view the licenses.

Important - To distribute licenses to CloudGuard IaaS Security Gateways, see the *R81.10 CloudGuard Controller Administration Guide*.

License Status

What can I do here?

Use this window to see a list of Software Blades a Security Gateway can enable or not enable according to licensing restrictions.

Getting Here - Gateways & Servers > Select Network object > Monitor > License Status

Managing Software Blade Licenses

After an administrator runs the First Time Configuration Wizard on a Security Management Server, and the Security Management Server connects to the Internet, it automatically activates its license and synchronizes with the Check Point User Center. If the Security Management Server loses Internet connectivity before the license is activated, it tries again, on an interval.

If the administrator makes changes to Management Software Blade licenses of a Security Management Server in the Check Point User Center, these changes are automatically synchronized with that Security Management Server.

Notes:

- Automatic activation is supported on Check Point appliances only.
- Automatic synchronization is supported on all R81.10 servers.

To make sure that your environment is synchronized with the User Center, even when the Security Management Server is not connected to the Internet, we recommend that you configure a Check Point server with Internet connectivity as a proxy.

In SmartConsole, you can see this information for most Software Blade licenses:

- License status
- Alerts
- Check Point User Center details

Monitoring Licenses in SmartConsole

To keep track of license issues, you can use these options:

Option	Description
License Status view	To see and export license information for Software Blades on each specific Security Management Server, gateway, or Log Server object.

Option	Description
License Status report	To see filter and export license status information for all configured Security Management Server, gateway, or Log Server objects.
License Inventory report	To see filter and export license information for Software Blades on all configured Security Management Server, gateway, or Log Server objects.

The SmartEvent Software Blade lets you customize the **License Status** and **License Inventory** information from the **Logs & Monitor** view of SmartConsole.
It is also possible to view license information from the **Gateways & Servers** view of SmartConsole without enabling the SmartEvent blade on Security Management Server.

The Gateways & Servers view in SmartConsole lets you see and export the *License Inventory* report.

Step	Description
1	**To see the License Inventory report from the Gateways & Servers view:** 1. In SmartConsole, from the left navigation panel, click **Gateways & Servers**. 2. From the top toolbar, click **Actions** > **License Report**. 3. Wait for the **SmartView** to load and show this report. By default, this report contains: ■ *Inventory* page: Blade Names, Devices Names, License Statuses ■ *License by Device* page: Devices Names, License statuses, CK, SKU, Account ID, Support Level, Next Expiration Date
2	**To export the License Inventory report from the Gateways & Servers view:** 1. In the top right corner, click the **Options** button. 2. Select the applicable export option - **Export to Excel**, or **Export to PDF**.

The Logs & Monitor view in SmartConsole lets you see, filter and export the *License Status* report.

Step	Description
1	**To see the License Status report from the Logs & Monitor view:** 1. In SmartConsole, from the left navigation panel, click **Logs & Monitor**. 2. At the top, open a new tab by clicking **New Tab**, or **[+]**. 3. In the left section, click **Views**. 4. In the list of reports, double-click **License Status**. 5. Wait for the **SmartView** to load and show this report. By default, this report contains: ▪ Names of the configured objects, License status for each object, CK, SKU, Account ID, Support Level, Next Expiration Date
2	**To filter the License Status report in the Logs & Monitor view:** 1. In the top right corner, click the **Options** button **> View Filter**. The **Edit View Filter** window opens. 2. Select a **Field** to filter results. For example, **Device Name**, **License Status**, **Account ID**. 3. Select the logical operator - **Equals**, **Not Equals**, or **Contains**. 4. Select or enter a filter value. Note - Click the **X** icon to delete a filter. 5. Optional: Click the **+** icon to configure additional filters. 6. Click **OK** to apply the configured filters. The report is filtered based on the configured filters.
3	**To export the License Status report in the Logs & Monitor view:** 1. In the top right corner, click the **Options** button. 2. Select the applicable export option - **Export to Excel**, or **Export to PDF**.

The Logs & Monitor view in SmartConsole lets you see, filter and export the *License Inventory* report.

Step	Description
1	**To see the License Inventory report from the Logs & Monitor view:** 1. In SmartConsole, from the left navigation panel, click **Logs & Monitor**. 2. At the top, open a new tab by clicking **New Tab**, or **[+]**. 3. In the left section, click **Reports**. 4. In the list of reports, double-click **License Inventory**. 5. Wait for the **SmartView** to load and show this report. By default, this report contains: ▪ *Inventory* page: Blade Names, Devices Names, License Statuses ▪ *License by Device* page: Devices Names, License statuses, CK, SKU, Account ID, Support Level, Next Expiration Date
2	**To filter the License Inventory report in the Logs & Monitor view:** 1. In the top right corner, click the **Options** button **> Report Filter**. The **Edit Report Filter** window opens. 2. Select a **Field** to filter results. For example, **Blade Name**, **Device Name**, **License Overall Status**, **Account ID**. 3. Select the logical operator - **Equals**, **Not Equals**, or **Contains**. 4. Select or enter a filter value. Note - Click the **X** icon to delete a filter. 5. Optional: Click the **+** icon to configure additional filters. 6. Click **OK** to apply the configured filters. The report is filtered based on the configured filters.
3	**To export the License Inventory report in the Logs & Monitor view:** 1. In the top right corner, click the **Options** button. 2. Select the applicable export option - **Export to Excel**, or **Export to PDF**.

Viewing Licenses in SmartConsole

Step	Description
1	In SmartConsole, from the left navigation panel, click **Gateways & Servers**.
2	From the **Columns** drop-down list, select **Licenses**.

You can see these columns:

Column	Description
License Status	The general state of the Software Blade licenses: ■ **OK** - All the blade licenses are valid. ■ **Not Activated** - Blade licenses are not installed. This is only possible in the first 15 days after the establishment of the SIC with the Security Management Server. After the initial 15 days, the absence of licenses will result in the blade error message. ■ **Error with <number> blade(s)** - The specified number of blade licenses are not installed or not valid. ■ **Warning with <number> blade(s)** - The specified number of blade licenses have warnings. ■ **N/A** - No available information.
CK	Unique Certificate Key of the license instance.
SKU	Catalog ID from the Check Point User Center.
Account ID	User's account ID.
Support Level	Check Point level of support.
Support Expiration	Date when the Check Point support contract expires.

To view license information for each Software Blade:

Step	Description
1	Select a Security Gateway or a Security Management Server.
2	In the **Summary** tab below, click the object's **License Status** (for example: **OK**). The **Device & License Information** window opens. It shows basic object information and **License Status**, license **Expiration Date**, and important quota information (in the **Additional Info** column) for each Software Blade. **Notes:** ■ Quota information, quota-dependent license statuses, and blade information messages are only supported for R80. ■ The tooltip of the SKU is the product name.

The possible values for the Software Blade **License Status** are:

Status	Description
Active	The Software Blade is active and the license is valid.
Available	The Software Blade is not active, but the license is valid.
No License	The Software Blade is active but the license is not valid.
Expired	The Software Blade is active, but the license expired.
About to Expire	The Software Blade is active, but the license will expire in thirty days (default) or less (7 days or less for an evaluation license).
Quota Exceeded	The Software Blade is active, and the license is valid, but the quota of related objects gateways, files, virtual systems, and so on, depending on the blade) is exceeded.
Quota Warning	The Software Blade is active, and the license is valid, but the number of objects of this blade is 90% (default) or more of the licensed quota.
N/A	The license information is not available.

Open Gaia Portal - Cluster

What can I do here?

Use this window to open select the cluster member to connect to.

Getting Here - SmartConsole > Gateways & Servers > Select a Cluster > Actions > Gaia Portal

Verify Software Package Task Details

What can I do here?

Use this window to the follow the progress of a task verification.

Getting Here - SmartConsole > Gateways & Servers > Select a Security Gateway > Actions > Install Hotfix/Jumbo

Or:

Gateways & Servers > Select a Security Gateway > Actions > Version Upgrade > Verify

Service Request Wizard

What can I do here?

Use this window to open a service request.

Getting Here - SmartConsole > Gateways & Servers > Actions > Support > New Service Request

Network Management - Security Gateway

What can I do here?

Use this window to add, edit, or delete network interfaces from a Security Gateway.

Getting Here - Gateways & Servers > Select gateway > Edit > Network Management > Click the *Expand* button 

Network Management - System Backup

What can I do here?

Use this window to back up the configuration of the Gaia operating system and of the Security Management Server database. You can restore a previously saved configuration. The configuration is saved to a .tgz file. You can store backups locally or remotely to a TFTP, SCP or FTP server. You can run the backup manually or on a schedule.

- **Server IP** - the server that will hold the backup
- **Protocol** - The file transfer protocol to use - SCP, FTP, TFTP
- **User Name and Password** -- to authenticate to the backup server.
- **Path** - to the backup folder on the server

Getting Here - Gateways & Servers > Select gateway > Edit > Network Management > System Backup

Network Management - Security Gateway Cluster

What can I do here?

Use this window to add, edit, or delete network interfaces from the cluster.

Getting Here - Gateways & Servers > Security Gateway Cluster > Edit > Network Management > Click the *Expand* button 

Network Management - Advanced

What can I do here?

Use this window to enable Extended Cluster Anti-spoofing.

Getting Here - Gateways & Servers > Security Gateway Cluster > Edit > Network Management > Advanced

Interface - General

What can I do here?

Use this window to set the IPv4/6 addresses of the selected interface, and configure the topology.

Getting Here - Gateways & Servers> Select gateway/Cluster > Edit > Network Management > Click the *Expand* button > Select an interface > Edit

Editing the Topology

Use this this window to edit the interface topology. If the gateway is a member of cluster, these options are available. This window shows topology information all detected interfaces in the cluster object and its related members.

General

- **Network Type** - The purpose of the network connected to the selected interface:
  - **Private** - An interface that is not part of the cluster but can be monitored or not monitored.

    Monitored - An interface that is not part of the cluster, but ClusterXL monitors the member state and failover occurs if a fault is detected. Applies to third-party clusters, and not supported for Small Business appliances.

    Not Monitored - An interface that is not part of the cluster. ClusterXL does not monitor the member state and there is no failover. This option is recommended for the management interface.
  - **Cluster** - A cluster interface that connects to an internal or external network. Enter the cluster virtual IP addresses for each network (internal or external). These addresses must be located in the calculated subnet, and represent the cluster as a whole rather than individual cluster members.

    Virtual IPv4/IPv6 address - Lists virtual interfaces. These are secondary cluster IP addresses on the same member interface, and apply only to third party OPSEC configurations. For details regarding such configurations, refer to the appropriate OPSEC product user guide. Synchronization and private interfaces do not have virtual interfaces.
  - **Sync** - A cluster synchronization interface. You must define one or more synchronization interfaces for redundancy. If you are using more than one synchronization interface, define which interface is the primary, secondary, or tertiary interface. Synchronization redundancy is not supported on Small Medium Business appliances. On these appliances, you can only select 1st sync and only for the LAN2/SYNC interface. You cannot configure VLANs on the synchronization interface.
  - **Cluster + Sync** - Cluster interface that is also a synchronization interface. This option is less secure and is not recommended. This option in not supported for Small Business appliances.

  Note - Changing the **Network Type** changes the **Advanced** options. For example, selecting **Cluster + Sync** adds **Synchronization** order to the **Advanced** Options. Selecting **Private** adds the **Monitoring** option to the **Advanced** page.

Member IPs

The physical IP address for each member interface.

Topology

Type of network (Internal or External) for Anti-Spoofing protection.

Interface - Member IPs

What can I do here?

Use this window to add or edit cluster member IP addresses and netmasks.

Getting Here - Gateways & Servers> Security Gateway Cluster > Edit > Network Management > New/edit interface > General tab > Member IPs > Modify

Interface - Topology Settings

What can I do here?

Use this window to configure the interface's topology.

Getting Here - Gateways & Servers> Select gateway > Edit > Network Management > Click the *Expand* button > Select an interface > Edit > Topology section > Modify

Understanding Topology

An interface can be defined as being External (leading to the Internet) or Internal (leading to the LAN).

The type of network that the interface **Leads To**:

- **Internet (External)** or **This Network (Internal)** - This is the default setting. It is automatically calculated from the topology of the gateway. To update the topology of an internal network after changes to static routes, click **Network Management** > **Get Interfaces** in the **General Properties** window of the gateway.
- **Override** - Override the default setting.

If you **Override** the default setting:

- **Internet (External)** - All external/Internet addresses
- **This Network (Internal)** -
  - **Not Defined** - All IP addresses behind this interface are considered a part of the internal network that connects to this interface
  - **Network defined by the interface IP and Net Mask** - Only the network that directly connects to this internal interface

- **Network defined by routes** - The gateway dynamically calculates the topology behind this interface. If the network changes, there is no need to click "Get Interfaces" and install a policy.
- **Specific** - A specific network object (a network, a host, an address range, or a network group) behind this internal interface
- **Interface leads to DMZ** - The DMZ that directly connects to this internal interface

VPN Tunnel Interfaces

If the interface is part of a VPN Tunnel, then the interface **Leads To** a **Point to Point** network. The interface is one end of the point to point connection. All traffic in the network behind the interface is part of the point to point connection. Click **Override** to define a specific network.

Dynamically Updating the Topology

This feature is supported only for Security Gateways R77.20 and above. Once selected, the range of IP addresses behind the internal interface is automatically calculated every second (default value) without the need for the administrator to click **Get Interfaces** and install a policy.

To configure dynamic topology updates:

1. Open **Gateway Properties > Network Management**.
2. Select an interface and click **Edit**.
3. In the **Topology** section, click **Modify**.
4. In the **Leads To** section, select **Network defined by routes**.
5. Click **OK**.

This default update value is configured in **SmartConsole > Preferences** and set to one second. The value set here applies to all internal interfaces for all gateways in the domain.

To set the update value for a specific interface:

1. Open **Gateway Properties > Network Management**.
2. Select an interface and click **Actions > Settings**.
3. Select **Use custom update time (seconds)** and set the applicable update time.
4. Click **OK**.

Dynamic Anti-Spoofing

When Anti-Spoofing is selected and you click **Get interfaces**, the Security Gateway generates a list of valid IP addresses based on the IP address and netmask of the interface and the routes assigned to the interface.

Anti-Spoofing drops packets with a source IP address that does not belong to the network behind the packet's interface. For example, packets with an internal IP address that comes from an external interface.

When the **Network defined by routes** option is selected along with **Perform Anti-Spoofing based on interface topology**, you get *Dynamic Anti-Spoofing*. The valid IP addresses range is automatically calculated without the administrator having to do click **Get Interfaces** or install a policy.

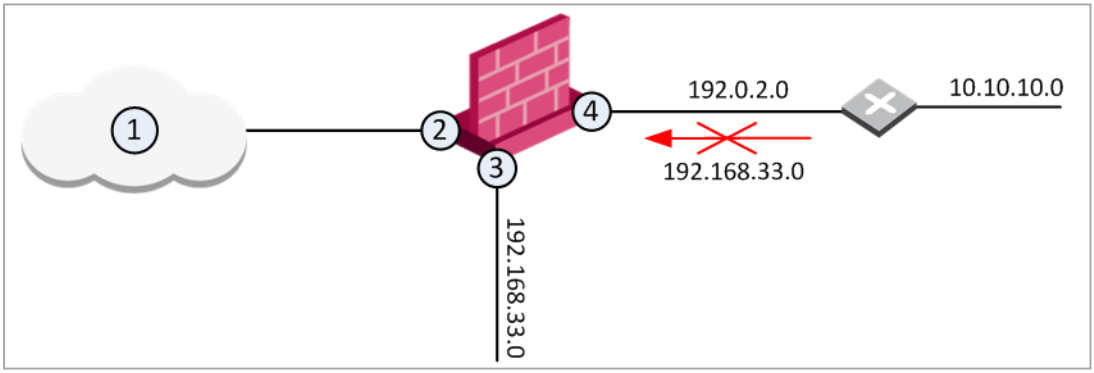
Preventing IP Spoofing

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

Anti-Spoofing detects if a packet with an IP address that is behind a certain interface, arrives from a different interface. For example, if a packet from an external network has an internal IP address, Anti-Spoofing blocks that packet.

Example:

The diagram shows a Gateway with interfaces 2 and 3, and 4, and some example networks behind the interfaces.



For the Gateway, anti-spoofing makes sure that

- All incoming packets to 2 come from the Internet (1)
- All incoming packets to 3 come from 192.168.33.0
- All incoming packets to 4 come from 192.0.2.0 or 10.10.10.0

If an incoming packet to B has a source IP address in network 192.168.33.0, the packet is blocked, because the source address is spoofed.

When you configure Anti-Spoofing protection on a Check Point Security Gateway interface, the Anti-Spoofing is done based on the interface topology. The interface topology defines where the interface **Leads To** (for example, **External** (Internet) or **Internal**), and the **Security Zone** of interface.

Configuring Anti-Spoofing

Make sure to configure Anti-Spoofing protection on all the interfaces of the Security Gateway, including internal interfaces.

To configure Anti-Spoofing for an interface:

1. In SmartConsole, go to **Gateways & Servers** and double-click the Gateway object.

   The **Gateway Properties** window opens.

2. From the navigation tree, select **Network Management**.

3. Click **Get Interfaces**.

4. Click **Accept**.

   The gateway network topology shows. If SmartConsole fails to automatically retrieve the topology, make sure that the details in the **General Properties** section are correct and the Security Gateway, the Security Management Server, and the SmartConsole can communicate with each other.

5. Select an interface and click **Edit**.

   The interface properties window opens.

6. From the navigation tree, click **General**.

7. In the **Topology** section of the page, click **Modify**.

   The **Topology Settings** window opens.

8. In the **Leads To** section, select the type of network, to which this interface leads:

   - **Internet (External)** - This is the default setting. It is automatically calculated from the topology of the Security Gateway. To update the topology of an internal network after changes to static routes, click **Network Management** > **Get Interfaces** in the **Gateway Properties** window.
   - **Override** - Override the default setting.

   If you **Override** the default setting:

- **Internet (External)** - All external/Internet addresses
- **This Network (Internal)** -
  - **Not Defined** - All IP addresses behind this interface are considered a part of the internal network that connects to this interface
  - **Network defined by the interface IP and Net Mask** - Only the network that directly connects to this internal interface
  - **Network defined by routes** - The Security Gateway dynamically calculates the topology behind this interface. If the network of this interface changes, there is no need to click **Get Interfaces** and install a policy.
  - **Specific** - A specific object (a Network, a Host, an Address Range, or a Network Group) behind this internal interface
  - **Interface leads to DMZ** - The DMZ that directly connects to this internal interface

9. **Optional:** In the **Security Zone** section, select **User defined**, check **Specify Security Zone** and choose the zone of the interface.
10. Configure **Anti-Spoofing Options**. Make sure that **Perform Anti-Spoofing based on interface topology** is selected.
11. Select an **Anti-Spoofing action**:
    - **Prevent** - Drops spoofed packets
    - **Detect** - Allows spoofed packets. To monitor traffic and to learn about the network topology without dropping packets, select this option together with the **Spoof Tracking Log** option.
12. Configure Anti-Spoofing exceptions (optional). For example, configure addresses, from which packets are not inspected by Anti-Spoofing:
    a. Select **Don't check packets from**.
    b. Select an object from the drop-down list, or click **New** to create a new object.
13. Configure **Spoof Tracking** - Select the tracking action that is done when spoofed packets are detected:
    - **Log** - Create a log entry (default)
    - **Alert** - Show an alert
    - **None** - Do not log or alert
14. Click **OK** twice to save Anti-Spoofing settings for the interface.

For each interface, repeat the configuration steps. When finished, install the Access Control policy.

Anti-Spoofing Options

- **Perform Anti-Spoofing based on interface topology** - Select this option to enable spoofing protection on this external interface.
- **Anti-Spoofing action is set to** - Select this option to define if packets will be rejected (the Prevent option) or whether the packets will be monitored (the Detect option). The Detect option is used for monitoring purposes and should be used in conjunction with one of the tracking options. It serves as a tool for learning the topology of a network without actually preventing packets from passing.
- **Don't check packets from** - Select this option to make sure anti-spoofing does not take place for traffic from internal networks that reaches the external interface. Define a network object that represents those internal networks with valid addresses, and from the drop-down list, select that network object. The anti-spoofing enforcement mechanism disregards objects selected in the **Don't check packets from** drop-down menu.
- **Spoof Tracking** - Select a tracking option.

VPN Tunnel Interface

What can I do here?

Use this window to edit the VPN Tunnel settings.

Getting Here - Gateways & Servers> Select gateway > Edit > Network Management > Click the *Expand* button > Select a VPN interface > Edit > VPN Tunnel

Network Management Settings

What can I do here?

When **Network defined by routes** is selected in the gateway's topology, use this window to set a custom update time. The gateway dynamically calculates the topology behind these interfaces according to the time interval set here. The interval applies only to those interfaces with **Network defined by routes** selected.

Getting Here - Gateways & Servers> Select gateway > Edit > Network Management > Actions > Settings

Interface - QoS

What can I do here?

Use this window to define:

- Direction and rate of bandwidth on the interface
- DiffServ and Low Latency Classes

Getting Here - Gateways & Servers> Select gateway > Edit > Network Management > Click the *Expand* button > Select an interface > Edit > QoS

Understanding QoS

Quality of Service is a set of intelligent network protocols and services that are used to efficiently manage the movement of information through a local or wide area networks. QoS services sort and classify flows into different traffic classes, and allocate resources to network traffic flows based on user or application ID, source or destination IP address, time of day, application specific parameters, and other user-specified variables. Fundamentally, QoS enables you to provide better service to certain flows. This is done by either raising the priority of a flow or limiting the priority of another flow.

A bandwidth management tool must be able to accurately classify communications. However, simply examining a packet in isolation does not provide all the information needed to make an informed decision. State information derived from past communications and other applications is also required. A packet's contents, the communication state and the application state (derived from other applications) must all be considered when making control decisions.

Low Latency QoS Class

What can I do here?

Use this window to define QoS Low Latency class properties. Specify the **Constant Bit Rate**, the rate at which packets of this class will be transmitted, and the **Maximal Delay**, the outer limit of the delay that will be tolerated for packets of this class, specified for active directions.

Note - DiffServ and Low Latency Class objects can only be defined in SmartDashboard.Open the SmartDashboard toolbar > Manage > QoS > QoS Classes

Getting Here - Gateways & Servers > Select gateway > Edit > Network Management > Click the *Expand* button > Select an interface > Edit > QoS > DiffServ and Low Latency Classes section > Click + > Low Latency Classes

Avoiding Low Drops

Avoiding drops means holding (possibly long) queues, which may lead to non-negligible delays. For some types of traffic, such as voice and video, bounding this delay is important. Long queues are inadequate for these types of traffic because they lead to substantial delay. Fortunately, for most "delay sensitive" applications, there is no need to drop packets from queues in order to keep them short.

Instead, the fact that the streams of these applications have a known, bounded bit rate can be utilized. If QoS is configured to forward as much traffic as the stream delivers, then only a small number of packets accumulate in the queues and delay is negligible.

QoS Low Latency Queuing makes it possible to define special Classes of Service for "delay sensitive" applications like voice and video. Rules under these classes can be used together with other rules in the security policy Rule Base. Low Latency classes require you to specify the maximal delay that is tolerated and a Constant Bit Rate. QoS then guarantees that traffic matching rules of this type is forwarded within the limits of the bounded delay.

For each Low Latency class defined on an interface, a constant bit rate and maximal delay should be specified for active directions. QoS checks packets matched to Low Latency class rules to make sure they have not been delayed for longer than their maximal delay permits. If the maximal delay of a packet has been exceeded, it is dropped. Otherwise, it is transmitted at the defined constant bit rate for the Low Latency class to which it belongs.

If the Constant Bit Rate of the class is defined correctly (meaning that it is not smaller than the expected arrival rate of the matched traffic), packets are not dropped (provided that the delay exceeds some minimum). On the other hand, when the arrival rate is higher than the specified Constant Bit Rate, packets exceeding this constant rate are dropped to ensure that those transmitted are within the maximal delay limitations.

Note - The maximal delay set for a Low Latency class is an upper limit. This means that packets matching the class are always forwarded with a delay not greater, but often smaller, than specified.

In most cases, one Low Latency class is sufficient to serve all bounded delay traffic. In some cases, however, the user may need to define more than one Low Latency class. For this purpose, Low Latency classes are assigned one out of five priority levels (not including the Expedited Forwarding class. These priority levels are relative to other Low Latency classes.

It is advisable to define more than one Low Latency class if different types of traffic require different maximal delays.

The class with the lower maximal delay should get a higher priority than the class with the higher delay. The reason for this is that when two packets are ready to be forwarded, one for each Low Latency class, the packet from the higher priority class is forwarded first. The remaining packet (from the lower class) then encounters greater delay. This implies that the maximal delay that can be set for a Low Latency class depends on the Low Latency classes of higher priority.

Other Low Latency classes can affect the delay incurred by a class and therefore must be taken into consideration when determining the minimal delay that is feasible for the class. This is best done by initially setting the priorities for all Low Latency classes according to maximal delay, and then defining the classes according to descending priority. When you define class two, for example, class one should already be defined.

DiffServ QoS Class Properties (Interface)

What can I do here?

Use this window to define QoS class properties specifying guaranteed bandwidth level and limits. In this window you can:

- Specify the DiffServ QoS Class.
- For the selected DiffServ QoS Class, specify - for inbound and outbound connections -- the guaranteed bandwidth and the limit at which the guaranteed bandwidth is exceeded.

Note - DiffServ and Low Latency Class objects can only be defined in SmartDashboard. Open the SmartDashboard toolbar > Manage > QoS > QoS Classes

Getting Here - Gateways & Servers > Select gateway > Edit > Network Management > Click the *Expand* button > Select an interface > Edit > QoS > DiffServ and Low Latency Classes section > Click + > DiffServ classes > Others
Or:
Edit Security Gateway that has QoS enabled > Network Management > Edit Interface with QoS > DiffServ and Low Latency classes > New (or Edit) > DiffServ Classes > Expedited Forwarding

Understanding DiffServ

DiffServ (Differentiated Services) is a technology in which packets are marked (in the IP header) inside the enterprise network as belonging to a certain class of service. These packets are then granted priority on the public network.

Interface - Multicast Restrictions

What can I do here?

Use this window to define multicast access restrictions for the interface. These restrictions specify multicast groups (addresses or address ranges) to allow or block.

Getting Here - Gateways & Servers > Select gateway > Edit > Network Management > Click the *Expand* button > Select an interface > Edit > Advanced

Per Interface Multicast Restrictions

A multicast enabled router forwards multicast datagrams from one interface to another. When multicast is enabled on a Security Gateway, you can define multicast access restrictions on each interface. These restrictions specify multicast groups (addresses or address ranges) to allow or block.

The enforcement is performed on outgoing multicast datagrams. Anti-spoofing makes sure that the source IP address of the packets entering an interface with multicast datagrams is performed on the multicast group address.

Gateway with per-interface multicast restrictions

When no restrictions for multicast datagrams are defined, multicast datagrams entering the gateway on one interface are allowed out of all others.

As well as defining a per-interface restrictions, a rule must also be defined in the Firewall Rule Base that allows multicast traffic and required services. The Destination of this rule must allow the required multicast groups.

VPN connections

Multicast traffic can be encrypted and sent across VPN links that are defined using multiple VPN tunnel interfaces (virtual interfaces associated with the same physical interface).

Multicast Restriction Options

- **Drop multicast packets whose destination is in the list** specifies that outgoing packets from this interface to the listed multicast destinations will be dropped.
- **Drop all multicast packets except those whose destination is in the list** specifies that outgoing packets from this interface to all multicast destinations except those listed will be dropped.
- **Tracking** lets you select a method for tracking dropped multicast packets.

Interface Names

This section shows the name of the interface in SmartConsole and the name the interface uses on the Gaia Operating system.

Synchronization

When **Sync** or **Cluster + Sync** is selected as the **Network Type** on the **General** page, select the sync order here.

Note -2nd and **3rd** Sync in no longer supported in R77.20 and higher.

Sync

- **1st, 2nd, 3rd Sync** - A cluster synchronization interface. You must define one or more synchronization interfaces for redundancy.

  1st Sync means that is the primary sync network.

  2nd Sync or 3rd Sync means it is a backup synchronization network. Failover occurs to the 2nd or 3rd sync network if the higher priority network fails.

- If you are using more than one synchronization interface, define which interface is the primary, secondary, or tertiary interface.
- Synchronization redundancy is not supported on Small Business Appliances. On these appliances, you can only select 1st sync and only for the LAN2/SYNC interface.
- You cannot configure VLANs on the synchronization interface.
- It is recommended that secure and dedicated networks are used for synchronization.
- For High Availability mode, synchronization is recommended. Otherwise, existing connections on a failed cluster member will be closed when cluster failover occurs.

Cluster + Sync

- **1st, 2nd, 3rd Sync** - Cluster interface that is also a synchronization interface.
- This option is less secure and is not recommended. This option in not supported for Small Business appliances.
- It is possible, though less secure (and therefore not recommended), to use a network which contains an internal cluster interface to serve as a synchronization network.
- This is option not supported for Small Business Appliances.

Monitoring

When **Private** is selected as the **Network Type** on the **General** page, you can monitor or not monitor the interface.

- **Monitored Interface** - An interface that is not part of the cluster, but ClusterXL monitors the member state and failover occurs if a fault is detected
- **Non-Monitored** - An interface that is not part of the cluster. ClusterXL does not monitor the member state and there is no failover. This option is recommended for the management interface

Install Database

What can I do here?

Use this window to manually install the management database (user database and network objects) on the selected targets.

Getting Here - SmartConsole > Menu > Install Database

User Database

Users defined in SmartConsole are saved to the *User Database* on the Security Management Server, together with the user authentication schemes and encryption keys. Then, the user database is installed on Security Gateways and Check Point hosts:

- On Security Gateways - When the policy is installed (when you click **Install Policy**)
- On Check Point hosts with an active **Management** blade (such as Log Server) - When the database is installed (when you click **Menu** > **Install Database**)

The user database does **not** contain information about users defined elsewhere than on the Security Management Server (such as users in external User Directory groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the management server.

Installing the User Database in SmartConsole

When you make changes to user definitions through SmartConsole, they are saved to the user database on the Security Management Server. User authentication methods and encryption keys are also saved in this database. The user database does **not** contain information about users defined externally to the Security Gateway (such as users in external User Directory groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the Security Management Server.

You must choose to install the policy or the user database, based on the changes you made:

- Install the policy, if you modified additional components of the Policy Package (for example, added new Security Policy rules) that are used by the installation targets
- Install the user database, if you only changed the user definitions or the administrator definitions - From the Menu, select **Install Database**

The user database is installed on:

- Security Gateways - during policy installation
- Check Point hosts with one or more Management Software Blades enabled - during database installation

You can also install the user database on Security Gateways and on a remote server, such as a Log Server, from the command line interface on the Security Management Server.

Installing the Database with API

Use the API "`install-database`". See the *Check Point Management API Reference* (at the top, select the correct version) .

Possible Loss of Data During Sync

For more on this issue, see: *"High Availability Status" below*

High Availability Status

What can I do here?

Use this window to see the High Availability status, and to change the server between primary (active) and secondary (standby).

Getting Here - Menu > Management High Availability

The High Availability Environment

A Management High Availability environment includes:

- One Active Security Management Server
- One or more Standby Security Management Server

For full redundancy, the active management server at intervals synchronizes its database with the secondary server or servers.

Active vs. Standby

In a standard High Availability configuration there is one Active server at a time. The administrator uses the Active server manage the High Availability configuration. The Active server automatically synchronizes the standby server(s) at regular intervals. You can open a Standby server only in Read Only mode. If the Active server fails, you can initiate a changeover to make a Standby server become the Active server. If communication with the Active server fails, there may be more than one Active server. This is called Collision Mode.

Primary Server vs. Secondary Server

The sequence in which you install management servers defines them as Primary or Secondary. The first management server installed becomes the Primary active server. When you install more Security Management Servers, you define them as Secondary. Secondary servers are Standby servers by default.

Important - Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the: *R81.10 Gaia Administration Guide*
- About the `migrate export` and `migrate import` commands, see the *R81.10 CLI Reference Guide*
- About the `mds_backup` and `mds_restore` commands, see the *R81.10 Multi-Domain Security Management Administration Guide*
- About Virtual Machine Snapshots, see the vendor documentation.

Single and Multi-Domain Management High Availability

For Security Management Server

Configuring a Secondary Server in SmartConsole

In the SmartConsole connected to the Primary server, create a network object to show the Secondary Security Management Server. After you publish, synchronize starts between the primary and secondary servers.

To configure the secondary server in SmartConsole:

1. Open SmartConsole.
2. In **Object Categories**, click **New > More > Network Object > Gateways and Servers > Check Point Host**.
3. On the **General Properties** page, enter a unique name and IP address for the server.
4. In the **Software Blades** section, select the **Management** tab.
5. Select **Network Policy Management**.

   This automatically selects the **Secondary Server, Logging and Status, and Provisioning**.
6. Create SIC trust between the Secondary Security Management Server and the Primary:
   a. Click **Communication**.
   b. Enter the SIC Activation Key of the secondary server.

c. Click **Initialize**.

d. Click **Close**.

7. Click **OK**.
8. Publish the SmartConsole session to save these session changes to the database.

   The initialization and synchronization between the servers start.
9. Monitor these tasks in the Task List, in the SmartConsole System Information area. Wait for the Task List to show that a full sync has completed.
10. Open the **High Availability Status** window and make sure there is one active server, and one standby.

Synchronizing Active and Standby Servers

At intervals, the Active server synchronizes with the standby server or servers, and when you publish the session. Sessions that are not published are not synchronized.

Understanding how Synchronization Works

When changes made in private sessions are published on the active server (made public) the changes are copied to the standby servers. During failover, all public and private sessions are copied from the active to the standby before the standby becomes active.

Monitoring High Availability

The **High Availability Status** window shows the status of each Security Management Server in the High Availability configuration.

To see the server status in your High Availability environment:

1. Open SmartConsole and connect to a primary or secondary server.
2. On the **Menu**, click **High Availability**.

   The **High Availability Status** window opens.

For the management server and its peer or peers in the High Availability configuration, the **High Availability Status** window shows:

- A Warning or Error message – The message shows if there is a problem between the High Availability peers.
- **Connected To** - The server that SmartConsole is connected to. Also, the High Availability mode of the server (Active or Standby), and the synchronization status and actions of the server.

- **Peers** - The servers that the connected server sees. Also, the High Availability mode of each server (Active or Standby), and the synchronization status and actions of each server.

Monitoring Synchronization Status

Status messages can be general, meaning that they apply to the full system, or they can apply to a specified active or standby server. General messages show in the yellow overview banner.

General Status Messages in Overview Banner	Description
	The database of the primary Security Management Server is identical with the database of the secondary.
Some servers could not be synchronized	A communication issue prevents synchronization, or some other synchronization issue exists.
	The active and standby servers are not communicating.
Communication Problem	Some services are down or cannot be reached.
Collision or HA conflict	More than one management server configured as active. Two active servers cannot sync with each other.

When connected to a specified *active* management server:

Status Window Area	Peer Status	Additional Information
Connected to:	Active	SmartConsole is connected to the active management server.
Peers	Standby	The peer is in standby. The message can also show: ■ Sync problem, last time sync ■ Synchronized successfully. Last sync time: <time> ■ No communication
	Not communicating, last sync time	
	Active	A state of collision exists between two servers both defined as active.

When connected to a specified *Standby* management server:

Status Window Area	Peer Status	Description
Connected to:	Standby	Also shows: last sync time.
Peers	Active	The peer is in standby. The message can also show: ■ No communication, last sync time ■ OK., last sync time: <time> ■ Sync problem, last sync time (in any direction)
	Standby *or* Unknown	Can also show: no communication.

Failover Between Active and Standby

Changeover between the primary (active) and secondary (standby) management server is not automatic. If the Active fails or it is necessary to change the Active to a Standby, you must do this manually. When the management server becomes Standby it becomes Read Only, and gets all changes from the new Active server.

Changing a Server to Active or Standby

The Active server synchronizes with the Standby server or servers at intervals, and when you publish the session. Sessions that are not published are not synchronized.

When the administrator initiates changeover, all public data is synchronized from the new Active to the new Standby server after the Standby becomes Active. Data from the new Active overrides the data on the new Standby. *Unpublished* changes are not synchronized.

Best Practice - We recommend that you publish changes before initiating a changeover to the Standby.

To Interchange the Active and Standby:

1. Open SmartConsole.
2. Connect to the Standby server.
3. On the Menu button, select **High Availability**.

   The **High Availability Status** window opens.
4. Use the **Action** buttons to change the Standby server to Active.

This changes the previous Active server to Standby.

High Availability Troubleshooting

These error messages show in the **High Availability Status** window when synchronization fails:

Not communicating

Solution:

1. Check connectivity between the servers.
2. Test SIC.

Collision or HA Conflict

More than one management server is configured as active.

Solution:

1. From the main SmartConsole menu, select **Management High Availability**.

   The **High Availability Status** window opens.
2. Use the **Actions** button to set one of the Active servers to Standby.

   Warning - When this server becomes the Standby, all its data is overwritten by the active server.

Sync Error

Solution: Do a manual sync.

For Multi-Domain Server

Synchronization

In a multi-domain environment, the Multi-Domain Servers work in active-active mode. All Mirror and Decrypt are active and synchronize each other.

The Domains managed by the Multi-Domain Server work in active-standby mode, where the Active Domain Server synchronizes all the standby Domain Servers.

The system automatically synchronizes periodically and when an administrator publishes changes to the configuration.

ICA Database Synchronization

When you create a new secondary Multi-Domain Server, the Internal Certificate Authority (ICA) on the Primary Multi-Domain Server generates a certificate when you establish SIC trust. The ICA can generate a certificate for a new administrator, if required by the authentication method. In a High Availability deployment with more than one Multi-Domain Server, the system synchronizes the ICA databases as necessary.

Uninstall Threat Policy

What can I do here?

Use this window to see candidates from which the threat policy can be removed.

Getting Here - Menu > Uninstall Threat Prevention Policy

Command Line - API

What can I do here?


Use this window to enter API commands or run API scripts.

Getting Here - Open command line window for management scripting - F9.

Understanding the API Server

If you do not see the command line window, make sure the startup settings and access settings for the API server are correctly configured in **Manage & Settings > Blades > Management API > Advanced Settings**.

API

You can configure and control the Management Server through API Requests you send to the API Server that runs on the Management Server.

The API Server runs scripts that automate daily tasks and integrate the Check Point solutions with third party systems, such as virtualization servers, ticketing systems, and change management systems.

To learn more about the management APIs, to see code samples, and to take advantage of user forums, see:

- The API Documentation:
  - Online - *Check Point Management API Reference* (at the top, select the correct version)
  - Local - `https://<Server IP Address>/api_docs`

    By default, access to the local API Documentation is disabled. Follow the instructions in sk174606.

    Note - On a Standalone server (a server which runs both a Security Management Server and a Security Gateway), the API Documentation web portal (`https://<Server IP Address>/api_docs`) stops working when you open SmartView Web Application (`https://<Server IP Address>/smartview`).
- The **Developers Network** section of *Check Point CheckMates Community*.

API Tools

You can use these tools to work with the API Server on the Management Server:

- Standalone management tool, included with Gaia operating system:

  `mgmt_cli`
- Standalone management tool, included with SmartConsole:

  `mgmt_cli.exe`

  You can copy this tool from the SmartConsole installation folder to other computers that run Windows operating system.
- Web Services APIs that allow communication and data exchange between the clients and the Management Server over the HTTP protocol.

  These APIs also let other Check Point processes communicate with the Management Server over the HTTPS protocol.

  `https://<IP Address of Management Server>/web_api/<command>`

Configuring the API Server

To configure the API Server:

1. Connect with SmartConsole to the Security Management Server or applicable Domain Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. In the upper left section, click **Blades**.
4. In the **Management API** section, click **Advanced Settings**.

The **Management API Settings** window opens.

5. Configure the **Startup Settings** and the **Access Settings**.

   Configuring Startup Settings

   Select **Automatic start** to automatically start the API server when you start or reboot the Management Server.

   Notes:
   - If the Management Server has more than 4GB of RAM installed, the **Automatic start** option is activated by default during Management Server installation.
   - If the Management Server has less than 4GB of RAM, the **Automatic Start** option is deactivated.

   Configuring Access Settings

   Select one of these options to configure which clients can connect to the API Server:

   - **Management server only** - Only the Management Server itself can connect to the API Server. This option only lets you use the `mgmt_cli` utility on the Management Server to send API requests. You cannot use SmartConsole or Web services to send API requests.
   - **All IP addresses that can be used for GUI clients** - You can send API requests from all IP addresses that are defined as **Trusted Clients** in SmartConsole. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.
   - **All IP addresses** - You can send API requests from all IP addresses. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.

6. Click **OK**.
7. In the upper left section, click **Permissions & Administrators**.
8. In the object of each applicable Administrator, make sure the assigned Permission Profile allows access to Management API.

   Instructions

   a. Edit the Administrator object.

   b. In the left panel, click **General**.

   c. In the **Permissions** section, on the right side of the selected Permission Profile, click the eye icon.

      The Permission Profile object opens in the read-only view.

   d. In the left panel, click **Management**.

e. The permission **Management API Login** has to be selected.

If it is not selected, then close this window and edit this Permission Profile object.

f. Click **Close**.

9. Publish the SmartConsole session.
10. Restart the API Server on the Management Server with this command:

```
api restart
```

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

- The output of this command must show:

```
API started successfully
```

11. Examine the status of the API server on the Management Server with this command:

```
api status
```

Notes:

- The output of this command must show:

```
-------------------------------------------
Overall API Status: Started
-------------------------------------------

API readiness test SUCCESSFUL. The server is up and ready
to receive connections
```

- The output this command may show the state of the "**API**" process as "**Stopped**" when the API access is set to "**All IP addresses that can be used for GUI clients**", and more than 200 Trusted Clients are configured:

```
Processes:

Name       State     PID       More Information
-----------------------------------------------
API        Stopped   ...
```

Where Used?

What can I do here?

Use this window to:

- See where and now the selected object is used in the database
- Change the way the object is used by replacing it with another object or policy from the database

Getting Here - Security Policies > Select object in Rule > Right-click > Where Used

Related Objects

What can I do here?

Use this window to view objects related to the validation error.

Getting Here - SmartConsole > Validation tab > Select a validation > right-click > Show Related Objects

Task Details

What can I do here?

Use this window to see a summary of task details.

Getting Here - SmartConsole connected to Multi-Domain Server or Security Management Server > Recent Tasks window > Details link

Task Details

What can I do here?

Use this window to see a summary of task details.

Getting Here - SmartConsole connected to Security Management Server or Multi-Domain Server > Recent Tasks window > Details link

Blade deactivated

What can I do here?

Use this window to leave feedback after deactivating a blade.

Getting Here - SmartConsole connected to Security Management Server or Multi-Domain Server > Recent Tasks window > Details link after deactivating blade.

Security Policies

Use the **Security Policies** View to configure:

- **Access Control**
- **Threat Prevention**
- **Shared Policies**
- **Manage layers**
- **Access the Application Wiki**
- **VPN Communities**
- **UserCheck**

Getting Here - SmartConsole > Security Policies

Access Control

What can I do here?

Use this window to define the Access Policy.

Getting Here - Security Policies > Access Control

Introducing the Unified Access Control Policy

Define one, unified Access Control Policy. The Access Control Policy lets you create a simple and granular Rule Base that combines all these Access Control features:

- Firewall - Control access to and from the internal network.
- Application Control and URL Filtering - Block applications and sites.
- Content Awareness - Restrict the Data Types that users can upload or download.
- IPsec VPN and Mobile Access - Configure secure communication with Site-to-Site and Remote Access VPNs.
- Identity Awareness - Identify users, computers, and networks.

There is no need to manage separate Rule Bases. For example, you can define one, intuitive rule that: Allows users in specified networks, to use a specified application, but prevents downloading files larger than a specified size. You can use all these objects in one rule:

- Security Zones
- Services
- Applications and URLs
- Data Types
- Access Roles

Information about these features is collected in one log:

- Network
- Protocol
- Application
- User
- Accessed resources
- Data Types

Creating a Basic Access Control Policy

A firewall controls access to computers, clients, servers, and applications using a set of rules that make up an Access Control Rule Base. You need to configure a Rule Base with secure Access Control and optimized network performance.

A strong Access Control Rule Base:

- Allows only authorized connections and prevents vulnerabilities in a network.
- Gives authorized users access to the correct internal resources.
- Efficiently inspects connections.

Basic Rules

Best Practice - These are basic Access Control rules we recommend for all Rule Bases:

- **Stealth rule** that prevents direct access to the Security Gateway
- **Cleanup rule** that drops all traffic that is not matched by the earlier rules in the policy

Note - If you delete the cleanup rule, there will still be an **implicit drop rule** that drops all traffic that did not match all other rules. This rule does not create log entries. If you want to log the traffic, create an **explicit Cleanup rule**.

Use Case - Basic Access Control

This use case shows a Rule Base for a simple Access Control Security Policy. (The **Hits**, **VPN** and **Content** columns are not shown.)

No	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Admin Access to Gateways	Admins (Access Role)	Gateways-group	Any	Accept	Log	Policy Targets
2	Stealth	Any	Gateways-group	Any	Drop	Alert	Policy Targets
3	Critical subnet	Internal	Finance HR R&D	Any	Accept	Log	CorpGW
4	Tech support	TechSupport	Remote1-web	HTTP	Accept	Alert	Remote1GW
5	DNS server	Any	DNS	Domain UDP	Accept	None	Policy Targets
6	Mail and Web servers	Any	DMZ	HTTP HTTPS SMTP	Accept	Log	Policy Targets
7	SMTP	Mail	NOT Internal net group	SMTP	Accept	Log	Policy Targets
8	DMZ & Internet	IntGroup	Any	Any	Accept	Log	Policy Targets
9	Cleanup rule	Any	Any	Any	Drop	Log	Policy Targets

Explanations:

Rule	Explanation
1	**Admin Access to Gateways** - SmartConsole administrators are allowed to connect to the Security Gateways.
2	**Stealth** - All internal traffic that is NOT from the SmartConsole administrators to one of the Security Gateways is dropped. When a connection matches the Stealth rule, an alert window opens in SmartView Monitor.

Rule	Explanation
3	**Critical subnet** - Traffic from the internal network to the specified resources is logged. This rule defines three subnets as critical resources: Finance, HR, and R&D.
4	**Tech support** - Allows the Technical Support server to access the Remote-1 web server which is behind the Remote-1 Security Gateway. Only HTTP traffic is allowed. When a packet matches the Tech support rule, the Alert action is done.
5	**DNS server** - Allows UDP traffic to the external DNS server. This traffic is not logged.
6	**Mail and Web servers** - Allows incoming traffic to the mail and web servers that are located in the DMZ. HTTP, HTTPS, and SMTP traffic is allowed.
7	**SMTP** - Allows outgoing SMTP connections to the mail server. Does not allow SMTP connections to the internal network, to protect against a compromised mail server.
8	**DMZ and Internet** - Allows traffic from the internal network to the DMZ and Internet.
9	**Cleanup rule** - Drops all traffic that does not match one of the earlier rules.

Use Case - Inline Layer for Each Department

This use case shows a basic Access Control Policy with a sub-policy for each department. The rules for each department are in an Inline Layer. An Inline Layer is independent of the rest of the Rule Base. You can delegate ownership of different Layers to different administrators.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
1	Critical subnet	Internal	Finance HR	Any	Any	Accept	Log
2	SMTP	Mail	NOT internal network (Group)	SMTP	Any	Accept	Log
3	R&D department	R&D Roles	Any	Any	Any	TechSupport Layer	N/A

No	Name	Source	Destination	Services & Applications	Content	Action	Track
3.1	R&D servers	Any	R&D servers (Group) QA network	Any	Any	Accept	Log
3.2	R&D source control	InternalZone	Source control servers (Group)	ssh, http, https	Any	Accept	Log
---	---	---	---	---	---	---	---
3.X	Cleanup rule	Any	Any	Any	Any	Drop	Log
4	QA department	QA network	Any	Any	Any	QA Layer	N/A
4.1	Allow access to R&D servers	Any	R&D Servers (Group)	Web Services	Any	Accept	Log
---	---	---	---	---	---	---	---
4.Y	Cleanup rule	Any	Any	Any	Any	Drop	Log
5	Allow all users to access employee portal	Any	Employee portal	Web Services	Any	Accept	None
---	---	---	---	---	---	---	---
9	Cleanup rule	Any	Any	Any	Any	Drop	Log

Explanations:

Rules	Explanation
1 2	General rules for the whole organization.
3 3.1 3.2 --- 3.X	An Inline Layer for the R&D department. Rule 3 is the parent rules of the Inline Layer. The **Action** is the name of the Inline Layer. **If a packet does not match on parent rule 3:** Matching continues to the next rule outside the Inline Layer (rule 4). **If a packet matches on parent rule 3:** Matching continues to 3.1, first rule inside the Inline Layer. If a packet matches on this rule, the rule action is done on the packet. If a packet does not match on rule 3.1, continue to the next rule inside the Inline Layer, rule 3.2. If there is no match, continue to the remaining rules in the Inline Layer. --- means one or more rules. The packet is matched only inside the inline layer. It never leaves the inline layer, because the inline layer has an implicit cleanup rule. It is not matched on rules 4, 5 and the other rules in the Policy Layer. Rule 3.X is a **cleanup rule**. It drops all traffic that does not match one of the earlier rules in the Inline Layer. This is a default explicit rule. You can change or delete it. **Best Practice** - Have an explicit cleanup rule as the last rule in each Inline Layer and Policy Layer.
4 4.1 --- 4.Y	Another Inline Layer, for the QA department.
5	More general rules for the whole organization.
--	One or more rules.
9	**Cleanup rule** - Drop all traffic that does not match one of the earlier rules in the Policy Layer. This is a default explicit rule. You can change or delete it. **Best Practice** - Have an explicit cleanup rule as the last rule in each Inline Layer and Policy Layer.

Configuring Site to Site VPN Rules in the Access Policy

You must configure rules to allow traffic to and from VPN Communities. Configure rules in SmartConsole > **Security Policies** > **Access Control**. All layers of the Access Control Policy can contain VPN rules.

To make a rule apply to a VPN Community, the **VPN** column of the Rule Base must contain one of these:

- **Any** - The rules applies to all VPN Communities and to non-VPN related traffic. If you configure a new VPN Community after the rule was created, the rule also applies to the new VPN Community.
- **One or more specified VPN communities** - For example, **MyIntranet**. Right-click in the VPN column of a rule and select **Specific VPN Communities**. The rule applies to the communities shown in the VPN column.

Examples:

- This rule allows encrypted traffic between domains of member gateways of "community_X."

Name	Source	Destination	VPN	Services & Applications
Allow traffic within community	*** Any**	***Any**	**MyCommunity**	*** Any**

- This rule allows traffic from all VPN Communities to the internal network on all services.

Name	Source	Destination	VPN	Services & Applications
Allow all VPN	*** Any**	**Internal_Network**	*** Any**	*** Any**

- This rule allows traffic between two VPN domains with all services.

Name	Source	Destination	VPN	Services & Applications
Site to Site VPN	**Local_VPN_Domain Peer_VPN_Domain**	**Local_VPN_Domain Peer_VPN_Domain**	**Site2Site**	*** Any**

Examples of Access Rules for Remote Access VPN

Examples:

This rule allows traffic from all VPN Communities to the internal network on all services:

Name	Source	Destination	VPN	Services & Applications
Allow all remote access	*** Any**	**Internal_Network**	*** Any**	*** Any**

This rule allows traffic from Remote Access VPN Community to the internal network on HTTP and HTTPS.

Name	Source	Destination	VPN	Services & Applications
Allow Remote Access community	*** Any**	**Internal_ Network**	**RemoteAccess**	**HTTP HTTPS**

This rule allows traffic from Remote Access VPN Community to the internal network on all services when the traffic starts from the Endpoint Security VPN client.

Name	Source	Destination	VPN	Services & Applications
Allow all from Endpoint Security VPN	**Endpoint Security VPN Access Role**	**Internal_ Network**	**RemoteAccess**	*** Any**

For details of how to create Access Roles for Remote Access and VPN Clients to include them in rules in the Access Control Rule Base, see *"Access Roles for Remote Access" on page 587*.

Creating Application Control and URL Filtering Rules

Create and manage the Policy for Application Control and URL Filtering in the Access Control Policy, in the **Access Control** view of SmartConsole. Application Control and URL Filtering rules define which users can use specified applications and sites from within your organization and what application and site usage is recorded in the logs.

To learn which applications and categories have a high risk, look through the **Application Wiki** in the **Access Tools** part of the **Security Policies** view. Find ideas for applications and categories to include in your Policy.

To see an overview of your Access Control Policy and traffic, see the **Access Control** view in **Logs & Monitor** > **New Tab** > **Views**.

Monitoring Applications

Scenario: I want to monitor all Facebook traffic in my organization. How can I do this?

To monitor all Facebook application traffic:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.

3. Click one of the **Add rule** toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
4. Create a rule that includes these components:
   - **Name** - Give the rule a name, such as **Monitor Facebook**.
   - **Source** - Keep it as **Any** so that it applies to all traffic from the organization.
   - **Destination** - Keep it as **Internet** so that it applies to all traffic going to the internet or DMZ.
   - **Services & Applications** - Click the plus sign to open the Application viewer. Add the **Facebook** application to the rule:
     - Start to type "face" in the Search field. In the Available list, see the **Facebook** application.
     - Click each item to see more details in the description pane.
     - Select items to add to the rule

     Note - Applications are matched by default on their **Recommended** services. Each service runs on a specific port. The recommended **Web Browsing Services** are `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`.
   - **Action** - Select **Accept**
   - **Track** - Select **Log**
   - **Install On** - Keep it as **Policy Targets** for or all gateways, or choose specific Security Gateways on which to install the rule

The rule allows all Facebook traffic but logs it. You can see the logs in the **Logs & Monitor** view, in the **Logs** tab. To monitor how people use Facebook in your organization, see the **Access Control** view (SmartEvent Server required).

Blocking Applications and Informing Users

Scenario: I want to block pornographic sites in my organization, and tell the user about the violation. How can I do this?

To block an application or category of applications and tell the user about the policy violation:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Create a rule that includes these components:

- **Services & Applications** - Select the **Pornography** category.
- **Action** - **Drop**, and a UserCheck **Blocked Message - Access Control**

  The message informs users that their actions are against company policy and can include a link to report if the website is included in an incorrect category.
- **Track** - **Log**

  Note - This Rule Base example contains only those columns that are applicable to this subject.

Name	Source	Destination	Services & Applications	Action	Track	Install On
Block Porn	Any	Internet	Pornography (category)	Drop Blocked Message	Log	Policy Targets

The rule blocks traffic to pornographic sites and logs attempts to access those sites. Users who violate the rule receive a UserCheck message that informs them that the application is blocked according to company Security Policy. The message can include a link to report if the website is included in an incorrect category.

Important - A rule that blocks traffic, with the **Source** and **Destination** parameters defined as **Any**, also blocks traffic to and from the Captive Portal.

Limiting Application Traffic

Scenario: I want to limit my employees' access to streaming media so that it does not impede business tasks.

If you do not want to block an application or category, there are different ways to set limits for employee access:

- Add a **Limit** object to a rule to limit the bandwidth that is permitted for the rule.
- Add one or more **Time** objects to a rule to make it active only during specified times.

The example rule below:

- Allows access to streaming media during non-peak business hours only.
- Limits the upload throughput for streaming media in the company to 1 Gbps.

To create a rule that allows streaming media with time and bandwidth limits:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.

3. Click one of the **Add Rule** toolbar buttons to add the rule in the position that you choose in the Rule Base.
4. Create a rule that includes these components:
   - **Services & Applications** - **Media Streams** category.

     Note - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this, see *"Services & Applications Column" on page 82*
   - **Action** - Click **More** and select **Action**: *Accept*, and a **Limit** object.
   - **Time** - Add a **Time** object that specifies the hours or time period in which the rule is active.

     Note - The **Time** column is not shown by default in the Rule Base table. To see it, right-click on the table header and select **Time**.

Name	Source	Destination	Services & Applications	Action	Track	Install On	Time
Limit Streaming Media	Any	Internet	Media Streams (Category)	Accept Upload_ 1Gbps	Log	All	Off-Work

Note - In ClusterXL Load Sharing modes, the specified bandwidth limit is divided between all defined cluster members, regardless of the cluster state. For example, if a rule sets 1Gbps limit in a cluster with three members, each member has a fixed limit of 333 Mbps.

Using Identity Awareness Features in Rules

Scenario: I want to allow a Remote Access application for a specified group of users and block the same application for other users. I also want to block other Remote Access applications for everyone. How can I do this?

If you enable Identity Awareness on a Security Gateway, you can use it together with Application Control to make rules that apply to an *access role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role **Identified_Users** that represents all identified users in the organization. You can use this to allow access to applications only for users who are identified on the Security Gateway.
- You want to allow access to the Radmin Remote Access tool for all identified users.

- You want to block all other Remote Access tools for everyone within your organization. You also want to block any other application that can establish remote connections or remote control.

To do this, add two new rules to the Rule Base:

1. Create a rule and include these components:
   - **Source** - The **Identified_Users** access role
   - **Destination** -**Internet**
   - **Services & Applications - Radmin**
   - **Action** -**Accept**
2. Create another rule below and include these components:
   - **Source - Any**
   - **Destination - Internet**
   - **Services & Applications** - The category: **Remote Administration**
   - **Action - Block**

Name	Source	Destination	Services & Applications	Action	Track	Install On
Allow Radmin to Identified Users	Identified_Users	Internet	Radmin	Allow	Log	All
Block other Remote Admins	Any	Internet	Remote Administration	Block	Log	All

Notes on these rules:

- Because the rule that allows Radmin is above the rule that blocks other Remote Administration tools, it is matched first.
- The Source of the first rule is the **Identified_Users** access role. If you use an access role that represents the Technical Support department, then only users from the technical support department are allowed to use Radmin.

- Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web browsing services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

For more about Access Roles and Identity Awareness, see the *R81.10 Identity Awareness Administration Guide*.

Blocking Sites

Scenario: I want to block sites that are associated with categories that can cause liability issues. Most of these categories exist in the Application and URL Filtering Database but there is also a custom defined site that must be included. How can I do this?

You can do this by creating a *custom group* and adding all applicable categories and the site to it. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an *access role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created
  - An Access Role that represents all identified users in the organization (*Identified_Users*).
  - A custom application for a site named *FreeMovies*.
- You want to block sites that can cause liability issues for everyone within your organization.
- You will create a custom group that includes Application and URL Filtering Database categories as well as the previously defined custom site named *FreeMovies*.

To create a custom group:

1. In the Object Explorer, click **New > More > Custom Application/Site > Application/Site Group**.
2. Give the group a name. For example, *Liability_Sites*.
3. Click **+** to add the group members:
   - Search for and add the custom application *FreeMovies*.
   - Select **Categories**, and add the ones you want to block (for example *Anonymizer*, *Critical Risk*, and *Gambling*)
   - Click **Close**.
4. Click **OK**.

You can now use the *Liability_Sites* group in the Access Control Rule Base.

In the Rule Base, add a rule similar to this:

In the Security Policies view of SmartConsole, go to the **Access Control** Policy.

- **Source** - The **Identified_Users** access role
- **Destination** -**Internet**
- **Services & Applications** - *Liability_Sites*
- **Action** -**Drop**

  Note - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

Name	Source	Destination	Services & Applications	Action	Track
Block sites that may cause a liability	Identified_ Users	Internet	Liability_Sites	Drop	Log

Blocking URL Categories

Scenario: I want to block pornographic sites. How can I do this?

You can do this by creating a rule that blocks all sites with pornographic material with the *Pornography category*. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an *Access role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role (*Identified_Users*) that represents all identified users in the organization.
- You want to block sites related to pornography.

The procedure is similar to *Blocking Applications and Informing Users*.

Scenario: I want to block pornographic sites in my organization, and tell the user about the violation. How can I do this?

To block an application or category of applications and tell the user about the policy violation:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.

3. Create a rule that includes these components:
   - **Services & Applications** - Select the **Pornography** category.
   - **Action** - **Drop**, and a UserCheck **Blocked Message - Access Control**

     The message informs users that their actions are against company policy and can include a link to report if the website is included in an incorrect category.
   - **Track** - **Log**

     Note - This Rule Base example contains only those columns that are applicable to this subject.

Name	Source	Destination	Services & Applications	Action	Track	Install On
Block Porn	Any	Internet	Pornography (category)	Drop Blocked Message	Log	Policy Targets

The rule blocks traffic to pornographic sites and logs attempts to access those sites. Users who violate the rule receive a UserCheck message that informs them that the application is blocked according to company Security Policy. The message can include a link to report if the website is included in an incorrect category.

Important - A rule that blocks traffic, with the **Source** and **Destination** parameters defined as **Any**, also blocks traffic to and from the Captive Portal.

In the Rule Base, add a rule similar to this:

- **Source** - The *Identified_Users* access role
- **Destination** - **Internet**
- **Services & Applications** - **Pornography** category
- **Action** - Drop

  Note - Categories are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

Policy Layers and Inline Layers

A policy is a set of rules that the gateway enforces on incoming and outgoing traffic. There are different policies for Access Control and for Threat Prevention.

You can organize the Access Control rules in more manageable subsets of rules using Policy Layers and Inline Layers.

The Need for Policy Layers and Inline Layers

Policy Layers and Inline Layers helps you manage your cyber security more efficiently. You can:

- Simplify the Rule Base, or organize parts of it for specific purposes.
- Organize the Policy into a hierarchy, using Inline Layers, rather than having a flat Rule Base.

  An Inline Layer is a *sub-policy* which is independent of the rest of the Rule Base.
- Reuse Policy Layers in multiple Policy packages, and reuse Inline Layers in multiple Layers.
- Simplify the management of the Policy by delegating ownership of different Layers to different administrators.
- Improve performance by reducing the number of rules in a Layer.

Order of Rule Enforcement in Inline Layers

The Policy Layer can contain Inline Layers.

This is an example of an Inline Layer:

No	Source	Destination	VPN	Services	Action
1					
2	Lab_network	Any	Any	Any	Lab_rules
2.1	Any	Any	Any	https http	Allow
2.2	Any	Any	Any	Any	Drop
3					

The Inline Layer has a parent rule (Rule 2 in the example), and sub rules (Rules 2.1 and 2.2). The Action of the parent rule is the name of the Inline Layer.

If the packet does not match the parent rule of the Inline Layer, the matching continues to the next rule of the Policy Layer (Rule 3).

If a packet matches the parent rule of the Inline Layer (Rule 2), the Firewall checks it against the sub rules:

- If the packet matches a sub rule in the Inline Layer (Rule 2.1), no more rule matching is done.

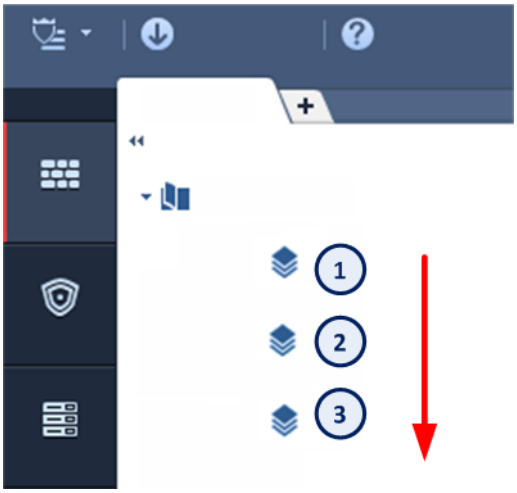
- If none of the higher rules in the Policy Layer match the packet, the explicit **Cleanup Rule** is applied (Rule 2.2). If this rule is missing, the **Implicit Cleanup Rule** is applied. No more rule matching is done.

Important - Always add an explicit **Cleanup Rule** at the end of each Inline Layer, and make sure that its **Action** is the same as the **Action** of the **Implicit Cleanup Rule**.

Order of Rule Enforcement in Policy Layers

When a packet arrives at the gateway, the gateway checks it against the rules in the first Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet.

If the **Action** of the matching rule is **Drop**, the gateway stops matching against later rules in the Policy Rule Base and drops the packet. If the **Action** is **Accept**, the gateway continues to check rules in the next Policy Layer.



Item	Description
1	Policy Layer 1
2	Policy Layer 2
3	Policy Layer 3

If none of the rules in the Policy Layer match the packet, the explicit **Default Cleanup Rule** is applied. If this rule is missing, the **Implicit Cleanup Rule** is applied.

Every Policy Layer has its own implicit cleanup rule. You can configure the rule to *Accept* or *Drop* in the Layer settings.

Important - Always add an explicit **Cleanup Rule** at the end of each Policy Layer, and make sure that its **Action** is the same as the **Action** of the **Implicit Cleanup Rule**.

Creating an Inline Layer

An Inline Layer is a *sub-policy* which is independent of the rest of the Rule Base.

The workflow for making an Inline Layer is:

1. Create a *parent* rule for the Inline Layer. Make a rule that has one or more properties that are the same for all the rules in the Inline Layer. For example, rules that have the same source, or service, or group of users.
2. Create *sub-rules* for the Inline Layer. These are rules that define in more detail what to do if the Firewall matches a connection to the parent rule. For example, each sub-rule can apply to specified hosts, or users, or services, or Data Types.

To create an Inline Layer:

1. Add a rule to the Policy Layer. This is the *parent* rule.
2. In the **Source**, **Destination**, **VPN**, and **Services & Applications** cells, define the match conditions for the Inline Layer.
3. Click the **Action** cell of the rule. Instead of selecting a standard action, select **Inline Layer** > **New Layer**.
4. The **Layer Editor** window opens.
5. Configure the properties of the Inline Layer:
   a. Enable one or more of these **Blades** for the rules of Inline Layer:
      - **Firewall**
      - **Application and URL Filtering**
      - **Content Awareness**
      - **Mobile Access**
   b. **Optional**: It is a best practice to share Layers with other Policy packages when possible.

      To enable this select **Multiple policies can use this layer**.
   c. Click **Advanced**.
   d. Configure the **Implicit Cleanup Rule** to *Drop* or *Accept*.
   e. Click **OK**.

   The name of the Inline Layer shows in the **Action** cell of the rule.
6. Under the parent rule of the Inline Layer, add *sub-rules*.
7. Make sure there is an explicit cleanup rule as the last rule of the Inline Layer.

Creating a Policy Layer

To create a Policy Layer:

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.
2. In the left pane, click **Layers**.

   You will see a list of the Layers. You can select **Show only shared Layers**.
3. Click the **New** icon in the upper toolbar.
4. Configure the settings in the **Layer Editor** window.
5. **Optional**: It is a best practice to share Layers with other Policy packages when possible. To enable this select **Multiple policies can use this layer**.
6. Click **OK**.
7. Click **Close**.
8. Publish the SmartConsole session

   This Policy Layer is not yet assigned to a Policy Package.

To add a Policy Layer to the Access Control Policy:

1. In SmartConsole, click **Security Policies**.
2. Right-click a Layer in the **Access Control Policy** section and select **Edit Policy**.

   The **Policy** window opens.
3. In the **Access Control** section, click the plus sign.

   You will see a list of the Layers that you can add. These are Layers that have **Multiple policies can use this layer** enabled.
4. Select the Layer.
5. Click **OK**.
6. Publish the SmartConsole session.

Pre-R80.10 Gateways: To create a Layer for URL Filtering and Application Control:

1. In SmartConsole, click **Security Policies**.
2. Right-click a Layer in the **Access Control Policy** section and select **Edit Policy**.

   The **Policy** window opens.
3. In the **Access Control** section, click the plus sign.

4. Click **New Layer**.

   The **Layer Editor** window opens and shows the **General** view.

5. Enable Application and URL Filtering on the Layer.

   a. Enter a name for the Layer.

      We recommend the name **Application**.

   b. In the **Blades** section, select **Application & URL Filtering**.

   c. Click **OK** and the **Layer Editor** window closes.

   d. Click **OK** and the **Policy** window closes.

6. Publish the SmartConsole session.

Enabling Access Control Features

Before creating the Access Control Policy, you must enable the Access Control features that you will use in the Policy.

Enable the features on the:

- Security Gateways on which you will install the Policy.
- Policy Layers and Inline Layers of the Policy. Here you can enable:
  - Firewall. This includes VPN.
  - Application & URL Filtering
  - Content Awareness
  - Mobile Access

Enabling Access Control Features on a Gateway

1. In SmartConsole, go to **Gateways & Servers** and double-click the gateway object.

   The **General Properties** window of the gateway opens.

2. From the navigation tree, click **General Properties**.

3. In the **Network Security** tab, select one or more of these Access Control features:

   - **IPsec VPN**
   - **Mobile Access**
   - **Application Control**
   - **URL Filtering**

- **Content Awareness**
- **Identity Awareness**

4. Click **OK**.

Enabling Access Control Features on a Layer

To enable the Access Control features on a Policy Layer:

1. In SmartConsole, click **Security Policies**.
2. Under **Access Control**, right-click **Policy** and select **Edit Policy**.
3. Click options  for the Layer.
4. Click **Edit Layer**.

   The **Layer Editor** window opens and shows the **General** view.
5. Enable the **Blades** that you will use in the Policy Layer:
   - **Firewall**.
   - **Application & URL Filtering**
   - **Content Awareness**
   - **Mobile Access**
6. Click **OK**.

To enable the Access Control features on an Inline Layer:

1. In SmartConsole, click **Security Policies**.
2. Select the Policy Layer.
3. In the parent rule of the Inline Layer, right-click the **Action** column, and select **Inline Layer** > **Edit Layer**.
4. Enable the **Blades** that you will use in the Inline Layer:
   - **Firewall**
   - **Application & URL Filtering**
   - **Content Awareness**
   - **Mobile Access**

   Note - Do not enable a Blade that is not enabled in the Policy Layer.
5. Click **OK**.

Types of Rules in the Rule Base

There are three types of rules in the Rule Base - **explicit**, **implied** and **implicit**.

Explicit rules

The rules that the administrator configures explicitly, to allow or to block traffic based on specified criteria.

Important - The **default Cleanup rule** is an explicit rule that is added by default to every new layer. You can change or delete the default Cleanup rule. We recommend that you have an explicit Cleanup rule as the last rule in each layer.

Implied rules

The default rules that are available as part of the **Global properties** configuration and cannot be edited. You can only select the implied rules and configure their position in the Rule Base:

- **First** - Applied first, before all other rules in the Rule Base - explicit or implied
- **Last** - Applied last, after all other rules in the Rule Base - explicit or implied, but before the **Implicit Cleanup Rule**
- **Before Last** - Applied before the last explicit rule in the Rule Base

Implied rules are configured to allow connections for different services that the Security Gateway uses. For example, the **Accept Control Connections** rules allow packets that control these services:

- Installation of the Security Policy on a Security Gateway
- Sending logs from a Security Gateway to the Security Management Server
- Connecting to third party application servers, such as RADIUS and TACACS authentication servers

Implicit cleanup rule

The default "catch-all" rule for the Layer that deals with traffic that does not match any explicit or implied rules in the Layer. It is made automatically when you create a Layer.

Implicit cleanup rules do not show in the Rule Base.

For Security Gateways R80.10 or later versions, the default implicit cleanup rule action is **Drop**. This is because most Policies have Whitelist rules (the Accept action). If the Layer has Blacklist rules (the Drop action), you can change the action of the implicit cleanup rule to **Accept** in the Layer Editor.

For Security Gateways R77.30 or earlier versions, the action of the implicit rule depends on the Policy Layer:

- **Drop** - for the **Network** Layer
- **Accept** - for a Layer with **Applications and URL Filtering** enabled

Note - If you change the default values, the policy installation will fail on R77.30 or earlier versions Security Gateways.

Order in which the Firewall Applies the Rules

1. **First Implied Rule** - No explicit rules can be placed before it.
2. **Explicit Rules** - These are the rules that you create.
3. **Before Last Implied Rules** - Applied before the last explicit rule.
4. **Last Explicit Rule** - We recommend that you use a **Cleanup rule** as the last explicit rule.

   Note - If you use the **Cleanup rule** as the last explicit rule, the **Last Implied Rule** and the **Implicit Cleanup Rule** are not enforced.
5. **Last Implied Rule** - Remember that although this rule is applied after all other explicit and implied rules, the Implicit Cleanup Rule is still applied last.
6. **Implicit Cleanup Rule** - The default rule that is applied if none of the rules in the Layer match.

Configuring the Implied Rules

Some of the implied rules are enabled by default. You can change the default configuration as necessary.

To configure the implied rules:

1. In SmartConsole, select the Access Control Policy.
2. From the toolbar above the policy, select **Actions** > **Implied Rules**.

   The **Implied Policy** window opens.
3. In the left pane, click **Configuration**.
4. Select a rule to enable it, or clear a rule to disable it.
5. For the enabled rules, select the position of the rules in the Rule Base: **First**, **Last**, or **Before Last**.
6. Click **OK**.
7. Install the policy.

Showing the Implied Rules

To see the implied rules:

In SmartConsole, from the **Security Policies** View, select **Actions** > **Implied Rules**.

The **Implied Policy** window opens.

It shows only the implied rules, not the explicit rules.

Configuring the Implicit Cleanup Rule

To configure the Implicit Cleanup Rule:

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.
2. In the left pane, click **Layers**.
3. Select a Layer and click **Edit**.

   The **Layer Editor** opens.
4. Click **Advanced**
5. Configure the **Implicit Cleanup Rule** to *Drop* or *Accept*.
6. Click **OK**.
7. Click **Close**.
8. Publish the SmartConsole session.

Administrators for Access Control Layers

You can create administrator accounts dedicated to the role of Access Control, with their own installation and SmartConsole Read/Write permissions.

You can also delegate ownership of different Layers to different administrators.

Sharing Layers

You may need to use the same rules in different parts of a Policy, or have the same rules in multiple Policy packages.

There is no need to create the rules multiple times. Define an Ordered Layer or an Inline Layer one time, and mark it as shared. You can then reuse the Inline Layer or Ordered layer in multiple policy packages or use the Inline Layer in multiple places in an Ordered Layer. This is useful, for example, if you are an administrator of a corporation and want to share some of the rules among multiple branches of the corporation:

- It saves time and prevents mistakes.
- To change a shared rule in all of the corporation's branches, you must only make the change once.

To mark a Layer as shared:

1. In SmartConsole, click **Menu** > **Manage policies and layers**.
2. In the left pane, click **Layers**.
3. Select a **Layer** in **Access Control** or in **Threat Prevention**.
4. Right-click and select **Edit Layer**.
5. Configure the settings in the **Layer Editor** window.
6. In **General**, select **Multiple policies and rules can use this layer**.
7. Click **OK**.
8. Click **Close**.
9. Publish the SmartConsole session.

To reuse a Threat Prevention Policy Layer:

1. In SmartConsole, go to **Menu** > **Manage policies and layers** > **Policies**.
2. Right-click the required policy and click **Edit**. The policy properties window opens.
3. In the Threat Prevention box, click the **+** sign.
4. Select the layer you want to include in this policy package.
5. Click **OK**.
6. Close the policy properties window.
7. In SmartConsole, install the policy.
8. Repeat this procedure for all policy packages.

For examples of Inline Layers and Policy Layer, see *"Unified Rule Base Use Cases" on page 89*

Visual Division of the Rule Base with Sections

To better manage a policy with a large number of rules, you can use **Sections** to divide the Rule Base into smaller, logical components. The division is only visual and does not make it possible to delegate administration of different **Sections** to different administrators.

Exporting Layer Rules to a .CSV File

You can export Layer rules to a .csv file. You can open and change the .csv file in a spreadsheet application such as Microsoft Excel.

To export Layer rules to a .csv file:

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.

   The **Manage Layers** window opens.
2. Click **Layers**.
3. Select a Layer, and then click **Actions** > **Export selected Layer**.
4. Enter a path and file name.

Managing Policies and Layers

To work with Policy Layers and Inline Layers in the Access Control Policy, select **Menu** > **Manage policies and layers** in SmartConsole.

The **Manage policies and layers** window shows.

To see the Layer in the policy package and their attributes:

In the **Layers** pane of the window, you can see:

- **Name** - Layer name
- **Number of Rules** - Number of rules in the Layer
- **Modifier** - The administrator who last changed the Layer configuration.
- **Last Modified** -Date the Layer was changed.
- **Show only Shared Layers** - A shared Layer has the **Multiple policies and rules can use this Layer** option selected.
- **Layer Details**

- **Used in policies** - Policy packages that use the Layer
- **Mode**:
  - **Ordered** - A Policy Layer. In a Multi-Domain Security Management environment, it includes global rules and a placeholder for local, Domain rules.
  - **Inline** - An Inline Layer, also known as a Sub-Policy.
  - **Not in use** - A Layer that is not used in a Policy package.

To see the rules in the Layer:

1. Select a Layer.
2. Right-click and select **Open layer in policy**.

Including Mobile Access in the Unified Policy

After you configure rules for Mobile Access in the Unified Access Control Policy, configure the gateway to use the **Unified Access Policy**.

To make an R80.x Mobile Access gateway use the Unified Access Control Policy:

1. In SmartConsole, Gateways & Servers, open a Mobile Access gateway object.
2. From the tree, select **Mobile Access**.
3. In the **Policy Source** area, select **Unified Access Policy**.
4. Install policy.

Configuring Mobile Access in the Unified Policy

- You can include Mobile Access rules in Policy Layers and Inline Layers. You must enable Mobile Access on each Layer that contains rule with Mobile Access applications.

  For more about layers, see the *R81.10 Security Management Administration Guide*
- To make a Mobile Access application show in the Mobile Access Portal or in Capsule Workspace, you must put the application in the **Services & Applications** column.
  - If you put **Any** in the **Services & Applications** column, the application does not show in the portal but it is allowed. You can open it from the Mobile Access Portal if you manually enter the URL, but not from Capsule Workspace. You can change this behavior. See sk112576 for details.

- If you put an application's service, such as HTTPS, in the **Services & Applications** column, it does not match Mobile Access https applications.

- In the **Services & Applications** column, you must use Mobile Access Application objects in rules to match Mobile Access traffic. You can define these applications in:
  - In SmartConsole: **Custom Applications/Sites** > **Mobile Applications**
  - In SmartConsole > **Mobile Access** tab > define an application

  Application objects defined for Application Control, for example, are not supported in Mobile Access rules.

- When you enable Mobile Access on a gateway, the gateway is automatically added to the **RemoteAccess** VPN Community. Include that Community in the **VPN** column of the rule or use **Any** to make the rule apply to Mobile Access gateways. If the gateway was removed from the VPN Community, the **VPN** column must contain **Any**.

- Use Access Roles as the **Source** or **Destination** for a rule to make the rule apply to specified users or networks. You can also use an Access Role to represent Mobile Access or other remote access clients.

  You must enable Identity Awareness on each gateway that is an installation target for rules with Access Roles.

Creating Mobile Access Rules in the Unified Access Control Policy

Create Mobile Access rules in the Access Control Policy with these requirements:

Column	Value	Explanation
No	Make sure that the rule position is logical.	The order of rules in the Rule Base is important. The first rule that matches the traffic is enforced.
Name	All	We recommend that you use a descriptive name.
Source	Access Role	Create an Access Role that includes the Users, User Groups, or Mobile/Remote Access Client that the rule applies to. See *"Access Roles for Remote Access" on page 587*.
Destination	The internal server on which the Mobile Access application is set.	Mobile Access Applications are defined in the **Services & Applications** column.

Column	Value	Explanation
VPN	**Any** or a Remote Access Community that includes the Mobile Access gateway	When you enable the Mobile Access or IPsec Software Blade on a gateway, the gateway is automatically added to the default **RemoteAccess** VPN Community. By default the community also contains a user group that contains all users. If you remove the gateway from the VPN Community, you must select **Any**.
Services & Applications	Mobile Applications Do not include applications or service objects that are not specified as Mobile Access.	To create a Mobile Application: Click + > click ✳ > **Mobile Applications** > select an application type and define it. To select an existing Mobile Application: Click + > ***All** > **Mobile Applications** and select one. Mobile Applications only show in the list if Mobile Access is enabled on the Layer
Content	**Any**	Content Awareness is not relevant for Mobile Access rules.
Action	**Accept** or **Drop**	Only **Accept** and **Drop** are supported. **Reject** is also supported but acts the same as **Drop**. You can also select **Inline Layer** to send all traffic that matches the rule to an Inline Layer under it.
Track	All log options	Right-click in the cell and select **More** > **Extended log**
Install On	One or more gateways	Each gateway must have Mobile Access and Identity Awareness enabled and have **Unified Access Policy** selected as the **Policy Source**.

Mobile Access Applications in the Unified Access Control policy

To use a Mobile Access application in the Unified Access Control Policy, you must define it as a **Mobile Application** from the SmartConsole or define it in the in SmartConsole > **Mobile Access** tab.

Other application objects, such as URL Filtering applications, are not relevant for Mobile Access. For example: To authorize Facebook as a web application in Mobile Access, you must create a new Web Application and specify Facebook's URL. You cannot use the URL Filtering Facebook application, because it is not for Mobile Access.

Creating Mobile Applications for the Access Control Policy

To create a Mobile Application object to use in the Access Control Policy:

1. In SmartConsole, expand the **Objects** pane.
2. Select **New** > **More** > **Custom Application/Site** > **Mobile Application**.
3. Select a type of Mobile Application.
4. Define the **General Properties** and **Authorized Locations**.
5. Optional: Define more settings for the Application.
6. Click **OK**.

The Columns of the Access Control Rule Base

These are the columns of the rules in the Access Control policy. Not all of these are shown by default. To select a column that does not show, right-click on the header of the Rule Base, and select it.

Column	Description
No	Rule number in the Rule Base Layer.
Hits	Number of times that connections match a rule.
Name	Name that the system administrator gives this rule.
Source **Destination**	Network objects that define ■ Where the traffic starts ■ The destination of the traffic.
VPN	The VPN Community to which the rule applies.
Services & Applications	Services, Applications, Categories, and Sites. If Application and URL Filtering is not enabled, only Services show.
Content	The data asset to protect, for example, credit card numbers or medical records. You can set the direction of the data to Download Traffic (into the organization), Upload Traffic (out of the organization), or Any Direction.
Action	Action that is done when traffic matches the rule. Options include: Accept, Drop, Ask, Inform (UserCheck message), Inline Layer, and Reject.
Track	Tracking and logging action that is done when traffic matches the rule.

Column	Description
Install On	Network objects that will get the rule(s) of the policy.
Time	Time period that this rule is enforced.
Comment	An optional field that lets you summarize the rule.

Source and Destination Column

In the Source and Destination columns of the Access Control Policy Rule Base, you can add Network objects including groups of all types. Here are some of the network objects you can include:

- Network
- Host
- Zones
- Dynamic Objects
- Domain Objects
- Access Roles
- Updatable Objects

VPN Column

You can configure rules for Site-to-Site VPN, Remote Access VPN, and the Mobile Access Portal and clients.

To make a rule for a VPN Community, add a Site-to-Site Community or a Remote Access VPN Community object to this column, or select **Any** to make the rule apply to all VPN Communities.

When you enable Mobile Access on a gateway, the gateway is automatically added to the **RemoteAccess** VPN Community. Include that Community in the **VPN** column of the rule or use **Any** to make the rule apply to Mobile Access gateways. If the gateway was removed from the VPN Community, the **VPN** column must contain **Any**.

IPsec VPN

The IPsec VPN solution lets the Security Gateway encrypt and decrypt traffic to and from other gateways and clients. Use SmartConsole to easily configure VPN connections between Security Gateways and remote devices.

For Site-to-Site Communities, you can configure Star and Mesh topologies for VPN networks, and include third-party gateways.

The VPN tunnel guarantees:

- Authenticity - Uses standard authentication methods
- Privacy - All VPN data is encrypted
- Integrity - Uses industry-standard integrity assurance methods

IKE and IPsec

The Check Point VPN solution uses these secure VPN protocols to manage encryption keys, and send encrypted packets. IKE (Internet Key Exchange) is a standard key management protocol that is used to create the VPN tunnels. IPsec is protocol that supports secure IP communications that are authenticated and encrypted on private or public networks.

Mobile Access to the Network

Check Point Mobile Access lets remote users easily and securely use the Internet to connect to internal networks. Remote users start a standard HTTPS request to the Mobile Access Security Gateway, and authenticate with one or more secure authentication methods.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet. Check Point Mobile Apps enable secure encrypted communication from unmanaged smartphones and tablets to your corporate resources. Access can include internal apps, email, calendar, and contacts.

To include access to Mobile Access applications in the Rule Base, include the **Mobile Application** in the **Services & Applications** column.

To give access to resources through specified remote access clients, create Access Roles for the clients and include them in the **Source** column of a rule.

To Learn More About VPN

To learn more about Site-to-Site VPN and Remote Access VPN, see these guides:

- *R81.10 Site to Site VPN Administration Guide*
- *R81.10 Remote Access VPN Administration Guide*
- *R81.10 Mobile Access Administration Guide*

Services & Applications Column

In the **Services & Applications** column of the Access Control Rule Base, define the applications, sites, and services that are included in the rule. A rule can contain one or more:

- Services
- Applications
- Mobile Applications for Mobile Access
- Web sites

- Default categories of Internet traffic
- Custom groups or categories that you create, that are not included in the Check Point Application and URL Filtering Database.

Service Matching

The Firewall identifies (*matches*) a service according to *IP protocol*, TCP and UDP *port number*, and *protocol signature*.

To make it possible for the Firewall to match services by protocol signature, you must enable **Applications and URL Filtering** on the Gateway and on the Policy Layer.

You can configure TCP and UDP services to be matched by *source port*.

Application Matching

If an application is *allowed* in the policy, the rule is matched only on the **Recommended** services of the application. This default setting is more secure than allowing the application on all services. For example: a rule that allows Facebook, allows it only on the Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`.

If an application is *blocked* in the policy, it is blocked on all services. It is therefore blocked on all ports.

You can change the default match settings for applications.

Configuring Matching for an Allowed Application

You can configure how a rule matches an application or category that is *allowed* in the policy. You can configure the rule to match the application in one of these ways:

- On any service
- On a specified service

To do this, change the **Match Settings** of the application or category. The application or category is changed everywhere that it is used in the policy.

To change the matched services for an allowed application or category:

1. In a rule which has applications or categories in the **Services & Applications** column, double-click an application or category.
2. Select **Match Settings**.
3. Select an option:
    - The default is **Recommended** services. The defaults for Web services are the Application Control **Web Browsing Services**.

- To match the application with all services, click **Any**.
- To match the application on specified services, click **Customize**, and add or remove services.
- To match the application with all services and exclude specified services, click **Customize**, add the services to exclude, and select **Negate**.

4. Click **OK**.

Configuring Matching for Blocked Applications

By default, if an application is *blocked* in the policy, it is blocked on all services. It is therefore blocked on all ports.

You can configure the matching for blocked applications so that they are matched on the recommended services. For Web applications, the recommended services are the *Application Control Web browsing services*.

If the match settings of the application are configured to **Customize**, the blocked application is matched on the customized services service. *It is not matched on all ports.*

To configure matching for blocked applications:

1. In SmartConsole, go to **Manage & Settings** > **Blades** > **Application and URL Filtering** > **Advanced Settings** > **Application Port Match**
2. Configure **Match application on Any port when used in Block rule**:
   - Selected - This is the default. If an application is *blocked* in the Rule Base, the application is matched to *Any* port.
   - Not selected - If an application is *blocked* in the Rule Base, the application is matched to the services that are configured in the application object of the application. However, some applications are still matched on Any. These are applications (Skype, for example) that do not limit themselves to a standard set of services.

Summary of Application Matching in a "Block" Rule

Application - Match Setting	Checkbox: Match web application on 'Any' port when used in 'Block' rule	Blocked Application is Matched on Service
Recommended services (default)	Selected (default)	Any
Recommended services (default)	Not selected	Recommended services
Customize	*Not relevant*	Customized

Application - Match Setting	Checkbox: Match web application on 'Any' port when used in 'Block' rule	Blocked Application is Matched on Service
Any	*Not relevant*	Any

Adding Services, Applications, and Sites to a rule

You can add services, applications and sites to a rule.

Note - Rules with applications or categories do not apply to connections from or to the Security Gateway.

To add services, applications or sites to a rule:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. To add applications to a rule, select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.
4. Search for the services, sites, applications, or categories.
5. Click the **+** next to the ones you want to add.

Creating Custom Applications, Categories, and Groups

You can create custom applications, categories or groups, which are not included in the Check Point Application and URL Filtering Database.

To create a new application or site:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.

   The Application viewer window opens.
4. Click **New > Custom Applications/Site** > **Application/Site**.
5. Enter a name for the object.
6. Enter one or more URLs.

   If you used a regular expression in the URL, click **URLs are defined as Regular Expressions**.

   Note - If the application or site URL is defined as a regular expression you must use the

correct syntax.

7. Click **OK**.

To create a custom category:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.

   The Application viewer window opens.
4. Click **New > Custom Applications/Site** > **User Category**.
5. Enter a name for the object.
6. Enter a description for the object.
7. Click **OK**.

Services and Applications on R80 and Lower Gateways, and after Upgrade

For R77.xx and lower Gateways:

- The Firewall matches TCP and UDP services by *port* number. The Firewall cannot match services by protocol signature.
- The Firewall matches applications by the application signature.

When you upgrade the Security Management Server and the Gateway to R80 and higher, this change of behavior occurs:

- Applications that were defined in the Application and URL Filtering Rule Base are accepted on their recommended ports

Content Column

You can add Data Types to the Content column of rules in the Access Control Policy.

To use the Content column, you must enable **Content Awareness**, in the General Properties page of the Security Gateway, and on the Layer.

A Data Type is a classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

You can set the direction of the data in the Policy to **Download Traffic** (into the organization), **Upload Traffic** (out of the organization), or **Any Direction**.

There are two kinds of Data Types: *Content Types* (classified by analyzing the file content) and *File Types* (classified by analyzing the file ID).

Content Type examples:

- PCI - credit card numbers
- HIPAA - Medical Records Number - MRN
- International Bank Account Numbers - IBAN
- Source Code - JAVA
- U.S. Social Security Numbers - According to SSA
- Salary Survey Terms

File type examples:

- Viewer File - PDF
- Executable file
- Database file
- Document file
- Presentation file
- Spreadsheet file

Note these limitations:

- Websocket content is not inspected.
- HTTP connections that are not RFC-compliant are not inspected.

To learn more about the Data Types, open the Data Type object in SmartConsole and press the **?** button (or **F1** key) to see the Help.

Note - Content Awareness and Data Loss Prevention (DLP) both use Data Types. However, they have different features and capabilities. They work independently, and the Security Gateway enforces them separately.

Actions

Action	Meaning
Accept	Accepts the traffic
Drop	Drops the traffic. The Firewall does not send a response to the originating end of the connection and the connection eventually does a time-out. If no UserCheck object is defined for this action, no page is displayed.
Ask	Asks the user a question and adds a confirmatory check box, or a reason box. Uses a UserCheck object.
Inform	Sends a message to the user attempting to access the application or the content. Uses a UserCheck object.

To see these actions, right-click and select More:

Action	Meaning
Reject	Rejects the traffic. The Firewall sends an RST packet to the originating end of the connection and the connection is closed.
UserCheck Frequency	Configure how often the user sees the configured message when the action is ask, inform, or block.
Confirm UserCheck	Select the action that triggers a UserCheck message: ■ **Per rule** - UserCheck message shows only once when traffic matches a rule. ■ **Per category** - UserCheck message shows for each matching category in a rule. ■ **Per application/Site** - UserCheck message shows for each matching application/site in a rule. ■ **Per Data type** - UserCheck message shows for each matching data type.
Limit	Limits the bandwidth that is permitted for a rule. Add a Limit object to configure a maximum throughput for uploads and downloads.
Enable Identity Captive Portal	Redirects HTTP traffic to an authentication (captive) portal. After the user is authenticated, new connections from this source are inspected without requiring authentication.

Important - A rule that drops traffic, with the **Source** and **Destination** parameters defined as **Any**, also drops traffic to and from the Captive Portal.

UserCheck Actions

UserCheck lets the Security Gateways send messages to users about possible non-compliant or dangerous Internet browsing. In the Access Control Policy, it works with URL Filtering, Application Control, and Content Awareness. (You can also use UserCheck in the Data Loss Prevention Policy, in SmartConsole). Create UserCheck objects and use them in the Rule Base, to communicate with the users. These actions use UserCheck objects:

- **Inform**
- **Ask**
- **Drop**

UserCheck on a Security Gateway

When UserCheck is enabled, the user's Internet browser shows the UserCheck messages in a new window.

You can enable UserCheck on Security Gateways that use:

- Access Control features:
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention features:
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
  - Threat Extraction
- Data Loss Prevention

UserCheck on a computer

The UserCheck client is installed on endpoint computers. This client:

- Sends messages for applications that are not based on Internet browsers, such as Skype and iTunes, and Internet browser add-ons and plug-ins.
- Shows a message on the computer when it cannot be shown in the Internet browser.

Tracking Column

These are some of the **Tracking** options:

- **None** - Do not generate a log.
- **Log** -This is the default **Track** option. It shows all the information that the Security Gateway used to match the connection.
- **Accounting** - Select this to update the log at 10 minute intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.

Unified Rule Base Use Cases

Here are some use cases that show examples of rules that you can define for the Access Control Policy.

Use Case - Application Control and Content Awareness Policy Layer

This use case shows an example unified Access Control Policy. It controls applications and content in one Policy Layer.

No	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
General compliance (1)								
1	Block categories	Any	Internet	Any	Anonymizer Critical Risk	Any	Drop Block Message	Log
Block risky executables (2)								
2	Block download of executable files from uncategorized and high risk sites	Internal Zone	Internet	Any	Uncategorized High Risk	Download Traffic Executable File	Drop	Log
redit card data (3-4)								
3	Allow uploading of credit cards numbers, by finance, and only over HTTPS	Finance (Access Role)	Web Servers	Any	https	Upload Traffic PCI - Credit Card Numbers	Accept	Log

No	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
4	Block other credit cards from company Web servers	Any	Web Servers	Any	Any	Any Direction PCI - Credit Card Numbers	Drop	Log
Inform about sensitive data over VPN (5)								
5	Inform the user about sensitive data from VPN sites	Any	Any	RemoteAccess	Any	Any Direction Salary Survey Report	Inform	Log
Cleanup (6)								
6	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log

Explanations:

Rule	Explanation
1	**General Compliance** section - Block access to unacceptable Web sites and applications.
2	**Block risky executables** section - Block downloading of high risk executable files.
3-4	**Credit card data** section - Allow uploading of credit cards numbers only by the finance department, and only over HTTPS. Block other credit cards.
5	**Block sensitive data over VPN** section - A remote user that connects over the organization's VPN sees an informational message.
6	**Cleanup rule** - Accept all traffic that does not match one of the earlier rules.

Use Case - Inline Layer for Web Traffic

This use case shows an example Access Control Policy that controls Web traffic. The Web server rules are in an Inline Layer.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
1	Headquarter WEB traffic - via proxy	HQ	Proxy	Web Proxy	Any	Ask Web Access Policy Access Noti... once a day per applic...	Log
2	Allow Proxy to the Internet	Proxy	Internet	Web	Any	Accept	None
3	Allow local branch to access the internet directly	Local Branch	Internet	Web	Any	Ask Web Access Policy Access Noti... once a day per applic...	Log
4	Web Servers	InternalZone	Web Servers	Web	Any	Web Servers protection	N/A

No	Name	Source	Destination	Services & Applications	Content	Action	Track
4.1	Block browsing with unapproved browsers	Any	Any	NEGATED Google Chrome Internet Explorer 11 Firefox Safari	Any	Drop	Log
4.2	Inform user when uploading Credit Cards only over HTTPS	Any	Any	https	Upload Traffic PCI - Credit Card Numbers	Inform Access Noti... once a day per applic...	Log
4.3	Block Credit Cards	Any	Any	Any	Any Direction PCI - Credit Card Numbers	Drop Block Message	Log
4.4	Block downloading of sensitive content	Any	Any	Any	Download Traffic HIPAA - Medical Record Headers	Drop	Log
4.5	Cleanup rule	Any	Any	Any	Any	Accept	None
5	Ask user when sending credit cards to PayPal	InternalZone	Internet	PayPal	Any Direction PCI - Credit Card Numbers	Ask Company Policy Access Noti... once a day per applic...	Log

No	Name	Source	Destination	Services & Applications	Content	Action	Track
6	Cleanup rule	Any	Any	Any	Any	Drop	Log

Explanations:

Rules	Explanation
4	This is the parent rule of the Inline Layer. The **Action** is the name of the Inline Layer. If a packet matches on the parent rule, the matching continues to rule 4.1 of the Inline Layer. If a packet does not match on the parent rule, the matching continues to rule 5.
4.1--4.4	If a packet matches on rule 4.1, the rule action is done on the packet, and no more rule matching is done. If a packet does not match on rule 4.1, continue to rule 4.2. The same logic applies to the remaining rules in the Inline Layer.
4.5	If none of the higher rules in the Policy Layer match the packet, the explicit *Cleanup Rule* is applied. The *Cleanup rule* is a default explicit rule. You can change or delete it. We recommend that you have an explicit cleanup rule as the last rule in each Inline Layer and Policy Layer.

Use Case - Content Awareness Policy Layer

This use case shows a Policy that controls the upload and download of data from and to the organization.

There is an explanation of some of the rules below the Rule Base.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
Regulatory compliance							
1	Block the download of executable files	InternalZone	Internet	Any	Download Traffic Executable file	Drop	Log

No	Name	Source	Destination	Services & Applications	Content	Action	Track
2	Allow uploading of credit cards numbers by finance users, only over HTTPS	Finance (Access Role)	Web Servers	https	Upload Traffic PCI - Credit Card Numbers	Accept	Log
3	Block other credit cards from company Web servers	InternalZone	Web Servers	Any	Any Direction PCI - Credit Card Numbers	Drop Block Message	Log
Personally Identifiable Information							
4	Matches U.S. Social Security Numbers (SSN) allocated by the U.S. Social Security Administration (SSA).	InternalZone	Internet	Any	Upload Traffic U.S. Social Security Numbers - According to SSA	Inform Access Notifi... once a day per applicati...	Log
5	Block downloading of sensitive medical information	InternalZone	Internet	Any	Download Traffic HIPAA - Medical Record Headers	Drop Block Message	Log
Human Resources							

No	Name	Source	Destination	Services & Applications	Content	Action	Track
6	Ask user when uploading documents containing salary survey reports.	InternalZone	Internet	Any	Upload Traffic Salary Survey Report	Ask Company Policy once a day per applicati...	Log
Intellectual Property							
7	Matches data containing source code	InternalZone	Internet	Any	Any Direction Source Code	Restrict source code	N/A
7.1		Any	Any	Any	Download Traffic Source Code	Accept	Log
7.2		Any	Any	Any	Upload Traffic Source Code	Ask Company Policy once a day per applicati...	Log
7.3	Cleanup Inline Layer	Any	Any	Any	Any	Drop Block Message	Log

Explanations:

Rule	Explanation
1-3	**Regulatory Compliance** section - Control the upload and download of executable files and credit cards. You can set the direction of the **Content**. In rule 1 it is **Download Traffic**, in rule 2 it is **Upload Traffic**, and in rule 3 it is **Any Direction**. Rule 1 controls executable files, which are File Types. The File Type rule is higher in the Rule Base than rules with Content Types (Rules 2 to 7). This improves the efficiency of the Rule Base, because File Types are matched sooner than Content Types.
4-5	**Personally Identifiable Information** section - Controls the upload and download of social security number and medical records. The rule Action for rule 4 is **Inform**. When an internal user uploads a file with a social security number, the user sees a message.
6	**Human resources** section - controls the sending of salary survey information outside of the organization. The rule action is **Ask**. If sensitive content is detected, the user must confirm that the upload complies with the organization's policy.
7	**Intellectual Property** section - A group of rules that control how source code leaves the organization. Rule 7 is the parent rule of an Inline Layer. The **Action** is the name of the Inline Layer. If a packet matches on rule 7.1, matching stops. If a packet does not match on rule 7.1, continue to rule 7.2. In a similar way, if there is no match, continue to 7.3. The matching stops on the last rule of the Inline Layer. We recommend that you have an explicit cleanup rule as the last rule in each Inline Layer

Use Case - Application and URL Filtering Policy Layer

This use case shows some examples of URL Filtering and Application Control rules for a typical policy that monitors and controls Internet browsing. (The **Hits, VPN** and **Install On** columns are not shown.)

No	Name	Source	Destination	Services & Applications	Action	Track	Time
1	Liability sites	Any	Internet	Potential liability (group)	Drop Blocked Message	Log	Any

No	Name	Source	Destination	Services & Applications	Action	Track	Time
2	High risk applications	Any	Internet	High Risk iTunes Anonymizer (category)	Drop Blocked Message	Log	Any
3	Allow IT department Remote Admin	IT (Access Role)	Any	Radmin	Allow	Log	Work-Hours
4	Allow Facebook for HR	HR (Access Role)	Internet	Facebook	Allow Download_1Gbps	Log	Any
5	Block these categories	Any	Internet	Streaming Media Protocols Social Networking P2P File Sharing Remote Administration	Drop Blocked Message	Log	Any
6	Log all applications	Any	Internet	Any	Allow	Log	Any

Explanations:

Rule	Explanation
1	**Liability sites** - Blocks traffic to sites and applications in the custom *Potential_liability* group. The UserCheck *Blocked Message* is shown to users and explains why their traffic is blocked.
2	**High risk applications** - Blocks traffic to sites and applications in the *High Risk* category and blocks the *iTunes* application. The UserCheck *Block Message* is shown to users and explains why their traffic is blocked.
3	**Allow IT department Remote Admin** - Allows the computers in the `IT` department network to use the *Radmin* application. Traffic that uses *Radmin* is allowed only during the *Work-Hours* (set to 8:00 through 18:30, for example).

Rule	Explanation
4	**Allow Facebook for HR** - Allows computers in the `HR` network to use *Facebook*. The total traffic downloaded from *Facebook* is limited to 1 Gbps, there is no upload limit.
5	**Block these categories** - Blocks traffic to these categories: *Streaming Media*, *Social Networking*, *P2P File Sharing*, and *Remote Administration*. The UserCheck *Blocked Message* is shown to users and explains why their traffic is blocked. **Note** - The *Remote Administration* category blocks traffic that uses the `Radmin` application. If this rule is placed before rule 3, then this rule can also block *Radmin* for the IT department.
6	**Log all applications** - Logs all traffic that matches any of the URL Filtering and Application Control categories.

Rule Matching in the Access Control Policy

The Firewall determines the rule to apply to a connection. This is called *matching* a connection. Understanding how the firewall matches connections will help you:

- Get better performance from the Rule Base.
- Understand the logs that show a matched connection.

Examples of Rule Matching

These example Rule Bases show how the Firewall matches connections.

Note that these Rule Bases intentionally do not follow *Best Practices for Access Control Rules*. This is to make the explanations of rule matching clearer.

Rule Base Matching - Example 1

For this Rule Base:

No	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	ftp-pasv	Download executable file	Drop
2	Any	Any	Any	Executable file	Accept
3	Any	Any	Gambling (Category)	Any	Drop
4	Any	Any	Any	Any	Accept

This is the matching procedure for an FTP connection:

Part of Connection	Firewall Action	Inspection Result
SYN	Run the Rule Base: Look for the first rule that matches: ■ Rule 1 - Match.	Final match (drop on rule 1). Shows in the log. The Firewall does not turn on the inspection engines for the other rules.

Rule Base Matching - Example 2

For this Rule Base:

No	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	Any	Download executable file	Drop
2	Any	Any	Gambling (category)	Any	Drop
3	Any	Any	ftp	Any	Drop
4	Any	Any	Any	Any	Accept

This is the matching procedure when browsing to a file sharing Web site. Follow the rows from top to bottom. Follow each row from left to right:

Part of Connection	Firewall Action	Inspection Result
SYN	Run the Rule Base. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - Possible match. ■ Rule 3 - No match. ■ Rule 4 - Match.	Possible match (Continue to inspect the connection).

Part of Connection	Firewall Action	Inspection Result
HTTP Header	The Firewall turns on inspection engines to examine the data in the connection. In this example turn on the: ■ URL Filtering engine - Is it a gambling site? ■ Content Awareness engine - Is it an executable file?	Application: File sharing (category). Content: Don't know yet.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - No match. ■ Rule 3 - No match. ■ Rule 4 - Match.	Possible match (Continue to inspect the connection).
HTTP Body	Examine the file.	Data: PDF file.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - No match. ■ Rule 2 - No match. ■ Rule 3 - No match. ■ Rule 4 - Match.	Final match (accept on rule 4). Shows in the log.

Rule Base Matching - Example 3

For this Rule Base:

No	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	Any	Download executable file	Drop
2	Any	Any	Gambling (Category)	Any	Drop
3	Any	Any	Any	Any	Accept

This is the matching procedure when downloading an executable file from a business Web site. Follow the rows from top to bottom. Follow each row from left to right:

Part of Connection	Firewall Action	Inspection Result
SYN	Run the Rule Base. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - Possible match. ■ Rule 3 - Match.	Possible match (Continue to inspect the connection).
HTTP Header	The Firewall turns on inspection engines to examine the content in the connection. In this example turn on the: ■ URL Filtering engine - is it a gambling site? ■ Content Awareness engine - Is it an executable file?	Application: Business (Category). Content: Don't know yet.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - Possible match. ■ Rule 2 - No match. ■ Rule 3 - Match.	Possible match (Continue to inspect the connection).
HTTP Body	Examine the file.	Content: Executable file.
	Optimize the Rule Base matching. Look for the first rule that matches: ■ Rule 1 - Match. ■ Rule 2 - No match. ■ Rule 3 - Match.	Final match (accept on rule 1). Shows in the log.

The matching examples show that:

- The Firewall sometimes runs the Rule Base more than one time. Each time it runs, the Firewall optimizes the matching, to find the first rule that applies to the connection.
- If the rule includes an application, or a site, or a service with a protocol signature (in the **Application and Services** column), or a Data Type (in the **Content** column), the Firewall:
  - Turns on one or more inspection engines.
  - Postpones making the final match decision until it has inspected the body of the connection.

- The Firewall searches for the first rule that applies to (*matches*) a connection. If the Firewall does not have all the information it needs to identify the matching rule, it continues to inspect the traffic.

Best Practices for Efficient Rule Matching

Recommendation	Reason
Place rules that check the source, destination, and port (network rules) higher in the Rule Base.	Network rules: ■ Are matched sooner. ■ Turn on fewer inspection engines.
Place rules that check applications and content (Data Types) below network rules. Do not define a rule with *Any* in the Source and in the Destination, and with an Application or a Data Type. For example these rules are not recommended: Source: *Any* | Destination: *Any*| Application: *Facebook* Or Source: *Any*| Destination: *Any*| Content: *Credit Card numbers* Instead, define these recommended rules: Source: *Any*| Destination: *Internet*| Application: *Facebook* Or Source: *Any*| Destination: *Server*| Content: *Credit Card numbers*	Application Control and Content Awareness rules require content inspection. Therefore, they: ■ Allow the connection until the Firewall has inspected connection header and body. ■ May affect performance.
For rules that check content (Data Types): Place rules that check File Types higher in the Rule Base than rules that check for Content Types.	File Types are matched sooner than Content Types.

Be sure to follow the other Best Practices for the Access Control Policies Rule Base.

Best Practices for Access Control Rules

1. Make sure you have these rules:
   - Stealth rule that prevents direct access to the Security Gateway
   - Cleanup rule that drops all traffic that is not allowed by the earlier rules in the policy.
2. Use Layers to add structure and hierarchy of rules in the Rule Base.

3. Add all rules that are based only on source and destination IP addresses and ports, in a Firewall/Network Policy Layer at the top of the Rule Base.
4. Create Firewall/Network rules to explicitly accept safe traffic, and add an explicit cleanup rule at the bottom of the Policy Layer to drop everything else.
5. Create an Application Control Policy Layer after the Firewall/Network Policy Layer. Add rules to explicitly drop unwanted or unsafe traffic. Add an explicit cleanup rule at the bottom of the Policy Layer to accept everything else.

   Alternatively, put Application Control rules in an Inline Layer as part of the Firewall/Network rules. In the parent rule of the Inline Layer, define the Source and Destination.
6. Share Ordered Layers and Inline Layers when possible.
7. For R80.10 Gateways and higher: If you have one Policy Layer for Firewall/Network rules, and another Policy Layer for Application Control - Add all rules that examine applications, Data Type, or Mobile Access elements, to the Application Control Policy Layer, or to a Policy Layer after it.
8. Turn off XFF inspection, unless the gateway is behind a proxy server. For more, see: sk92839.
9. Disable a rule when working on it. Enable the rule when you want to use it. Disabled rules do not affect the performance of the Gateway. To disable a rule, right-click in the **No** column of the rule and select **Disable**.

Best Practices for Efficient rule Matching

1. Place rules that check the source, destination, and port (network rules) higher in the Rule Base.

   Reason: Network rules are matched sooner, and turn on fewer inspection engines.
2. Place rules that check applications and content (Data Types) below network rules.
3. Do not define a rule with *Any* in the Source and in the Destination, and with an Application or a Data Type. For example these rules are not recommended:

Source	Destination	Services & Applications	Content
Any	Any	Facebook	
Any	Any		Credit Card numbers

   Instead, define one of these recommended rules:

Source	Destination	Services & Applications	Content
Any	Internet	Facebook	
Any	Server		Credit Card numbers

Reason for 2 and 3: Application Control and Content Awareness rules require content inspection. Therefore, they:

- Allow the connection until the Firewall has inspected connection header and body.
- May affect performance.

4. For rules with Data Types: Place rules that check File Types higher in the Rule Base than rules that check for Content Types.

   Reason: File Types are matched sooner than Content Types.

To see examples of some of these best practices, see the *"Unified Rule Base Use Cases" on page 89* and *"Creating a Basic Access Control Policy" on page 52*

Managing Pre-R80.10 Security Gateways

When you upgrade a pre-R80 Security Management Server that manages pre-R80.10 Security Gateways to R80 or higher, the existing Access Control policies are converted in this way:

- The pre-R80 **Firewall** policy is converted into the **Network** Policy Layer of the R80 Access Control Policy. The implicit cleanup rule for it is set to **Drop** all traffic that is not matched by any rule in this Layer.
- The pre-R80 **Application & URL Filtering** policy is converted into the **Application** Policy Layer, which is the second Layer of the R80 Access Control Policy. The implicit cleanup rule for it is set to **Accept** all traffic that is not matched by any rule in this Layer.

Important: After upgrade, do not change the **Action** of the implicit cleanup rules, or the order of the Policy Layers. If you do, the policy installation will fail.

New Access Control Policy for pre-R80 Security Gateways on an R80 Security Management Server must have this structure:

1. The first Policy Layer is the Network Layer (with the **Firewall** Software Blade enabled on it).
2. The second Policy Layer is the Application and URL Filtering Layer (with the **Application & URL Filtering** blade enabled on it).
3. There are no other Policy Layers.

If the Access Control Policy has a different structure, the policy will fail to install.

You can change the names of the Layers, for example, to make them more descriptive.

Each new Policy Layer will have the explicit default rule, added automatically and set to **Drop** all the traffic that does not match any rule in that Policy Layer. We recommend that the **Action** is set to **Drop** for the Network Policy Layer and **Accept** for the Application Control Policy Layer.

If you remove the default rule, the **Implicit Cleanup Rule** will be enforced. The **Implicit Cleanup Rule** is configured in the Policy configuration window and is not visible in the Rule Base table. Make sure the **Implicit Cleanup Rule** is configured to **Drop** the unmatched traffic for the Network Policy Layer and to **Accept** the unmatched traffic for the Application Control Policy Layer.

Analyzing the Rule Base Hit Count

Use the Hit Count feature to show the number of connections that each rule matches. Use the Hit Count data to:

- Analyze a Rule Base - You can delete rules that have no matching connection

  Note - If you see a rule with a zero Hit Count it only means that in the Security Gateways enabled with Hit Count there were no matching connections. There can be matching connections on other Security Gateways.

- Better understand the behavior of the Access Control Policy

You can show Hit Count for the rules in these options:

- The percentage of the rule hits from total hits
- The indicator level (very high, high, medium, low, or zero)

These options are configured in the Access Control Policy Rule Base and also changes how Hit Count is shown in other supported Software Blades.

When you enable Hit Count, the Security Management Server collects the data from supported Security Gateways (from version R75.40 and up). Hit Count works independently from logging and tracks the hits even if the **Track** option is **None**.

Enabling or Disabling Hit Count

By default, Hit Count is globally enabled for all supported Security Gateways (from R75.40). The timeframe setting that defines the data collection time range is configured globally. If necessary, you can disable Hit Count for one or more Security Gateways.

After you enable or disable Hit Count you must install the Policy for the Security Gateway to start or stop collecting data.

To enable or disable Hit Count globally:

1. In SmartConsole, click **Menu** > **Global properties**.
2. Select **Hit Count** from the tree.
3. Select the options:

- **Enable Hit Count** - Select to enable or clear to disable all Security Gateways to monitor the number of connections each rule matches.
- **Keep Hit Count data up to** - Select one of the time range options. The default is 3 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.

4. Click **OK**.
5. Install the Policy.

To enable or disable Hit Count on each Security Gateway:

1. From the **Gateway Properties** window for the Security Gateway, select **Hit Count** from the navigation tree.
2. Select **Enable Hit Count** to enable the feature or clear it to disable Hit Count.
3. Click **OK**.
4. Install the Policy.

Configuring the Hit Count Display

These are the options you can configure for how matched connection data is shown in the **Hits** column:

- **Value** - Shows the number of matched hits for the rule from supported Security Gateways. Connection hits are not accumulated in the total Hit Count for:
  - Security Gateways that are not supported
  - Security Gateways that have disabled the Hit Count feature

  The values are shown with these letter abbreviations:
  - K = 1,000
  - M = 1,000,000
  - G = 1,000,000,000
  - T = 1,000,000,000,000

  For example, 259K represents 259 thousand connections and 2M represents 2 million connections.
- **Percentage** -Shows the percentage of the number of matched hits for the rule from the total number of matched connections. The percentage is rounded to a tenth of a percent.
- **Level** -The Hit Count level is a label for the range of hits according to the table.

The Hit Count range = Maximum hit value - Minimum hit value (does not include zero hits)

Hit Count Level	Icon	Range
Zero		0 hits
Low		Less than 10 percent of the Hit Count range
Medium		Between 10 - 70 percent of the Hit Count range
High		Between 70 - 90 percent of the Hit Count range
Very High		Above 90 percent of the Hit Count range

To show the Hit Count in the Rule Base:

Right-click the heading row of the Rule Base and select **Hits**.

To configure the Hit Count in a rule:

1. Right-click the rule number of the rule.
2. Select **Hit Count** and one of these options (you can repeat this action to configure more options):
   - **Timeframe** - Select **All**, **1 day**, **7 days**, **1 month**, or **3 months**
   - **Display** - Select **Percentage**, **Value**, or **Level**

To update the Hit Count in a rule:

1. Right-click the rule number of the rule.
2. Select **Hit Count > Refresh**.

Searching a Rule Base

What can I do here?

Use this window to search the access control, NAT, or Threat Prevention Rule Base.

Getting Here - Security Policies > Access/NAT/Threat Prevention > Policy. Click inside the Rule Base search bar.

Rule Base Search

The search box looks for the query term in all columns of the Rule Base. For example, if the query term is "Check Point" , the search finds all rules that use this term. The results returned by the query are direct or indirect.

- **Direct** - The object in the query matches a rule
- **Indirect** - The object in the query matches a group inside a rule

You can also search the Rule Base using these predefined tokens:

Button Name	Text Name	Refers to an object in the:
Source	`src:`	Source column
Destination	`dst:`	Destination column
VPN	`vpn:`	VPN column
Services	`svc:`	Services and Applications column
Applications	`app:`	Services and Applications column
Install On	`installOn:`	Install On column
Action	`action:`	Action column
Track	`track:`	Track column

Note - These tokens are used for searching the access control policy. The NAT and Threat Prevention policies use different but similar ones.

To use a token in a search:

1. Enter a token in to the search bar
   - Click on a token button, for example **Source** or **Destination**.

     Suggestions for Source or Destination show.
   - Type the full name, for example **Source:** with a colon at the end.

     Suggestions for source show after typing the final colon (:)
   - Type the shortcut name, for example: src:

     Suggestions for source show after typing the final colon (:)

   A token can be written in any combination of upper and lower case letters.
2. Select one or more of the suggestions from the list.

The content name is appended to the token, for example: `src:DMZNet`.

3. Click the search icon or hit Enter.

Note - Typing the token name into the search box does not always produce the same results as selecting from the list. For example:

- `app:http` searches for words with an http prefix.
- Typing `app:` then selecting **http** from the list searches for exact matches on **http** . Objects selected from the list show in bold font.

IP Search

You can run an advanced search for an IP address, network, or port. It returns direct and indirect matches for your search criteria.

- IP address: xxx.xxx.xxx.xxx
- Network: xxx.xxx.0.0/16 or xxx.xxx
- Port: svc:<xxx>

These are the different IP search modes:

- **General ?** (Default). Returns direct matched results and indirect results in IP ranges, networks, groups, groups with exclusion, and rules that contain these objects.
- **Packet** ? Matches rules as if a packet with your IP address arrives at the gateway.

General IP Search

This is the default search mode. Use it to search in Rule Bases and in objects. If you enter a string that is not a valid IP or network, the search engine treats it as text.

When you enter a valid IP address or network, an advanced search is done and on these objects and rules:

- Objects that have the IP address as a text value for example, in a comment
- Objects that have an IP address property (direct results)
- Groups, networks, and address ranges that contain objects with the text value or address value
- Rules that contain those objects

Packet Search

A Packet Search matches rules as if a packet with your IP address arrives at the gateway. It matches rules that have:

- The IP address in a column of the rule
- "Any"
- A Group-with-exclusion or negated field with the IP address in its declaration

To run a Packet Search:

1. Click the search box.

   The search window opens.
2. Click **Packet** or enter: "mode:Packet"
3. To search a specific rule column, enter: *ColumnName:Criteria*

Rule Base Results

When you enter search criteria and view the matched results, the value that matched the criteria in a rule is highlighted.

If there is:	This is highlighted
A direct match on an object name or on textual columns	Only the specific matched characters
A direct match on object properties	The entire object name
A negated column	The negated label
A match on "Any"	"Any"

Known Limitation: Packet search does not support IPv6.

Using Boolean Operators in a Search Query

Use operators by typing them into the query in upper case format only. For example: "mycompany **OR** src: AuxiliaryNet".

If an operator is not used, the default AND operator applies. For example `app:http John` produces the same result as `app:http` **AND** `John`.

Query Examples:

- Drop AND dst: Gateways
- src:Alice AND dst:Bosa
- src:bob OR dst:Cellarix OR app:IKE
- src:bob AND (dst:Cellarix OR app:IKE)

- Alice OR Bob
- src:192.168.50.0

To stop a running query:

- Click the **X** button in the search box.
- Clear the search box and press enter.
- Start a new search. The new search overrides the previous one.

Query Examples

- Drop AND dst: Gateways
- src:Alice AND dst:Bosa
- src:bob OR dst:Cellarix OR app:IKE
- src:bob AND (dst:Cellarix OR app:IKE)
- Alice OR Bob
- src:192.168.50.0

Stopping a Running Query

1. Click the **X** button in the search box.
2. Clear the search box and press enter.
3. Start a new search. The new search overrides the previous one.

Keyboard Navigation

- Ctrl + F from the Rule Base focuses on the search box.
- Hitting Enter when the cursor is in the search runs a search.
- Up and down arrows navigate the list of suggestions.
- Hitting Enter while in the suggestions list selects the object and closes the list but does not run a search
- Hitting Escape while in the search box closes the list and returns focus to the Rule Base
- F3 (in the Rule Base or search box) navigates to the next result in a circular fashion
- Shift + F3 navigates previous results.

Go to Rule

Use this window to locate changed rules in the Rule Base.

If you have enabled the **Sessions Pane** in Manage & Settings > Preferences > Check Point Lab, a list of rules changed in the session shows in the pane.

Right-click a rule and select **Open** to find the rule the Rule Base or see a list of layers that use that rule.

Note - Publishing the session clears the pane of entries.

Getting Here - Gateways & Servers > Access Control > Policy > Session Pane > Click on rule in pane > Open

Implied Policy - Rules

What can I do here?

Use this window to see some of the implied rules. These rules apply to each layer in the Access Control Policy.

For a full list of implied rules, see: sk119497

Getting Here - Security Policies > Access Control > Actions > Implied Rules

Implied Policy - First Rules

What can I do here?

Use this window to see rules that are applied before each layer in the Access Control Policy.

Getting Here - Security Policies > Access Control > Actions > Implied Rules > First Rules

Implied Policy - Before last rules

What can I do here?

Use this window to see the implied rules that are applied before the last rule in each layer of the Access Control Policy.

Getting Here - Security Policies > Access Control > Actions > Implied Rules > Before Last Rules

Implied Policy - Last rules

What can I do here?

Use this window to see the last implied rules.

Getting Here - Security Policies > Access Control > Actions > Implied Rules > Last Rules

Implied Policy - Configuration

What can I do here?

Use this window to configure the implied rules. Select properties and position of the rules in the Rule Base.

Getting Here - Security Policies > Access Control > Actions > Implied Rules > Configuration

NAT Rule Base

What can I do here?

In this Rule Base you can configure manual network address translation (NAT) Rules, and examine all NAT rules, both manual and automatic.

Available NAT Methods

- Static
- Hide
- Carrier Grade Hide
- Stateful NAT 64
- Stateless NAT 46

Getting Here - Security Policies > Access Control > NAT

NAT

NAT can be defined *automatically* via the network object (Node, Network or Address Range). When you define NAT via the network object, rules are automatically added to the NAT Rule Base

You can *manually* specify NAT rules, by adding or editing NAT rules to the NAT Rule Base. You can specify the source, destination and service separately for the original and the translated packet.

Automatic NAT rules cannot be edited in the Rule Base.

NAT Rule Base Structure

The NAT Rule Base is divided into two sections. Each section in the NAT Rule Base Editor is divided into **Source** , **Destination** , and **Service** .

- The **Original Packet** section specifies the conditions when the rule is applied.
- The **Translated Packet** section specifies the *action* taken when the rule is applied.

The Rule Base *action* in NAT is always the same:

- Translate **Source** under **Original Packet**, to **Source**under **Translated Packet**.
- Translate **Destination**under **Original Packet**, to **Destination**under **Translated Packet**.
- Translate **Service**under **Original Packet**, to **Service**under **Translated Packet** .

Rule Base Operations

Operations that can be performed on the NAT Rule Base include:

- **Add** a network object to the cell.
- **Add (static)** adds a statically translated network object to the cell.
- **Add (Hide)**adds a Hide NAT translated network object to the cell.

NAT Rule Separator

- In the **Address Translation** tab of SmartConsole you can now add a **Section Title**above manually added rules or above the first automatic rule. You can not add a **Section Title** between the automatic rules.

Translating IP Addresses

NAT (Network Address Translation) is a feature of the Firewall Software Blade and replaces IPv4 and IPv6 addresses to add more security. You can enable NAT for all SmartConsole objects to help manage network traffic. NAT protects the identity of a network and does not show internal IP addresses to the Internet. You can also use NAT to supply more IPv4 addresses for the network.

The Firewall can change both the source and destination IP addresses in a packet. For example, when an internal computer sends a packet to an external computer, the Firewall translates the source IP address to a new one. The packet comes back from the external computer; the Firewall translates the new IP address back to the original IP address. The packet from the external computer goes to the correct internal computer.

SmartConsole gives you the flexibility to make necessary configurations for your network:

- Easily enable the Firewall to translate all traffic that goes to the internal network.
- SmartConsole can automatically create Static and Hide NAT rules that translate the applicable traffic.
- You can manually create NAT rules for different configurations and deployments.

How Security Gateways Translate Traffic

A Security Gateway can use these procedures to translate IP addresses in your network:

- **Static NAT** - Each internal IP address is translated to a different public IP address. The Firewall can allow external traffic to access internal resources.

  The configuration of static NAT on a *range* results in the translation of the IP addresses in the range into a *range of the same size, starting with the IP address specified.*

- **Hide NAT** - The Firewall uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the internal IP structure. Connections can only start from internal computers; external computers CANNOT access internal servers. The Firewall can translate up to 50,000 connections at the same time from external computers and servers.
- **Hide NAT with Port Translation** - Use one IP address and let external users access multiple application servers in a hidden network. The Firewall uses the requested service (or destination port) to send the traffic to the correct server. A typical configuration can use these ports: FTP server (port 21), SMTP server (port 25) and an HTTP server (port 80). It is necessary to create manual NAT rules to use Port Translation.

Using Hide NAT

For each SmartConsole object, you can configure the IP address that is used to translate addresses for Hide NAT mode:

- Use the IP address of the external Security Gateway interface
- Enter an IP address for the object

Hide NAT uses dynamically assigned port numbers to identify the original IP addresses. There are two pools of port numbers: 600 to 1023, and 10,000 to 60,000. Port numbers are usually assigned from the second pool. The first pool is used for these services:

- `rlogin` (destination port 512)
- `rshell` (destination port 513)
- `rexec` (destination port 514)

If the connection uses one of these services, and the source port number is below 1024, then a port number is assigned from the first pool.

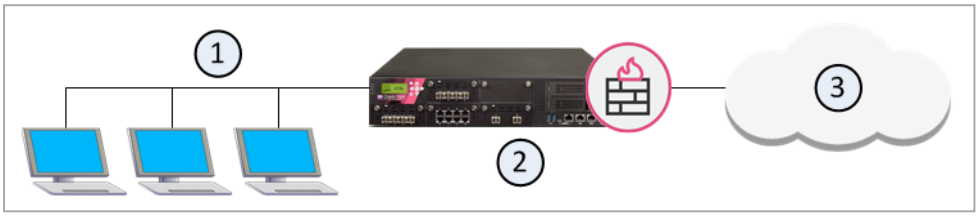
You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

Sample NAT Deployments

Static NAT

Firewalls that do Static NAT, translate each internal IP address to a different external IP address.

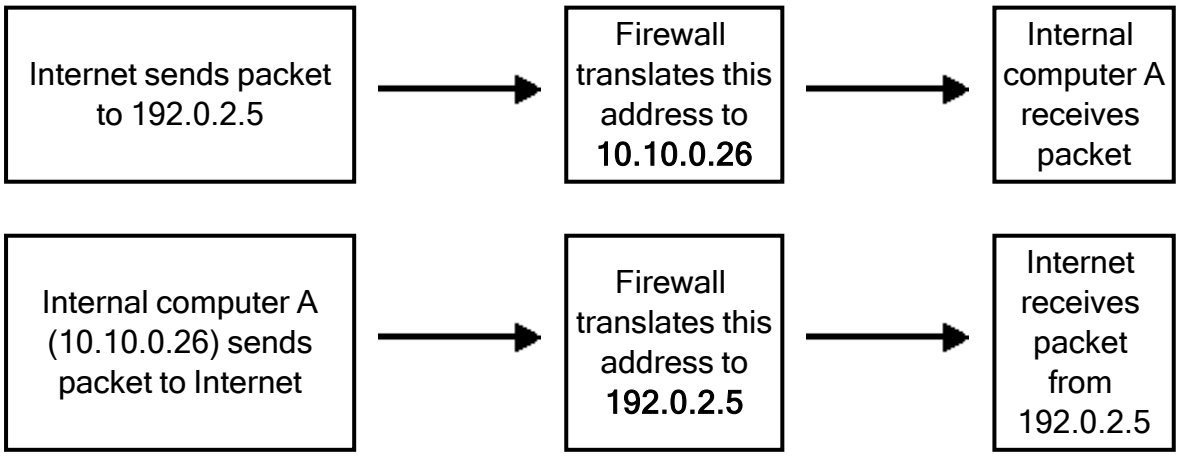


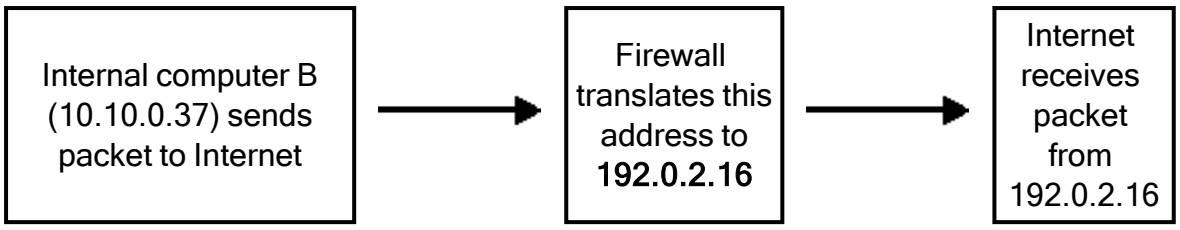
Item	Description
3	External computers and servers in the Internet
2	Security Gateway - Firewall is configured with Static NAT
1	Internal computers

Sample Static NAT Workflow

An external computer in the Internet sends a packet to 192.0.2.5. The Firewall translates the IP address to 10.10.0.26 and sends the packet to internal computer A. Internal computer A sends back a packet to the external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.5.

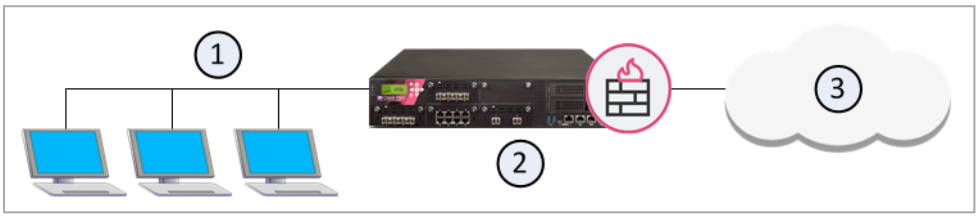
Internal computer B (10.10.0.37) sends a packet to an external computer. The Firewall intercepts the packet translates the source IP address to 192.0.2.16.





Hide NAT

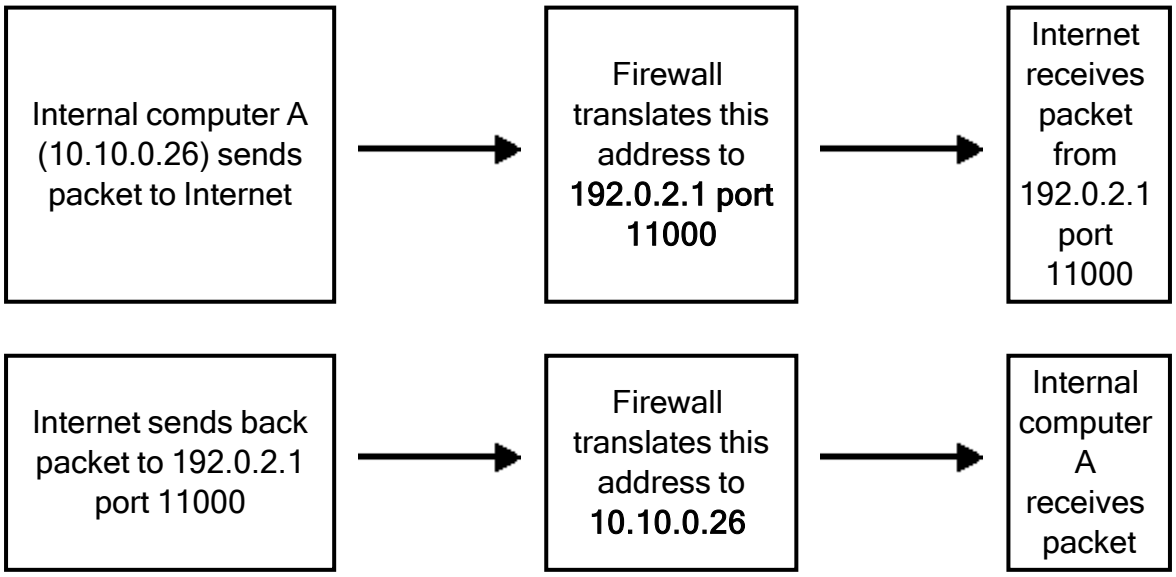
Firewalls that do Hide NAT use different port numbers to translate internal IP address to one external IP address. External computers cannot start a connection to an internal computer.



Item	Description
1	Internal computers
2	Security Gateway - Firewall is configured with Hide NAT
3	External computers and servers in the Internet

Sample Hide NAT Workflow

Internal computer A (10.10.0.26) sends a packet to an external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.1 port 11000. The external computer sends back a packet to 192.0.2.1 port 11000. The Firewall translates the packet to 10.10.0.26 and sends it to internal computer A.



NAT Rules

You can create Automatic NAT rules for these objects:

- Security Gateways
- Hosts
- Networks
- Address Ranges

The Management Server creates two Automatic NAT rules for Static NAT, to translate the source and the destination of the packets.

For Hide NAT, one rule translates the source of the packets.

For Network and Address Range objects, the Management Server creates a different rule to NOT translate intranet traffic. IP addresses for computers on the same object are not translated.

This table summarizes the Automatic NAT rules:

Type of Traffic	Automatic NAT - Static	Automatic NAT - Hide
Internal to external	Rule translates source IP address	Rule translates source IP address
External to internal	Rule translates destination IP address	N/A (External connections are not allowed)
Intranet (for network and address range objects)	Rule does not translate IP address	Rule does not translate IP address

Example of Automatic NAT Rules

Static NAT for a Network object

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for HR (1-3)								

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	HR	HR	Any	= Original	= Original	= Original	Policy Targets	
2	HR	Any	Any	S HR (Valid Address)	= Original	= Original	Policy Targets	
3	Any	HR (Valid Address)	Any	= Original	S HR	= Original	Policy Targets	

1. Intranet connections in the HR network are not translated.

   The Security Gateway does not translate a connection between two computers that are part of the HR object.

   The Security Gateway does not apply rules 2 and 3 to traffic that matches rule 1.

2. Connections from IP addresses from the HR network to any IP address (usually external computers) are translated to the Static NAT IP address.

3. Connections from any IP address (usually external computers) to the HR are translated to the Static NAT IP address.

Hide NAT for an Address Range object

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for Sales (1-2)								
1	Sales	Sales	Any	= Original	= Original	= Original	Policy Targets	

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
2	Sales	Any	Any	H Sales (Hiding Address)	= Original	= Original	Policy Targets	

1. Intranet connections in the Sales address range are not translated.

   The Firewall does not translate a connection between two computers that use IP addresses that are included in the Sales object.

   The Firewall does not apply rule 2 to traffic that matches rule 1.

2. Connections from IP addresses from the Sales address range to any IP address (usually external computers) are translated to the Hide NAT IP address.

Configuring Automatic NAT

Configure the NAT settings in each object, for which you need to create Automatic NAT rules, and configure the Access Control rules to allow traffic to the applicable objects.

Procedure

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.

   The **General Properties** window of the gateway opens.
3. From the navigation tree, select **NAT** > **Advanced**.
4. Select **Add automatic address translation rules to hide this Gateway behind another Gateway**.
5. Select the **Translation method**: **Hide** or **Static**.
6. Configure the NAT IP address for the object.
   - **Hide behind Gateway** - Uses the IP address of the corresponding Security Gateway's interface
   - **Hide behind IP address** - Enter the IP address.
7. Click **Install on Gateway** and select **All** or the Security Gateway that translates the IP address.
8. Click OK.
9. Install the Access Control Policy.

Example Deployment

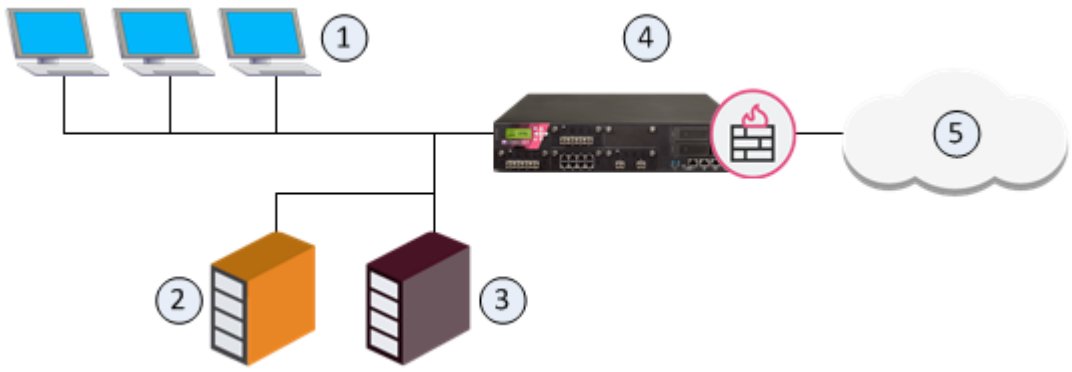
Example

The goal for this sample deployment is to configure:

- Static NAT for the EMail server and the Web server on the internal network.

  These servers can be accessed from the Internet using public addresses.
- Hide NAT for the users on the internal network that gives them Internet access.

  This network cannot be accessed from the Internet.



Item	Description
1	Internal computers (**Alaska_LAN**, IPv6 2001:db8::/64)
2	Web server (**Alaska_Web**, IPv6 2001:db8:0:10::5 is translated to IPv6 2001:db8:0:a::5)
3	Mail server (**Alaska_Mail**, IPv6 2001:db8:0:10::6 is translated to IPv6 2001:db8:0:a::6)
4	Security Gateway (**Alaska_GW**, external IPv6 2001:db8:0:a::1)
5	External computers and servers in the Internet

Configuration Procedure:

1. Configure Automatic Static NAT for the Web server:
    a. Double-click the **Alaska_Web** object.
    b. From the left, click **NAT**.
    c. Select **Add Automatic Address Translation Rules**.
    d. In **Translation method**, select **Static**.
    e. Select **Hide behind IP Address** and enter **2001:db8:0:a::5**.
    f. Click **OK**
2. Enable Automatic Static NAT for the EMail server:
    a. Double-click the **Alaska_Mail** object.
    b. From the left, click **NAT**.
    c. Select **Add Automatic Address Translation Rules**.

d. In **Translation method**, select **Static**.

e. Select **Hide behind IP Address** and enter **2001:db8:0:a::6**.

f. Click **OK**.

3. Enable Automatic Hide NAT for the internal computers:

a. Double-click the **Alaska_LAN** object.

b. From the left, click **NAT**.

c. Select **Add Automatic Address Translation Rules**.

d. In **Translation method**, select **Hide**.

e. Select **Hide behind Gateway**.

4. Click **OK**.

5. Install the Access Control Policy.

The Management Server creates these Automatic NAT rules in **Security Policies** view > **Access Control** > **NAT**:

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for Sales (1-2)								
1	Alaska_Web	Alaska_Web	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_Web	Any	Any	S Alaska_Web (Valid Address)	= Original	= Original	Policy Targets	

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
3	Any	Alaska_Web	Any	= Original	S Alaska_Web (Valid Address)	= Original	Policy Targets	
4	Alaska_Mail	Alaska_Mail	Any	= Original	= Original	= Original	Policy Targets	
5	Alaska_Mail	Any	Any	S Alaska_Mail (Valid Address)	= Original	= Original	Policy Targets	
6	Any	Alaska_Mail	Any	= Original	S Alaska_Mail (Valid Address)	= Original	Policy Targets	
7	Alaska_LAN	Alaska_LAN	Any	= Original	= Original	= Original	Policy Targets	
8	Alaska_LAN	Any	Any	H Alaska_LAN (Hiding Address)	= Original	= Original	Policy Targets	

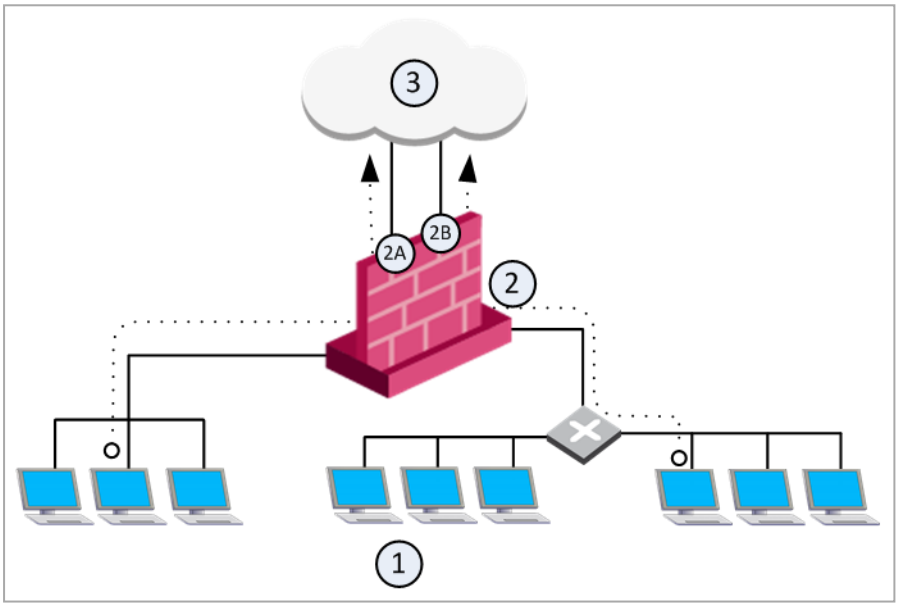
Automatic Hide NAT to External Networks

For large and complex networks, it can be impractical to configure the Hide NAT settings for all the internal IP addresses.

Explanation

An easy alternative is to enable a Security Gateway to automatically Hide NAT for all traffic with external networks. The Security Gateway translates all traffic that goes through an external interface to the valid IP address of that interface.

In this sample configuration, computers in internal networks open connections to external servers on the Internet. The source IP addresses of internal clients are translated to the IP address of an external interface.



Item	Description
1	Internal networks
2	Security Gateway is configured with Automatic Hide NAT.
2A and 2B	Two external interfaces 192.0.2.1 and 192.0.2.100.
1 -->3	External computers and servers on the Internet

Source IP addresses are translated to the applicable external interface IP address: **192.0.2.1** or **192.0.2.100**.

Note - If a connection matches a regular NAT rule and a NAT-for-internal-networks rule, the regular NAT rule takes precedence.

To enable Automatic Hide NAT:

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.
3. From the navigation tree, click **NAT**.
4. Select **Hide internal networks behind the Gateway's external IP**.
5. Click **OK**.
6. Install the Access Control Policy.

Note - When you enable this option, no rule is added to the NAT Rule Base. You can see the NAT activity in the Firewall logs.

For some deployments, it is necessary to manually define the NAT rules.

For example:

- Rules that are restricted to specific destination IP addresses and to specific source IP addresses
- Translating both source and destination IP addresses in the same packet.
- Static NAT in only one direction
- Translating services (destination ports)
- Rules that only use specified services (ports)
- Translating IP addresses for dynamic objects

General workflow when working with manual NAT rules:

1. Create SmartConsole objects that use the **valid** (NATed) IP addresses.
2. Create Manual NAT rules to translate the original IP addresses of the objects to valid IP addresses.
3. Configure the Access Control Policy to allow traffic to the applicable translated objects with the valid IP addresses.

Note - For Manual NAT rules, it is necessary to configure Proxy ARP entries to associate the translated IP address. See *Automatic and Proxy ARP*.

Example of a Manual NAT Rule

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	HTTP_Client	Web_Server	http	= Original	Web_Server	= Original	Policy Targets	

Configuring Manual NAT

Procedure

1. From the left navigation panel, click **Security Policies**.
2. Click **Access Control** > **NAT**.
3. Add a new rule in one of these ways:
   - From the top toolbar, click the **Add Rule** icon (the leftmost icon).
   - If there are existing Manual NAT rules, then right-click in the **No.** column of the applicable rule > in the line **New Rule**, click **Above** or **Below**.
4. In the new rule, select the required objects and configure the required translation.

   If the required objects do not exist, you can create them in the selection window (in the top right corner, click **New**).
5. Install the Access Control Policy.

Configuring Hide NAT behind Address Range

By default, when an administrator configures a Hide NAT rule and in the **Translated Source** column selects an Address Range object, the Security Gateway selects a Hide IP address from this range based only on the connection's source IP address.

Starting from R81.10 Jumbo Hotfix Accumulator Take 131, you can configure the Security Gateway to select a Hide IP address from the configured range based on the connection's source IP address and source port:

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Enable the corresponding kernel parameter. Run:

   ```
   fw ctl set -f int fwx_hide_range_with_port 1
   ```
3. Reboot the Security Gateway / each Cluster Member.

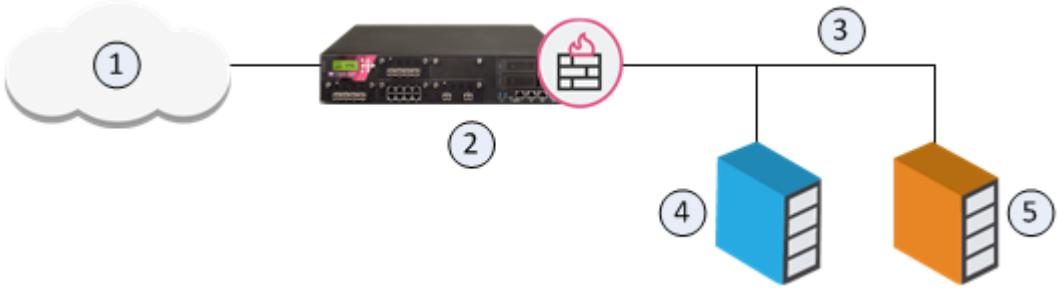
   Note - In a cluster, this can cause a failover.

Example Deployment

Example

This example configuration shows how to let external computers access an internal web server and an internal mail server in a DMZ network from one IP address.

To do this, you must configure Hide NAT for the DMZ network object and create manual NAT rules for the servers.



Item	Description
1	External computers and servers on the Internet
2	Security Gateway (**Alaska_GW**, external IPv6 2001:db8:0:c::1)
3	DMZ network (**Alaska_DMZ**, IPv6 2001:db8:a::/128)
4	Web server (**Alaska_DMZ_Web**, IPv6 2001:db8:a::35:5 is translated to IPv6 2001:db8:0:c::1)
5	Mail server (**Alaska_DMZ_Mail**, IPv6 2001:db8:a::35:6 is translated to IPv6 2001:db8:0:c::1)

Configuration Procedure:

1. Configure Automatic Hide NAT for the DMZ network:
   a. Double-click the Network object **Alaska_DMZ**.
   b. From the left, click **NAT**.
   c. Select **Add Automatic Address Translation Rules**.
   d. In **Translation method**, select **Hide**.
   e. Select **Hide behind Gateway**.
   f. Click **OK**.

   The Management Server creates these Automatic NAT rules in **Security Policies** view > **Access Control** > **NAT**:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	= Original	= Original	Policy Targets	

2. Create a Manual NAT rule to translate incoming HTTP traffic to the internal Web server:

a. In SmartConsole, go to **Security Policies** view > **Access Control** > **NAT**.

b. Add a new rule (#3) below the existing Automatic NAT rules.

c. Select these objects:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	= Original	= Original	Policy Targets	
3	Any	Alaska_GW	http	= Original	S Alaska_DMZ_Web	= Original	Policy Targets	

3. Create a Manual NAT rule to translate incoming SMTP traffic to the internal Mail server:

a. Add a new rule (#4) below the existing NAT rules.

b. Select these objects:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	= Original	= Original	Policy Targets	
3	Any	Alaska_GW	http	= Original	S Alaska_DMZ_Web	= Original	Policy Targets	
4	Any	Alaska_GW	smtp	= Original	S Alaska_DMZ_Mail	= Original	Policy Targets	

4. Create an Access Control rule to allow the incoming HTTP and SMTP traffic to the internal servers:

a. In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.

b. Add a new rule.

c. Select these objects:

No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
...	Incoming HTTP and SMTP traffic to internal servers	Any	Alaska_DMZ	Any	http smtp	Accept	Log	Policy Targets

5. Install the Access Control Policy.

Working with Automatic NAT Rules

You can create Automatic NAT rules for these objects:

- Security Gateways
- Hosts
- Networks
- Address Ranges

The Management Server creates two Automatic NAT rules for Static NAT, to translate the source and the destination of the packets.

For Hide NAT, one rule translates the source of the packets.

For Network and Address Range objects, the Management Server creates a different rule to NOT translate intranet traffic. IP addresses for computers on the same object are not translated.

This table summarizes the Automatic NAT rules:

Type of Traffic	Automatic NAT - Static	Automatic NAT - Hide
Internal to external	Rule translates source IP address	Rule translates source IP address
External to internal	Rule translates destination IP address	N/A (External connections are not allowed)
Intranet (for network and address range objects)	Rule does not translate IP address	Rule does not translate IP address

Example of Automatic NAT Rules

Static NAT for a Network object

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for HR (1-3)								
1	HR	HR	Any	= Original	= Original	= Original	Policy Targets	
2	HR	Any	Any	S HR (Valid Address)	= Original	= Original	Policy Targets	
3	Any	HR (Valid Address)	Any	= Original	S HR	= Original	Policy Targets	

1. Intranet connections in the HR network are not translated.

   The Security Gateway does not translate a connection between two computers that are part of the HR object.

   The Security Gateway does not apply rules 2 and 3 to traffic that matches rule 1.

2. Connections from IP addresses from the HR network to any IP address (usually external computers) are translated to the Static NAT IP address.
3. Connections from any IP address (usually external computers) to the HR are translated to the Static NAT IP address.

Hide NAT for an Address Range object

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for Sales (1-2)								
1	Sales	Sales	Any	= Original	= Original	= Original	Policy Targets	
2	Sales	Any	Any	$_H$ Sales (Hiding Address)	= Original	= Original	Policy Targets	

1. Intranet connections in the Sales address range are not translated.

   The Firewall does not translate a connection between two computers that use IP addresses that are included in the Sales object.

   The Firewall does not apply rule 2 to traffic that matches rule 1.
2. Connections from IP addresses from the Sales address range to any IP address (usually external computers) are translated to the Hide NAT IP address.

Configuring Automatic NAT

Configure the NAT settings in each object, for which you need to create Automatic NAT rules, and configure the Access Control rules to allow traffic to the applicable objects.

Procedure

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.

   The **General Properties** window of the gateway opens.
3. From the navigation tree, select **NAT** > **Advanced**.
4. Select **Add automatic address translation rules to hide this Gateway behind another Gateway**.
5. Select the **Translation method**: **Hide** or **Static**.
6. Configure the NAT IP address for the object.
   - **Hide behind Gateway** - Uses the IP address of the corresponding Security Gateway's interface
   - **Hide behind IP address** - Enter the IP address.
7. Click **Install on Gateway** and select **All** or the Security Gateway that translates the IP address.
8. Click OK.
9. Install the Access Control Policy.

Example Deployment

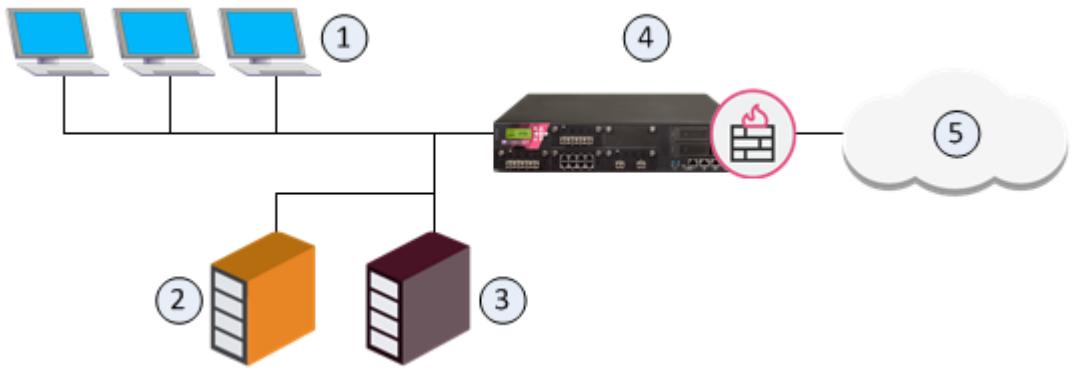
Example

The goal for this sample deployment is to configure:

- Static NAT for the EMail server and the Web server on the internal network.

  These servers can be accessed from the Internet using public addresses.
- Hide NAT for the users on the internal network that gives them Internet access.

  This network cannot be accessed from the Internet.



Item	Description
1	Internal computers (**Alaska_LAN**, IPv6 2001:db8::/64)
2	Web server (**Alaska_Web**, IPv6 2001:db8:0:10::5 is translated to IPv6 2001:db8:0:a::5)
3	Mail server (**Alaska_Mail**, IPv6 2001:db8:0:10::6 is translated to IPv6 2001:db8:0:a::6)
4	Security Gateway (**Alaska_GW**, external IPv6 2001:db8:0:a::1)
5	External computers and servers in the Internet

Configuration Procedure:

1. Configure Automatic Static NAT for the Web server:
    a. Double-click the **Alaska_Web** object.
    b. From the left, click **NAT**.
    c. Select **Add Automatic Address Translation Rules**.
    d. In **Translation method**, select **Static**.
    e. Select **Hide behind IP Address** and enter **2001:db8:0:a::5**.
    f. Click **OK**
2. Enable Automatic Static NAT for the EMail server:
    a. Double-click the **Alaska_Mail** object.
    b. From the left, click **NAT**.
    c. Select **Add Automatic Address Translation Rules**.

d. In **Translation method**, select **Static**.

e. Select **Hide behind IP Address** and enter **2001:db8:0:a::6**.

f. Click **OK**.

3. Enable Automatic Hide NAT for the internal computers:

a. Double-click the **Alaska_LAN** object.

b. From the left, click **NAT**.

c. Select **Add Automatic Address Translation Rules**.

d. In **Translation method**, select **Hide**.

e. Select **Hide behind Gateway**.

4. Click **OK**.

5. Install the Access Control Policy.

The Management Server creates these Automatic NAT rules in **Security Policies** view > **Access Control** > **NAT**:

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Automatic Generated Rules								
NAT Rules for Sales (1-2)								
1	Alaska_Web	Alaska_Web	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_Web	Any	Any	S Alaska_Web (Valid Address)	= Original	= Original	Policy Targets	

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
3	Any	Alaska_Web	Any	= Original	S Alaska_Web (Valid Address)	= Original	Policy Targets	
4	Alaska_Mail	Alaska_Mail	Any	= Original	= Original	= Original	Policy Targets	
5	Alaska_Mail	Any	Any	S Alaska_Mail (Valid Address)	= Original	= Original	Policy Targets	
6	Any	Alaska_Mail	Any	= Original	S Alaska_Mail (Valid Address)	= Original	Policy Targets	
7	Alaska_LAN	Alaska_LAN	Any	= Original	= Original	= Original	Policy Targets	
8	Alaska_LAN	Any	Any	H Alaska_LAN (Hiding Address)	= Original	= Original	Policy Targets	

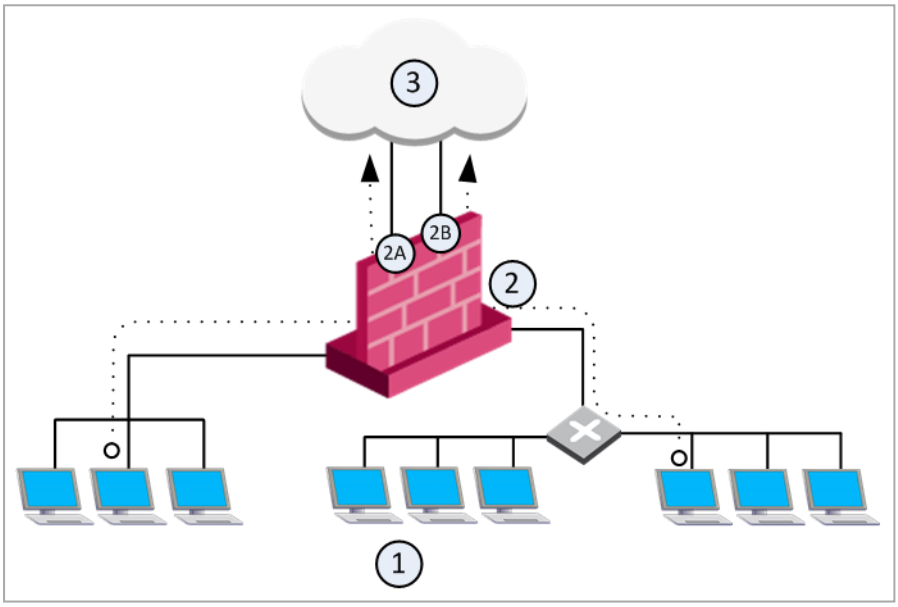
Automatic Hide NAT to External Networks

For large and complex networks, it can be impractical to configure the Hide NAT settings for all the internal IP addresses.

Explanation

An easy alternative is to enable a Security Gateway to automatically Hide NAT for all traffic with external networks. The Security Gateway translates all traffic that goes through an external interface to the valid IP address of that interface.

In this sample configuration, computers in internal networks open connections to external servers on the Internet. The source IP addresses of internal clients are translated to the IP address of an external interface.



Item	Description
1	Internal networks
2	Security Gateway is configured with Automatic Hide NAT.
2A and 2B	Two external interfaces 192.0.2.1 and 192.0.2.100.
1 -->3	External computers and servers on the Internet

Source IP addresses are translated to the applicable external interface IP address: **192.0.2.1** or **192.0.2.100**.

Note - If a connection matches a regular NAT rule and a NAT-for-internal-networks rule, the regular NAT rule takes precedence.

To enable Automatic Hide NAT:

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.
3. From the navigation tree, click **NAT**.
4. Select **Hide internal networks behind the Gateway's external IP**.
5. Click **OK**.
6. Install the Access Control Policy.

Note - When you enable this option, no rule is added to the NAT Rule Base. You can see the NAT activity in the Firewall logs.

For some deployments, it is necessary to manually define the NAT rules.

For example:

- Rules that are restricted to specific destination IP addresses and to specific source IP addresses
- Translating both source and destination IP addresses in the same packet.
- Static NAT in only one direction
- Translating services (destination ports)
- Rules that only use specified services (ports)
- Translating IP addresses for dynamic objects

General workflow when working with manual NAT rules:

1. Create SmartConsole objects that use the **valid** (NATed) IP addresses.
2. Create Manual NAT rules to translate the original IP addresses of the objects to valid IP addresses.
3. Configure the Access Control Policy to allow traffic to the applicable translated objects with the valid IP addresses.

Note - For Manual NAT rules, it is necessary to configure Proxy ARP entries to associate the translated IP address. See *Automatic and Proxy ARP*.

Example of a Manual NAT Rule

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	HTTP_Client	Web_Server	http	= Original	Web_Server	= Original	Policy Targets	

Configuring Manual NAT

Procedure

1. From the left navigation panel, click **Security Policies**.
2. Click **Access Control** > **NAT**.
3. Add a new rule in one of these ways:
   - From the top toolbar, click the **Add Rule** icon (the leftmost icon).
   - If there are existing Manual NAT rules, then right-click in the **No.** column of the applicable rule > in the line **New Rule**, click **Above** or **Below**.
4. In the new rule, select the required objects and configure the required translation.

   If the required objects do not exist, you can create them in the selection window (in the top right corner, click **New**).
5. Install the Access Control Policy.

Configuring Hide NAT behind Address Range

By default, when an administrator configures a Hide NAT rule and in the **Translated Source** column selects an Address Range object, the Security Gateway selects a Hide IP address from this range based only on the connection's source IP address.

Starting from R81.10 Jumbo Hotfix Accumulator Take 131, you can configure the Security Gateway to select a Hide IP address from the configured range based on the connection's source IP address and source port:

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Enable the corresponding kernel parameter. Run:

   ```
   fw ctl set -f int fwx_hide_range_with_port 1
   ```
3. Reboot the Security Gateway / each Cluster Member.

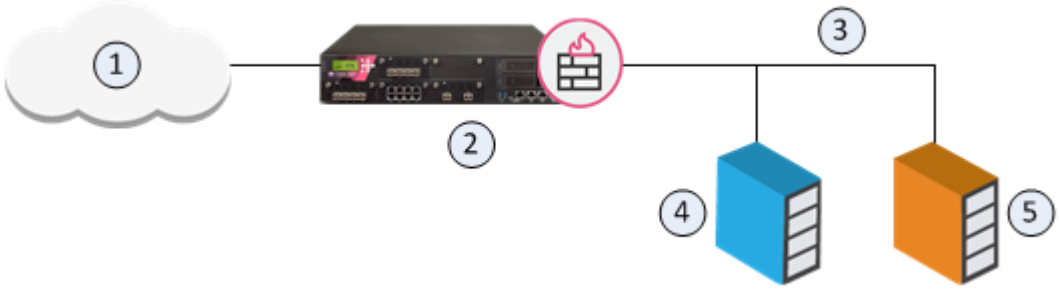
   Note - In a cluster, this can cause a failover.

Example Deployment

Example

This example configuration shows how to let external computers access an internal web server and an internal mail server in a DMZ network from one IP address.

To do this, you must configure Hide NAT for the DMZ network object and create manual NAT rules for the servers.



Item	Description
1	External computers and servers on the Internet
2	Security Gateway (**Alaska_GW**, external IPv6 2001:db8:0:c::1)
3	DMZ network (**Alaska_DMZ**, IPv6 2001:db8:a::/128)
4	Web server (**Alaska_DMZ_Web**, IPv6 2001:db8:a::35:5 is translated to IPv6 2001:db8:0:c::1)
5	Mail server (**Alaska_DMZ_Mail**, IPv6 2001:db8:a::35:6 is translated to IPv6 2001:db8:0:c::1)

Configuration Procedure:

1. Configure Automatic Hide NAT for the DMZ network:
   a. Double-click the Network object **Alaska_DMZ**.
   b. From the left, click **NAT**.
   c. Select **Add Automatic Address Translation Rules**.
   d. In **Translation method**, select **Hide**.
   e. Select **Hide behind Gateway**.
   f. Click **OK**.

   The Management Server creates these Automatic NAT rules in **Security Policies** view > **Access Control** > **NAT**:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	= Original	= Original	Policy Targets	

2. Create a Manual NAT rule to translate incoming HTTP traffic to the internal Web server:

a. In SmartConsole, go to **Security Policies** view > **Access Control** > **NAT**.

b. Add a new rule (#3) below the existing Automatic NAT rules.

c. Select these objects:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	= Original	= Original	Policy Targets	
3	Any	Alaska_GW	http	= Original	S Alaska_DMZ_Web	= Original	Policy Targets	

3. Create a Manual NAT rule to translate incoming SMTP traffic to the internal Mail server:

a. Add a new rule (#4) below the existing NAT rules.

b. Select these objects:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	= Original	= Original	Policy Targets	
3	Any	Alaska_GW	http	= Original	S Alaska_DMZ_Web	= Original	Policy Targets	
4	Any	Alaska_GW	smtp	= Original	S Alaska_DMZ_Mail	= Original	Policy Targets	

4. Create an Access Control rule to allow the incoming HTTP and SMTP traffic to the internal servers:

a. In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.

b. Add a new rule.

c. Select these objects:

No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
...	Incoming HTTP and SMTP traffic to internal servers	Any	Alaska_DMZ	Any	http smtp	Accept	Log	Policy Targets

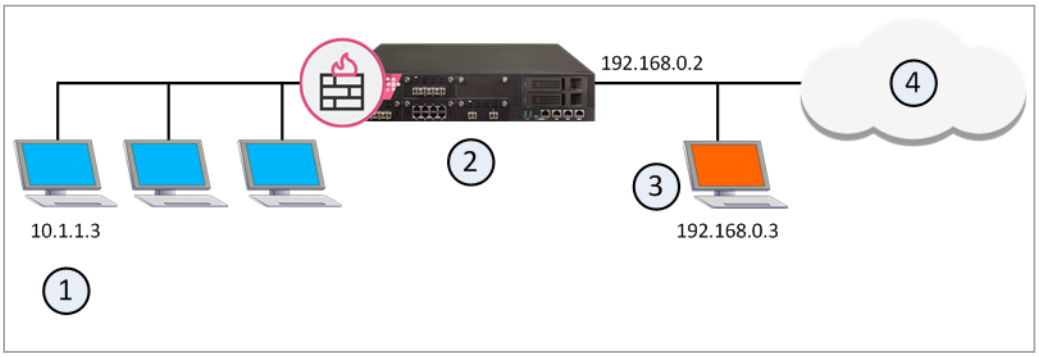
5. Install the Access Control Policy.

Advanced NAT Settings

This section includes advanced NAT settings. It discusses how to configure NAT in some network deployments.

Automatic and Proxy ARP

Giving a computer on the internal network an IP address from an external network using NAT makes that computer appear on the external network. When NAT on the Security Gateway is configured automatically, the Security Gateway replies on behalf of translated network objects to ARP Requests that are sent from the external network for the IP address of the internal computer.



Item	Description
1	Computer on the internal network with IP address 10.1.1.3
2	Security Gateway with external interface IP address 192.168.0.2 responds to ARP Requests on behalf of translated internal objects
3	Translated IP Address 192.168.0.3 on the external network
4	External network

If you are using manual NAT rules, you must configure Proxy ARP entries to associate the translated IP address with the MAC address of the Security Gateway interface that is on the same network as the translated IP addresses.

See sk30197 for more information about configuring:

- Proxy ARP for IPv4 Manual NAT
- Proxy ARP for Scalable Platforms

See sk91905 for more about configuring Proxy NDP for IPv6 Manual NAT.

NAT and Anti-Spoofing

NAT is performed after Anti-Spoofing checks, which are performed only on the source IP address of the packet. This means that spoofing protection is configured on the interfaces of the Security Gateway in the same way as NAT.

Disabling NAT in a VPN Tunnel

When communicating within a VPN, it is normally not necessary to perform NAT. You can disable NAT in a VPN tunnel with a single click in the VPN community object. Disabling NAT in a VPN tunnel by defining a NAT rule slows down the performance of the VPN.

Connecting Translated Objects on Different Interfaces

These sections describe how to allow connections in both directions between statically translated objects (hosts, networks or address ranges) on different Security Gateway interfaces.

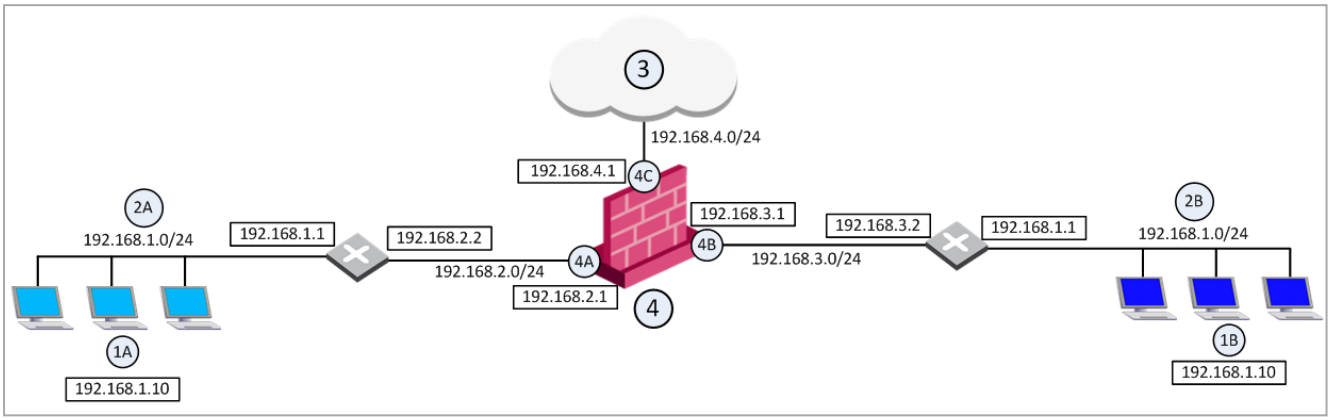
If NAT is defined through the network object (as opposed to using Manual NAT Rules), then you must ensure that bidirectional NAT is enabled.

Internal Communication with Overlapping Addresses

If two internal networks have overlapping (or partially overlapping) IP addresses, Security Gateway enables:

- Communication between the overlapping internal networks.
- Communication between the overlapping internal networks and the outside world.
- Enforcement of a different security policy for each overlapping internal network.

Network Configuration



For example, assume both Network 2A and Network 2B share the same address space (**192.168.1.0/24**), therefore standard NAT cannot be used to enable communication between the two networks. Instead, overlapping NAT must be performed on a per interface basis.

Users in Network 2A who want to communicate with users in Network 2B must use the **192.168.30.0/24** network as a destination. Users in Network 2B who want to communicate with users in Network 2A must use the **192.168.20.0/24** network as a destination.

The Security Gateway (4) translates the IP addresses in the following way for each individual interface:

Interface 4A

- Inbound source IP addresses are translated to the virtual network **192.168.20.0/24**.
- Outbound destination IP addresses are translated to the network **192.168.1.0/24**.

Interface 4B

- Inbound source IP addresses are translated to the network **192.168.30.0/24**.
- Outbound destination IP addresses are translated to the network **192.168.1.0/24**.

Interface 4C

Overlapping NAT is not configured for this interface. Instead, use NAT Hide in the normal way (not on a per-interface basis) to hide source addresses behind the interface's IP address (**192.168.4.1**).

Communication Examples

This section describes how to enable communication between internal networks, and between an internal network and the Internet

Communication Between Internal Networks

If user 1A, at IP address **192.168.1.10** in Network 2A, wants to connect to user 1B, at IP address **192.168.1.10** (the same IP address) in Network 2B, user 1A opens a connection to the IP address **192.168.30.10**.

Communication Between Internal Networks

Step	Source IP address	Destination IP address
Interface 4A - before NAT	**192.168.1.10**	**192.168.30.10**
Interface 4A - after NAT	**192.168.20.10**	**192.168.30.10**
Security Gateway enforces the security policy for packets from network **192.168.20.0/24** to network **192.168.30.0/24**.		
Interface 4B - before NAT	**192.168.20.10**	**192.168.30.10**
Interface 4B - after NAT	**192.168.20.10**	**192.168.1.10**

Communication Between an Internal Network and the Internet

If user 1A, at IP address **192.168.1.10** in network 2A, connects to IP address **192.0.2.10** on the Internet (3).

Communication Between an Internal Network and the Internet

Step	Source IP address	Destination IP address
Interface 4A - before NAT	**192.168.1.10**	**192.0.2.10**
Interface 4A - after NAT	**192.168.20.10**	**192.0.2.10**
The Security Gateway (4) enforces the security policy for packets from network **192.168.20.0/24** to the Internet (3).		
Interface 4C - before NAT	**192.168.20.10**	**192.0.2.10**
Interface 4C - after NAT Hide	**192.168.4.1**	**192.0.2.10**

Routing Considerations

To allow routing from Network 2A to Network 2B, routing must be configured on the Security Gateway.

These sections contain sample routing commands for Windows and Linux operating systems (for other operating systems, use the equivalent commands).

On Windows

- **route add 192.168.30.0 mask 255.255.255.0 192.168.3.2**
- **route add 192.168.20.0 mask 255.255.255.0 192.168.2.2**

On Linux

- **route add -net 192.168.30.0/24 gw 192.168.3.2**
- **route add -net 192.168.20.0/24 gw 192.168.2.2**

Object Database Configuration

To activate the overlapping NAT feature, use Database Tool (GuiDBEdit Tool) (see sk13009), or the `dbedit` command (see sk13301). In the sample network configuration, the per interface values for interface 4A and interface 4B are set in the following way:

Sample Network Configuration: Interface Configuration

Parameter	Value
enable_ overlapping_ nat	**true**
overlap_nat_ dst_ipaddr	The overlapping IP addresses (before NAT). In the sample network configuration, **192.168.1.0** for both interfaces.
overlap_nat_ src_ipaddr	The IP addresses after NAT. In the sample network configuration, **192.168.20.0** for interface 4A, and **192.168.30.0** for interface 4B.
overlap_nat_ netmask	The net mask of the overlapping IP addresses. In the sample network configuration, **255.255.255.0**.

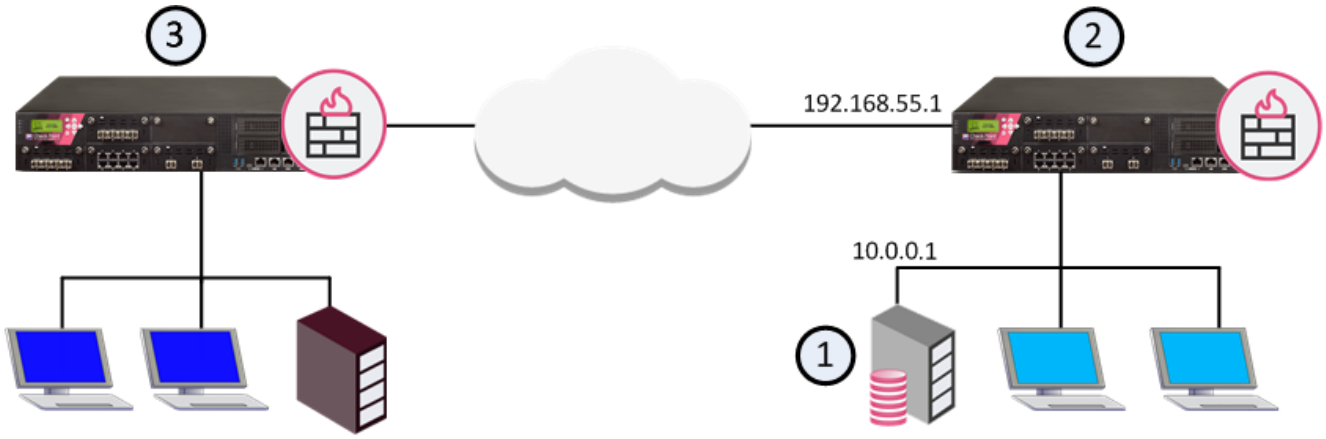
Security Management Behind NAT

The Security Management Server sometimes uses a private IP address (as listed in RFC 1918) or some other non-routable IP address, because of the lack of public IP addresses.

NAT (Static or Hide) for the Security Management Server IP address can be configured in one click, while still allowing connectivity with managed Security Gateways. All Security Gateways can be controlled from the Security Management Server, and logs can be sent to the Security Management Server. NAT can also be configured for a Management High Availability server and a Log Server.

Note - Security Management behind NAT is not supported for deployments where the Security Management Server also acts as a Security Gateway and must be addressed from outside the NATed domain, for example, when it receives SAM commands.

In a typical Security Management Behind NAT scenario: the Security Management Server (1) is in a network on which Network Address Translation is performed (the "NATed network"). The Security Management Server can control Security Gateways inside the NATed network, on the border between the NATed network and the outside world and outside the NATed network.



Item	Description
1	Primary Security Management Server. ■ Real IP address - 10.0.0.1 ■ Translated IP address - 192.168.55.1
2	Local Security Gateway that is directly connected to the Security Management Server. The Remote Security Gateway connects to the Security Management Server through this Local Security Gateway.
3	Remote Security Gateway that must connect to the Security Management Server.

In ordinary Hide NAT configurations, connections cannot be established from the external side the NAT A Security Gateway. However, when using Hide NAT on the Security Management Server, Security Gateways can send logs to the Security Management Server.

When using the Security Management behind NAT feature, the remote Security Gateway automatically selects the Security Management address to be addressed and simultaneously applies NAT considerations.

To enable NAT for the Security Management Server:

- From the **NAT** page of the Security Management Server object, define NAT and select **Apply for Security Gateway control connections**.

Non-Corresponding Security Gateway Addresses

Sometimes the Security Gateway contacts the Security Management Server with an address that does not correspond to the deployment of the remote Security Gateway.

For example:

- When the automatic selection of the Security Gateway does not conform with the routing of the deployment of the Security Gateway. In this case, define the masters and loggers manually, to allow the remote Security Gateway to contact the Security Management Server using the required address. When an inbound connection from a managed Security Gateway enters the Security Gateway, port translation is used to translate the hide address to the real IP address of the Security Management Server.

To define masters and loggers, select **Use local definitions for Log Servers** and **Use local definitions for Masters** and specify the correct IP addresses on the Security Gateway.

This solution encompasses different scenarios:

- The remote Security Gateway addresses the NATed IP when you want it to address the real IP.
- The remote Security Gateway addresses the real IP when you want it to address the NATed IP. In this case, specify the SIC name of the Security Management Server in the masters file.

Notes:

- Only one object can be defined with these settings, unless the second object is defined as a Secondary Security Management Server or as a Log Server.
- Ensure that you properly define the Topology settings on all Security Gateways. All workarounds required for previous versions still function with no changes in their behavior.

Configuring the Security Management Server Object

To configure the Security Management Server object:

1. From the **NAT** page on the Primary_Security_Management object, select either Static NAT or Hide NAT. If using Hide NAT, select **Hide behind IP Address**, for example, **192.168.55.1**. Do not select **Hide behind Gateway** (address **0.0.0.0**).
2. Select **Install on Gateway** to protect the NATed objects or network. Do not select **All**.
3. Select **Apply for Security Gateway control connections**.

Configuring the Security Gateway Object

To configure the Security Gateway object:

1. Open the Security Gateway **Network Management** page
2. Create the Interface. Click **Actions** > **New interface**.
3. In the **General** page of the **Interface** window, define the **IP** address and the Net Mask.
4. In the **Topology** section, click **Modify**.
5. Select **Override**.
6. Select **Network defined by the interface IP and Net Mask**.

IP Pool NAT

An IP Pool is a range of IP addresses (an address range, a network or a group of one of these objects) that is routable to the Security Gateway. IP Pool NAT ensures proper routing for encrypted connections for the following two connection scenarios:

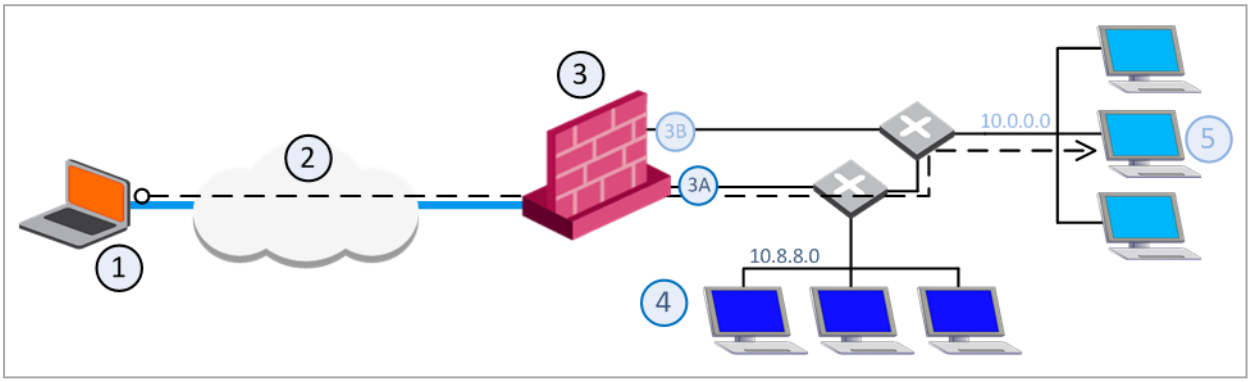
- Remote Access Client to MEP (Multiple Entry Point) Security Gateways
- Security Gateway to MEP Security Gateways

When a connection is opened from a Remote Access Client or a client behind a gateway, to a server behind the MEP Security Gateways, the packets are routed through one of the MEP Security Gateways. Return packets in the connection must be routed back through the same Security Gateway in order to maintain the connection. To ensure that this occurs, each of the MEP Security Gateways maintains a pool of IP addresses that are routable to the Security Gateway. When a connection is opened to a server, the Security Gateway substitutes an IP address from the IP pool for the source IP address. Reply packets from the server return to the Security Gateway, which restores the original source IP address and forwards the packets to the source.

IP Pool Per Interface

You can define a separate IP address pool on one or more of the Security Gateway interfaces instead of defining a single pool of IP addresses for the Security Gateway.

Defining an IP pool per interface solves routing issues that occur when the Security Gateway has more than two interfaces. Sometimes it is necessary that reply packets return to the Security Gateway through the same Security Gateway interface. This illustration shows one of the MEP Security Gateways in a Remote Access Client to MEP (Multiple Entry Point) Security Gateway deployment.



Item	Description
1	Packets from source host: Source: Original Destination:
2	VPN tunnel through the Internet
3	MEP Security Gateway
3A	IP Pool 1 packets: Source: 10.55.8.x Destination:
3B	IP Pool 2 packets: Source: 10.55.10.x Destination:
4	Internal network 10.8.8.0
5	Target host in internal network 10.10.10.0

If a remote client opens a connection to the internal network, reply packets from hosts inside the internal networks are routed to the correct Security Gateway interface through the use of static IP pool NAT addresses.

The remote client's IP address is NATed to an address in the IP pool on one of the Security Gateway interfaces. The addresses in the IP pool can be routed only through that Security Gateway interface so that all reply packets from the target host are returned only to that interface. Therefore, it is important that the IP NAT pools of the interfaces do not overlap.

When the packet returns to the Security Gateway interface, the Security Gateway restores the remote peer's source IP address.

The routing tables on the routers that lie behind the Security Gateway must be edited so that addresses from a Security Gateway IP pool are returned to the correct Security Gateway interface.

Switching between IP Pool NAT per Security Gateway and IP Pool NAT per interface and then installing the security policy deletes all IP Pool allocation and all NATed connections.

NAT Priorities

IP Pool NAT can be used both for encrypted (VPN) and non-encrypted (decrypted by the Security Gateway) connections.

Note - To enable IP Pool NAT for clear connections through the Security Gateway, configure INSPECT changes in the **user.def** file (see sk98239). Contact *Check Point Support*.

For non-encrypted connections, IP Pool NAT has the following advantages over Hide NAT:

- New back connections (for example, X11) can be opened to the NATed host.
- User-to-IP server mapping of protocols that allow one connection per IP can work with a number of hosts instead of only one host.
- IPsec, GRE and IGMP protocols can be NATed using IP Pool NAT (and Static NAT). Hide NAT works only with TCP, UDP and ICMP protocols.

Because of these advantages, you can specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.

The order of NAT priorities are:

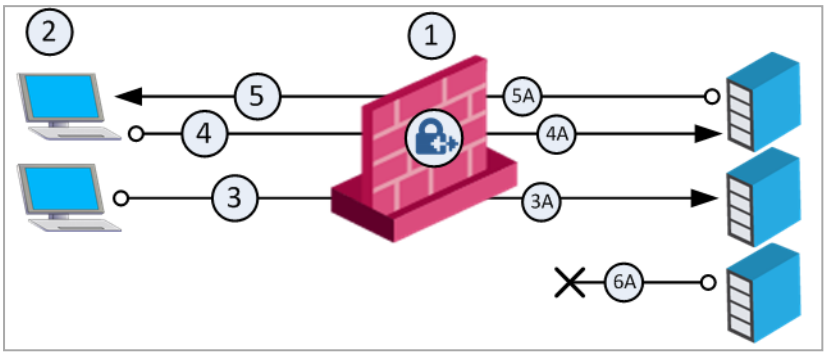
1. Static NAT
2. IP Pool NAT
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

Reusing IP Pool Addresses For Different Destinations

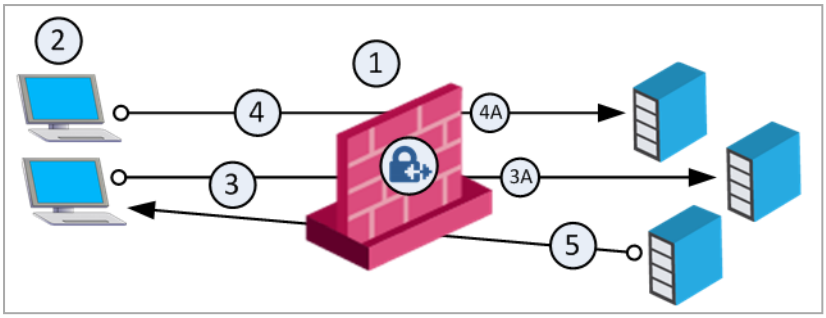
IP Pool addresses can be reused for different destinations, which makes more efficient use of the addresses in the pool. If a pool contains N addresses, then any number of clients can be assigned an IP from the pool as long as there are no more than N clients per server.

Using IP Pool allocation per destination, two different clients can receive the same IP from the pool as long as they communicate with different servers (connections 1 and 2). When reusing addresses from the IP Pool, back connections are supported from the original server only (connection 3). This means that connections back to the client can be opened only from the specific server to which the connection was opened.



Item	Description
1	Security Gateway with IP Pool addresses A to Z
2	Clients. Source: Original Destination:
3A	NATed packet from connection 3. Source: A Destination:
4A	NATed packet from connection 4. Source: A Destination:
5A	NATed packet from reply connection 5. Source: Original Destination: A
6A	This server cannot open a connection with Destination A back to the client.

The default **Do not reuse IP Pool NAT** behavior means that each IP address in the IP Pool is used once (connections 1 and 2 in the following illustration). In this mode, if an IP pool contains 20 addresses, up to 20 different clients can be NATed and back connections can be opened from any source to the client (connection 3).



Item	Description
1	Security Gateway with IP Pool addresses A to Z.
2	Clients. Source: Original Destination:
3A	NATed packet from connection 3. Source: A Destination:
4A	NATed packet from connection 4. Source: Z Destination:
5	Connection. Source: Original Destination: A

Switching between the **Reuse** and **Do not reuse** modes and then installing the security policy, deletes all IP Pool allocations and all NATed connections.

Configuring IP Pool NAT

To configure IP Pool NAT:

1. From the SmartConsole **Menu**, select **Global properties**.
2. In the **Global properties** > **NAT** page, select **Enable IP Pool NAT** and the required tracking options.
3. In the Security Gateway's **General Properties** page, ensure the Security Gateway version is specified correctly.
4. For each Security Gateway or Security Gateway interface, create a network object that represents its IP pool NAT addresses. The IP pool can be a network, group, or address range.

For example, for an address range, do the following:

a. From the **Objects Bar (F11)**, In the network objects tree, select **New > More > Network Object > Address Range > Address Range**.

The **Address Range Properties** window opens.

b. In the **General** tab, enter the first and last IP of the address range.

c. Click **OK**. The new address range appears in the **Address Ranges** branch of the network objects tree.

5. Edit the Security Gateway object, and select **NAT** > **IP Pool NAT**.
6. In the **IP Pool NAT** page, select one of the following:

a. **Allocate IP Addresses from** and then select the address range you created to configure IP Pool NAT for the whole Security Gateway, or

b. **Define IP Pool NAT on Gateway interfaces** to configure IP Pool NAT per interface.

7. If required, select one or more of the following options:

a. **Use IP Pool NAT for VPN client connections**

b. **Use IP Pool NAT for gateway to gateway connections**

c. **Prefer IP Pool NAT over Hide NAT** to specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.

8. Click **Advanced**.

a. **Return unused addresses to IP Pool after**:

Addresses in the pool are reserved for 60 minutes (default), even if the user logs off. If the user disconnects from their ISP and then redials and reconnects, there will be two Pool NAT addresses in use for the user until the first address from the IP Pool times out. If users regularly lose their ISP connections, you may want to decrease the time-out to prevent the IP Pool from being depleted.

b. **Reuse IP addresses from the pool for different destinations**:

This is a good option unless it is necessary to allow back connections to be opened to clients from any source, rather than just from the specific server to which the client originally opened the connection.

9. Click **OK**.

10. Edit the routing table of each internal router so that packets with an IP address assigned from the NAT pool are routed to the appropriate Security Gateway or, if using IP Pools per interface, the appropriate Security Gateway interface.

IP Pool NAT for Clusters

IP Pools for clusters are configured in two places in SmartConsole:

- In the Cluster object > **NAT > IP Pool NAT** page, select the connection scenario.
- In the Cluster Member object > **IP Pool NAT** page, define the IP Pool on the Cluster Member. A separate IP pool must be configured for each cluster member. It is not possible to define a separate IP Pool for each Cluster Member interface.

Desktop, DLP, QoS, andMobile Access Policies

What can I do here?

Use this window to open the Desktop, DLP, QoS, or Mobile Access policy in SmartConsole.

Getting Here - Security Policies > Access Control > Policy > Desktop/QoS
Or:
Security Policies > Shared Policies > Mobile Access/DLP

Mobile Access Authentication

Mobile Access has multiple login and authentication options.

User Authentication to the Mobile Access Portal

To enter the Mobile Access Portal and get access to its applications, users defined in SmartConsole must authenticate to the Security Gateway. Authentication ensures that a user is who he or she claims to be. Users authenticate using one or more of these authentication schemes:

- **Username and password** - Users enter a user name and password.
- **Client Certificates** - Digital Certificates are issued by the Internal Certificate Authority or by a third party OPSEC certified Certificate Authority.
- **RADIUS Server** - Remote Authentication Dial-In User Service (RADIUS) is an external authentication scheme. The Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users. The RADIUS protocol uses UDP for communications with the gateway. RADIUS Servers and RADIUS Server Group objects are defined in SmartConsole.

For more about configuring a Security Gateway to use a RADIUS server, see the *R81.10 Security Management Administration Guide*

- **SecurID** - SecurID is a proprietary authentication method of RSA Security. An external SecurID server manages access by changing passwords every few seconds. Each user carries a SecurID token, a piece of hardware or software that is synchronized with the central server and displays the current password. The Security Gateway forwards authentication requests by remote users to the Authentication Manager.

  For more about configuring a Security Gateway to use SecurID, see the *R81.10 Security Management Administration Guide*

- **DynamicID One Time Password** - DynamicID One Time Password can be required as a secondary or later authentication method (not the first). When this is configured, users who successfully complete the first-phase or phases of authentication are challenged to enter an additional credential: a DynamicID One Time Password (OTP). The OTP is sent by email or text message to a mobile phone, or other mobile communication device.

- **Defined on user record (Legacy Authentication)** - The authentication method for each user is defined on the user record. For internal users, it is in the **Authentication** page of the User Properties. For LDAP users, it is on the user record in LDAP.

A user who tries to authenticate with an authentication scheme that is not configured for the Mobile Access gateway will not be allowed to access resources through the gateway.

Configuring Authentication for Pre-R80.x Gateways

Permitted authentication schemes must be configured for each Security Gateway.

In the Security Gateway object, configure authentication in the **Mobile Access** > **Authentication**. If you select an authentication method on this page, that is the method that all users must use to authenticate to Mobile Access. You can configure other authentication methods that users must use for different blades on different pages.

The default authentication scheme is **Username and Password**.

In the **Mobile Access** tab in SmartConsole, select **Authentication** to show an overview of the Mobile Access Security Gateways and their authentication schemes.

On this page you can also configure settings for Two- Factor Authentication with a DynamicID One Time Password. Configure settings for the gateway or global settings that are used for all gateways that do not have their own DynamicID settings.

Requiring Certificates for Mobile Devices on Pre-R80.x Gateways

To require client certificates for mobile devices:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The gateway window opens and shows the **General Properties** page.

2. From the navigation tree, click **Mobile Access > Authentication**.
3. Make sure that the Authentication Method is one of these options:
   - **Username and password**
   - **RADIUS**
   - **SecurID**
4. From the **Certificate Authentication for mobile devices** section, click **Require client certificate when using ActiveSync applications or Capsule Workspace Mail**.
5. Click **OK**.
6. Install the policy.

Multiple Login Options for R80.XX Gateways

On R80.10 and higher Mobile Access and IPsec VPN gateways, you can configure multiple login options. The options can be different for each gateway and each supported Software Blade, and for some client types. Users select one of the available options to log in with a supported client.

By default, all clients connect with the pre-R80.XX method. When you create new login options, newer clients can see them in addition to the pre-R80.XX option, but older clients cannot.

To see which clients support the new multiple login options, see sk111583.

Each configured login option is a global object that can be used with multiple gateways and the Mobile Access and IPsec VPN Software Blades.

Compatibility with Older Clients

Older clients connect with the same login options available on pre-R80 gateways. If you upgrade all or most clients to versions that support multiple login options, you can block older clients from connecting. After you do this, only clients that support multiple login options can connect to the gateway.

By default, **Allow older clients to connect to this gateway** is selected in **Mobile Access > Authentication**. If you clear the option, older clients are blocked.

You can choose if newer clients that support multiple login options can connect with the authentication settings defined for older clients.

Configuring the Authentication Method for Newer Clients

To block newer clients from using the authentication method defined for older clients:

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. In the **Compatibility with Older Clients section**, click **Settings**.

   The **Single Authentication Clients Settings** window opens.
3. Clear **Allow newer clients that support Multiple Login Options to use this authentication method**.
4. Click **OK**.
5. Install policy.

To let newer clients connect to the gateway with the authentication settings defined for older clients:

Select **Allow newer clients that support Multiple Login options to use this authentication method**.

Configuring Authentication Settings for Older Clients

To let older clients connect to the R80.10 or higher gateway:

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. Select **Allow older clients to connect to this gateway**.

   If this is not selected, older clients cannot connect to the gateway.

To change the authentication method for older clients:

1. In the **Gateway Properties**, select **Mobile Access** > **Authentication** or **VPN Clients** > **Authentication**.
2. In the **Compatibility with Older Clients** section, click **Settings**.

   The **Single Authentication Clients Settings** window opens.
3. Change the **Display Name** to change the way the authentication method is shown in SmartConsole.

1. Select an **Authentication method**.
2. Click **Customize** to change the description of fields that are shown to users in the **login** window.
3. To require DynamicID with the selected authentication method, select **Enable DynamicID**. After you select this, you must configure the DynamicID settings for the gateway from **Authentication** > **DynamicID Settings** > **Edit**.
4. Define the settings for **Capsule Workspace**:
   - Select **Require client certificate** to require **Capsule Workspace** to always use client certificates.
   - Select Allow DynamicID to require DynamicID in addition to the selected authentication method. After you select this, you must configure the DynamicID settings for the gateway from **Authentication** > **DynamicID Settings** > **Edit**.
5. Click **OK**.
6. Click **OK**.
7. Install policy on the Security Gateway.

To configure global DynamicID settings that all gateways use:

1. For each Security Gateway, in **Gateway Properties** > **Mobile Access** > **Authentication** > **DynamicID Settings**, select **Use Global Settings**.
2. In SmartConsole, select **Security Policies** > **Shared Policies** > **Mobile Access** and click **Open Mobile Access Policy in SmartConsole**.

   SmartConsole opens and shows the **Mobile Access** tab.
3. Configure the global settings in **Mobile Access** tab > **Authentication** > **Two-Factor Authentication with DynamicID**.
4. Close SmartDashboard
5. Install policy in SmartConsole.

Configuring Multiple Log-in Options

You can configure login options from:

- **Gateway Properties** > **Mobile Access** > **Authentication**
- **Gateway Properties** > **VPN Clients** > **Authentication**
- SmartConsole > **Mobile Access** tab > **Authentication**

The login options selected for Mobile Access clients, such as the Mobile Access Portal and Capsule Workspace, show in the **Mobile Access** > **Authentication** page in the **Multiple Authentication Client Settings** table.

The login options selected for VPN clients, such as Endpoint Security VPN, Check Point Mobile for Windows, and SecuRemote, show in the **VPN Clients** > **Authentication** page in the **Multiple Authentication Client Settings** table.

To configure multiple login options for Mobile Access Clients:

1. From the Gateway Properties tree of a Security Gateway select **Mobile Access** > **Authentication**.
2. In the **Multiple Authentication Clients Settings** table, see a list of configured login options.

   The default login options are:

   - **Personal_Certificate** - Require a user certificate.
   - **Username_Password** - Require a username and password.
   - **Cert_Username_Password** - Require a username and password and a user certificate.
3. Click **Add** to create a new option or **Edit** to change an option. Each configured login option is a global object that can be used with multiple gateways and Software Blades.
4. For each login option select one or more **Authentication Factors** and relevant **Authentication Settings**.

   For example, if you select **SecurID**, select the SecurID **Server** and **Token Card Type**. If you select **Personal Certificate**, select which certificate field the gateway uses to fetch the username. See Certificate Parsing.
5. Select **Customize Display** to configure what users see when they log in with this option. See Customize Display Settings.
6. Click **OK**.
7. Use the **Up** and **Down** arrows to set the order of the login options.
   - If you include **Personal Certificates**, it must be first.
   - If you include **DynamicID**, it cannot be first.
8. On each **Login Option** > **Usage in Gateway**, select if the login option is available from:
   - The **Mobile Access Portal**
   - **Capsule Workspace**
9. Click **OK**.

Selecting a Client for a Login Option

For login options created from the **Mobile Access** > **Authentication** page, you can select if the login option is available for the Mobile Access Portal, Capsule Workspace, or both.

The login option will only be visible for the clients that you select.

Customize Display Settings

Enter descriptive values to make sure that users understand what information to input. These fields must all be the same language but they do not need to be in English.

- **Headline** - The title of the login option, for example, **Log in with a Certificate** or **Log in with your SecurID Pinpad**.
- **Username label** - A description of the username that users must enter, for example, **Email address** or **AD username**.
- **Password label** - A description of the password that users must enter, for example, **AD password**.

Certificate Parsing

When you select **Personal Certificate** as a Login option, you can also configure what information the gateway sends to the LDAP server to parse the certificate. The default is the DN. You can configure the settings to use the user's email address or a serial number instead.

To change the certificate parsing:

1. In the **Multiple Authentication Clients Settings** table on the **Authentication** page, select a **Personal_Certificate** entry and click **Edit**.

   The **Authentication Factor** window opens.
2. In the **Authentication Settings area** in the **Fetch Username from** field, select the information that the gateway uses to parse the certificate.
3. Click **OK**.
4. Install policy.

Deleting Login Options

To permanently delete a Login option:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **Mobile Access** and click **Open Mobile Access Policy in SmartConsole**.
2. In SmartConsole go to the **Mobile Access** tab > **Authentication** page.
3. From the list of login options, select an option and click **Delete**.

Viewing all Gateways Authentication Settings

To see all gateways and their authentication settings:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **Mobile Access** and click **Open Mobile Access Policy in SmartConsole**.
2. In SmartConsole go to the **Mobile Access** tab.
3. From the tree, select **Gateways**.
4. Click a Security Gateway to see its authentication settings.

Multi-Factor Authentication with DynamicID

Multi-factor authentication is a system where two or more different methods are used to authenticate users. Using more than one factor delivers a higher level of authentication assurance. DynamicID is one option for multi-factor authentication.

Users who successfully complete the first-phase authentication can be challenged to provide an additional credential: a DynamicID One Time Password (OTP). The OTP is sent to their mobile communications device (such as a mobile phone) via SMS or directly to their email account.

On Security Gateways R80.10 and higher, DynamicID is supported for all Mobile Access and IPsec VPN clients.

How DynamicID Works

When logging in to the Mobile Access Portal, users see an additional authentication challenge such as:

Please type the verification code sent to your phone.

Users enter the one time password that is sent to the configured phone number or email address and they are then admitted to the Mobile Access Portal.

On the User Portal sign in screen, the "**I didn't get the verification code**" link shows. If the user does not receive an SMS or email with the verification code within a short period of time, the user can click that button to receive options for resending the verification code.

Administrators can allow users to select a phone number or email address from a list. Only some of the phone number digits are revealed. Users can then select the correct phone number or email address from the list and click **Send** to resend the verification code. By default, users can request to resend the message three times before they are locked out of the Portal.

Match Word

The Match Word feature ensures that users can identify the correct DynamicID verification code in situations when they may receive multiple messages. Users are provided with a match word on the Login page that will also appear in the correct message. If users receive multiple SMS messages, they can identify the correct one, as it will contain the same match word.

The SMS Service Provider

In R77.30 and lower versions, proxy settings for the SMS service provider were configured in **Gateway Properties** > **Mobile Access** > **HTTP Proxy**.

In R80.10 and higher, this is configured in **Gateway Properties** > **Network Management** > **Proxy**.

To access the SMS service provider, configure the proxy settings on the gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway object.

   The Security Gateway window opens and shows the **General Properties** page.

2. From the navigation tree, click **Network Management** > **Proxy**.

3. Define the Proxy settings.

   If no proxy is defined on this page, no proxy is used for the SMS provider.

Whichever provider you work with, in order for the SMS messages to be sent to users, valid account details must be obtained from the provider and be configured in Mobile Access.

DynamicID Authentication Granularity

You can make multi-factor authentication with DynamicID a requirement to log in to the gateway. Alternatively, you can make DynamicID a requirement to access specified applications. This flexibility gives you different security clearance levels.

To make multi-factor authentication with DynamicID a requirement to access specified applications, configure a Protection Level to require multi-factor authentication, and associate the Protection Level with Mobile Access applications.

In an environment with multiple Mobile Access gateways, make multi-factor authentication a requirement for a specified gateway, configure multi-factor authentication for that gateway.

On Security Gateways R80.10, DynamicID authentication can be part of a login option that is required for the Mobile Access Portal or Capsule Workspace, or both.

Basic DynamicID Configuration for SMS or Email

The workflow for basic configuration of two-factor authentication via DynamicID is:

1. Obtaining the SMS provider credentials and/or email settings.
2. Configuring the Phone Directory.
3. Basic SmartConsole Configuration of DynamicID.
4. Testing DynamicID Two-Factor Authentication.

Obtaining the SMS Provider Credentials

Get these required SMS service provider settings from your SMS provider.

- A URL in the format specified by the SMS provider or a valid email address.
- Account credentials:
  - User name
  - Password
  - API ID (optional and may be left empty)

Note - If DynamicID is configured to work with email only, an SMS Service Provider is not necessary.

Configuring the Phone Directory

The default phone number and email search method is that the gateway searches for phone numbers or email addresses in user records on the LDAP account unit, and then in the phone directory on the local gateway. If the phone number configured is actually an email address, an email will be sent instead of an SMS message. The phone number and email search method can be changed in the **Phone Number or Email Retrieval** section of the **Two-Factor Authentication with DynamicID - Advanced** window.

Configuring Phone Numbers or Email Addresses in LDAP

If users authenticate via LDAP, configure the list of phone numbers on LDAP by defining a phone number or email address for each user. By default, Mobile Access uses the **Mobile** field in the **Telephones** tab. If the phone number configured is actually an email address, an email will be sent instead of an SMS message.

Configuring Phone Numbers or Email Addresses on Each Security Gateway

Configure the list of phone numbers or email addresses on each Mobile Access gateway. For a Mobile Access cluster, configure the directory on each cluster member.

To configure a list of phone numbers on a gateway:

1. Log in to the Mobile Access gateway using a secure console connection.
2. Change to the Expert mode: Type `expert` and then the expert mode password.
3. Backup `$CPDIR/conf/dynamic_id_users_info.lst`

Note - If this file does not yet exist, create it.

4. Edit `$CPDIR/conf/dynamic_id_users_info.lst`, and add to it a list of user names and phone numbers, and/or email addresses. The list must be followed by a blank line. Use this syntax:

```
{<user name> | <Full DN>} {<phone number> | <email address>}
```

Parameter	Meaning
user name or Full DN	Either a user name or, for users that log in using a certificate, the full DN of the certificate.
phone number	All printable characters can be used in the phone number, excluding the space character, which is not allowed. Only the digits are relevant.
email address	A valid email address in the format user@domain.com

Example of acceptable ways to enter users and their phone numbers or email addresses in the `$CPDIR/conf/dynamic_id_users_info.lst` file:

```
bob +044-888-8888
jane tom@domain.com
CN=tom,OU=users,O=example.com +044-7777777
CN=mary,OU=users,O=example.com +mary@domain.com
```

Configuring Multiple Phone Numbers

You can let users choose from multiple phone numbers when resending the verification code.

To configure choice of numbers:

Enter one number in the LDAP directory in the Mobile field and one or more in the Security Gateway configuration file:

`$CPDIR/conf/dynamic_id_users_info.lst`

Enter multiple phone numbers separated by white space in the Security Gateway configuration file:

`$CPDIR/conf/dynamic_id_users_info.lst`

For example, `user_a 917-555-5555 603-444-4444`

Note -If the configuration file does not yet exist, create it.

Basic SmartDashboard Configuration of DynamicID

Configure the **Authentication** settings to make two-factor authentication necessary for all mobile devices.

This table explains parameters used in the SMS Provider and Email Settings field. The value of these parameters is automatically used when sending the SMS or email.

Parameter	Meaning
$APIID	The value of this parameter is the API ID.
$USERNAME	The value of this parameter is the username for the SMS provider.
$PASSWORD	The value of this parameter is the password for the SMS provider.
$PHONE	User phone number, as found in Active Directory or in the local file on the gateway, including digits only and without a + sign.
$EMAIL	The email address of the user as found in Active Directory or in the local `dynamic_id_users_info.lst` file on the gateway. If the email address should be different than the listed one, it can be written explicitly. if the file does not exist, create it.
$MESSAGE	The value of this parameter is the message configured in the Advanced Two-Factor Authentication Configuration Options in SmartConsole.
$RAWMESSAGE	The text from $Message but without HTTP encoding.

To configure DynamicID settings for all gateways in SmartConsole:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **Mobile Access** and click **Open Mobile Access Policy in SmartConsole**.

   SmartConsole opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Authentication**.
3. From the **Dynamic ID Settings** section, click **Edit**.
1. Select **Challenge users to provide the DynamicID one time password**.
2. Fill in the **SMS Provider and Email Settings** field using one of these formats:
   a. To let the DynamicID code to be delivered by SMS only, use the following syntax:

   ```
   https://api.example.com/http/sendmsg?api_id=$APIID&user=
   $USERNAME&password=$PASSWORD&to=$PHONE&text=$MESSAGE
   ```

b. To let the DynamicID code to be delivered by email only, without an SMS service provider, use the following syntax:

```
mail:TO=$EMAIL;SMTPSERVER=smtp.example.com;FROM=sslvpn@examp
le.com;
BODY=$RAWMESSAGE
```

c. To let the DynamicID code to be delivered by SMS or email, use the following syntax:

```
sms:https://api.example.com/sendsms.php?username=$USERNAME&p
assword=
$PASSWORD&phone=$PHONE&smstext=$MESSAGE mail:TO=$EMAIL;
SMTPSERVER=smtp.example.com;FROM=sslvpn@example.com;
BODY=$RAWMESSAGE
```

3. In the **SMS Provider Account Credentials** section, enter the credentials received from the SMS provider:
   - **Username**
   - **Password**
   - **API ID** (optional)
4. For additional configuration options, click **Advanced**.
5. Click **OK**.
6. Click **Save** and then close SmartConsole.
7. From SmartConsole, install policy.

To configure the Mobile Access Security Gateway to let computers and devices use DynamicID:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Authentication**.
3. In the **Two-Factor Authentication** section, configure these settings:
   - For a Security Gateway that uses the global authentication settings, select **Global settings**.
   - For a Security Gateway that uses different authentication settings, select **Custom settings**.
   - For mobile devices, select **Allow DynamicID for mobile devices**.

4. Click **OK**.
5. Install the policy.

Testing Two-Factor Authentication

To test the two-factor authentication via DynamicID, after completing the configuration:

1. Browse to the URL of the Mobile Access Portal.
2. Log in as a user.
3. Supply the gateway authentication credentials.
4. Wait to receive the DynamicID code on your mobile communication device or check your email.
5. Enter the DynamicID code in the portal.

   Make sure that you are logged in to the Mobile Access Portal.

Advanced Two-Factor Authentication Configuration

To configure settings for a specified gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Mobile Access > Authentication**.
3. From the **Two-Factor Authentication with DynamicID** section, click **Custom settings for this gateway**.
4. Click **Configure**.

   The **Two-Factor Authentication with DynamicID** window opens.

To configure global settings for all the gateways:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **Mobile Access** and click **Open Mobile Access Policy in SmartConsole**.

   SmartConsole opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Authentication**.
3. From the **DynamicID Settings** section, click **Edit**.
4. Click **Advanced**.

   The **Two-Factor Authentication with DynamicID** window opens.

DynamicID Message

- **Message text to be sent to the user**

  By default, the text of the message is "**Mobile Access DynamicID one time password:** ". The message can contain the template fields shown in the following table to include the user's name and prompt users to use enter a One Time Password.

  For example, the message could say: **$NAME, use the verification code $CODE to enter the portal**.

Parameter	Meaning
`$NAME`	User name used in the first phase of authentication to the portal.
`$CODE`	Replaced with the One Time Password. By default, $CODE is added to the end of the message.

DynamicID Settings

- **Length of one time password** is 6 digits by default
- **One time password expiration (in minutes)** is 5 minutes by default. Ensure there is a reasonably sufficient time for the message to arrive at the mobile communication device or email account, for the user to retrieve the password, and to type it in.
- **Number of times users can attempt to enter the one time password before the entire authentication process restarts.** By default the user has 3 tries.

Display User Details

- **In the portal, display the phone number or email address that received the DynamicID.** By default, the phone number to which the SMS message was sent is not shown.

Country Code

- **Default country code for phone numbers that do not include country code.** The default country code is added if the phone number stored on the LDAP server or on the local file on the gateway starts with 0.

Phone Number or Email Retrieval

- **Active Directory and Local File**
  Try to retrieve the user details from the Active Directory user record. If unsuccessful, retrieve from the local file on the gateway. The LDAP account unit is defined in the **Users and Authentication > Authentication > LDAP Account Units** page of the SmartConsole Mobile Access tab. The phone directory on the local gateway is in `$CPDIR/conf/dynamic_id_users_info.lst`

Note - If the directory file does not exist yet, create it.

- **Active Directory Only**
  Retrieve phone numbers from Active Directory user record without using the local file on the gateway. The LDAP account unit is defined in the **Users and Authentication > Authentication > LDAP Account Units** page of the SmartConsole Mobile Access tab.
- **Local File Only**
  Retrieve the user details from the local file on the gateway. The phone directory on the local gateway is in `$CPDIR/conf/dynamic_id_users_info.lst`

Configuring Resend Verification and Match Word

The DynamicID troubleshooting and match word features are configured in Database Tool (GuiDBEdit Tool) (see sk13009) or dbedit (see sk13301).

The Database Tool (GuiDBEdit Tool) table to edit depends on the Two Factor Authentication with SMS One Time Password (OTP) setting that you configured in SmartConsole in the Mobile Access Gateway Properties page > Authentication.

- If your DynamicID One Time Password settings are global across all of your gateways (use the global settings configured in the Mobile Access tab is selected), in Database Tool (GuiDBEdit Tool) select **Other > Mobile Access Global Properties**.
- If your DynamicID One Time Password settings are configured for a specific gateway (this gateway has its own two-factor authentication settings is selected), in Database Tool (GuiDBEdit Tool) select **network_objects** and then select the specific gateway you want to edit.

This table shows the DynamicID features that can be configured, and where in Database Tool (GuiDBEdit Tool) to configure them.

Feature	Field Names to Edit	Value Options
Match Word	`use_message_matching_helper`	**true**: match word provided **false**: match word not provided (default)
Resend message	`enable_end_user_re_transmit_message`	**true**: enable resend SMS feature (default) **false**: disable resend SMS feature
Display multiple phone numbers	enable_end_user_select_phone_num	**true**: enable option to choose from multiple phone numbers or email addresses when resending the verification code (default) **false**: one phone number or email address from the LDAP server or local file is used automatically without choice

Feature	Field Names to Edit	Value Options
Conceal displayed phone numbers	Edit both: `reveal_partial_phone_num` and `number_of_digits_revealed`	**true**: conceal part of the phone number or email address (default) **false**: display the full phone number or email address **1-20**: Choose the amount of digits to reveal (default is 4)

After editing the values in Database Tool (GuiDBEdit Tool), save the changes, connect to SmartConsole, and install the policy.

Configuring the Number of Times Messages are Resent

By default, users can request to resend the verification code message three times by clicking the **I didn't get the verification code** link before they are locked out of the Mobile Access Portal. The number of times the message can be resent is configured using the `cvpnd_settings` command from the Mobile Access CLI in expert mode.

The instructions below relate to actually resending the verification code message. The number of times users can try to input the verification code is configured in SmartConsole in the **Two Factor Authentication Advanced** window.

To change the number of times the verification code message can be resent to 5, run:

```
cvpnd_settings set smsMaxResendRetries 5
```

You can replace "5" with any other number to configure a different amount of retries.

After making the changes, run `cvpnrestart` to activate the settings.

If the Mobile Access gateway is part of a cluster, be sure to make the same changes on each cluster member.

Two-Factor Authentication per Gateway

To configure two-factor authentication Globally on, with custom settings per gateway:

1. Set up basic two-factor authentication.
2. For each Security Gateway, go to **Gateway Properties > Mobile Access > Authentication**.
3. Do one of these options:

- **To use the global settings** - Select **Global settings** and the global settings are used from the **Authentication to Gateway** page of the Mobile Access tab. This is the default.
- **To turn off two-factor authentication for the gateway** - Select **Custom Settings for this Gateway** and click **Configure.** In the window that opens, do not select the check box. This turns off two-factor authentication for this gateway.
- **To activate two-factor authentication for the gateway with custom settings** - Select **Custom Settings for this Gateway** and click **Configure.** In the window that opens, select the check box. You must then configure custom SMS Provider Credentials for this gateway. Optionally, configure **Advanced** options.

4. Repeat **step 2** to **step 3** for all other gateways.
5. Install the policy.

Two-Factor Authentication per Application

To configure two-factor authentication per application:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **Mobile Access** and click **Open Mobile Access Policy in SmartConsole**.

   SmartConsole opens and shows the **Mobile Access** tab.
2. Configure basic two-factor authentication.
   a. Configure the phone directory.
   b. Configure the application settings in **Mobile Access** tab > **Authentication**.
   c. Configure the Mobile Access Security Gateways to let the mobile devices use DynamicID.
3. Configure the Protection Level.
   a. In the **Protection Level** window, from the navigation tree click Authentication.
   b. Select **User must successfully authenticate via SMS**.
   c. Click **OK**.
4. Assign the protection level to Mobile Access applications that require two-factor authentication.
5. Click **Save** and then close SmartConsole.
6. From SmartConsole, install the policy.

Changing the SMS Provider Certificates and Protocol

By default, it is recommended to use a secure (https) protocol for communication with the SMS provider. Mobile Access also validates the provider server certificate using a predefined bundle of trusted CAs.

If your SMS provider uses a non-trusted server certificate you can do one of the following:

- Add the server certificate issuer to the trusted CA bundle under `$CVPNDIR/var/ssl/ca-bundle/` and run: `$CVPNDIR/bin/rehash_ca_bundle`
- Ignore the server certificate validation by editing `$CVPNDIR/conf/cvpnd.C` and replacing the `SmsWebClientProcArgs` value with `("-k")`.

If your SMS provider is working with the non-secure http protocol, edit the file `$CVPNDIR/conf/cvpnd.C` and replace the `SmsWebClientProcArgs` value with `("")`.

Multiple Log-in Options for Pre-R80 Gateways

On Pre-R80 gateways Multiple Log-in options is called Multiple Realms and is configured in Database Tool (GuiDBEdit Tool) (see sk13009) or dbedit (see sk13301). It gives support for multiple authentication realms in the Mobile Access Portal. If you use this feature, we recommend that you upgrade your gateways to R81.10. and configure Multiple Login Options for R80.x Gateways in SmartConsole.

If you upgrade your server and gateways to R81.10, see sk115856 for information about upgrading the multi-realms configuration.

If you upgrade your Security Management Server to R80.x and do not upgrade the gateways, reconfigure Multiple Realms in Database Tool (GuiDBEdit Tool) after the upgrade.

How the Gateway Searches for Users

If you configure authentication for a blade from the main Security Gateway **Legacy Authentication** page, the Security Gateway searches for users in a standard way when they try to authenticate. The gateway searches in this order:

1. The internal users database.

   If the specified user is not defined in this database, the gateway queries the User Directory (LDAP) serversdefined in the Account Unit one at a time, and according to their priority.

   If more than one Account Unit exists, the gateway searches in all at the same time .
2. With multiple servers, the priority for servers can be set only in the scope of one account unit, but not between several account units.
3. If the information still cannot be found, the gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

Session Settings

To open the Session window:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **Mobile Access** and click **Open Mobile Access Policy in SmartConsole**.

   SmartConsole opens and shows the **Mobile Access** tab.

2. From the navigation tree, click **Additional Settings > Session**.

Simultaneous Logins to the Portal

Having a single user logged in to Mobile Access more than once, from two different locations for example, is a potential security issue.

Simultaneous login prevention enables a gateway to automatically disconnect a remote user who is logged more than once.

When simultaneous login prevention is enabled, and a user's authentication information used to log in from two different computers, only the later login is considered legitimate, and the earlier session is logged out.

Configuring Simultaneous Login Prevention

Simultaneous login prevention is configured in SmartConsole from the Mobile Access tab by selecting **Additional Settings > Session.**

The options are:

- **User is allowed several simultaneous logins to the Portal**

  Simultaneous login detection is disabled. This is the default option.

- **User is allowed only a single login to the portal**
  Inform user before disconnecting his previous session (option not selected)

  The earlier user is disconnected and the later user is allowed. The earlier user is logged out. For Mobile Access Portal users, the following message appears: "**Your Mobile Access session has timed out. would you like to sign in again now?**". The later user is not informed that an earlier user is logged in.

- **User is allowed only a single login to the portal** *selected*
  Inform user before disconnecting his previous session (option selected)

  The later user is informed that an earlier user is logged in, and is given the choice of canceling the login and retaining the existing session, or logging in and terminating the existing session. If the existing session is terminated, the user is logged out with the message: "**Your Mobile Access session has timed out. would you like to sign in again now?**".

Tracking of Simultaneous Logins

To track simultaneous login events, select **All Events** in the **Tracking** section of the **Additional Settings > Session** page.

When the gateway disconnects a user, the gateway records a log of the disconnection, containing the connection information of both logins.

All disconnect and connect events create a corresponding entry in the traffic log. The following values of the authentication status field relate to simultaneous logins:

- *Success* - User successfully logged in. Existing active sessions were terminated.
- *Inactive* - User successfully authenticated, but existing sessions need to be terminated prior to logging on.
- *Disconnected* - An existing user session has been terminated because the same user has logged on to another session.

Simultaneous Login Issues

These issues may arise in connection with simultaneous login:

Endpoint Connect- Simultaneous Login Issues

For Endpoint Connect users, Mobile Access does not prevent simultaneous login. This is equivalent to the **User can have several simultaneous logins to the portal** option. An Endpoint Connect user cannot log out another user with the same user name, and cannot be logged out by another user with the same user name.

SecureClient Mobile - Simultaneous Login Issues

With **User can have only a single simultaneous login to the portal** *selected* and **Inform user before disconnecting previous sessions** *not selected* SecureClient Mobile users can be logged off by another user, and can log off other users.

However, the **Inform user before disconnecting his previous session** option does not work, because no message can be sent to those users. User can be logged off, but cannot log off other users.

Other Simultaneous Login Issues

1. When a session is disconnected by another user and SSL Network Extender application mode client is being used, the SSL Network Extender window remains open, while the session is disconnected. Similarly, when a session is disconnected by another user and Secure Workspace is being used, Secure Workspace remains open, while the session is disconnected.
2. When a session is disconnected by another user and Citrix is being used, the Citrix window remains open, while the session is disconnected.

3. All current sessions are deleted when changing the section from **User can have only a single login to the Portal** to **User is allowed several simultaneous logins to the Portal**.

Session Timeouts

Once authenticated, remote users work in a Mobile Access session until they log out or the session terminates. Security best practices provide for limiting the length of active and inactive Mobile Access sessions to prevent abuse of secure remote resources.

Note - Mobile Access uses the system time to keep track of session timeouts. Changing the system time may disrupt existing session timeouts. Therefore, it is recommended to change the system time during low activity hours.

Mobile Access provides two types of session timeouts, both of which are configured in SmartConsole from the Mobile Access tab by selecting **Additional Settings > Session**.

- **Re-authenticate users every** is the maximum session time. When this period is reached, the user must log in again. The default value is 60 minutes. Changing this timeout affects only future sessions, not current sessions.
- **Disconnect idle sessions after** is the disconnection time-out if the connection remains idle. The default value is 15 minutes. When users connect via SSL Network Extender, this timeout does not apply.

For Capsule Clients:

1. Go to **SmartConsole > Mobile Access** tab > **Capsule Workspace Settings > Mobile Profiles**.
2. Create or edit the applicable profile.
3. In the **Access Settings** section, configure the applicable value in the **Session timeout** field.

Roaming

The **Roaming** option allows users to change their IP addresses during an active session.

Note - SSL Network Extender users can always change IP address while connected, regardless of the Roaming setting.

Tracking

Configure Mobile Access to log session activity, including login attempts, logouts, timeouts, activity states and license expiration warnings.

Securing Authentication Credentials

Having multiple users on the same machine accessing the Mobile Access Portal can be a security hazard. A user logged in to the Mobile Access Portal can open a new browser window and get the access of the earlier session. Then the user can browse directly to the Mobile Access Portal without entering the login credentials again.

To make sure authentication credentials are not stolen by others, recommend to users that they log off or close all browser windows when done using a browser.

Mobile Access Authentication Use Cases

Use Case: Two-Factor Authentication with Certificates in Pre-R80 Gateways

Select a main authentication method for pre- R80.x gateways. If you also select **Require client certificate when using Mobile applications** on the **Authentication** page, you require two-factor authentication for Capsule Workspace users: the main authentication method, and certificate.

With these settings, users authenticate to the Mobile Access Portal with only the main authentication method.

Capsule Workspace users receive the certificate information and register only one time. They provide the main authentication method credentials one time per session. Users might also need to enter a passcode, based on settings in the **Capsule Workspace Settings** on the **Mobile Access** tab.

To configure two-factor authentication with certificates for mobile devices on pre-R80.x gateways:

1. Open the gateway object.
2. Select **Mobile Access** > **Authentication**.
3. Select a main authentication method from these options:
   - Username and Password
   - RADIUS
   - SecurID
4. Select **Require client certificate when using Mobile applications** or **Require client certificate when using ActiveSync applications**.
5. Click **OK**.
6. Install policy.

To configure two-factor authentication with the Mobile Access Portal in pre-R80 gateways, see sk86240.

Use Case: Two Factor Authentication with Certificates on R80.x Gateways

You can configure two factor authentication with certificate on an R80.x gateway in these ways:

- Create a new Login Option with Personal Certificate as the first factor and one or more additional methods that you choose as additional factors.
- Use the default Login Option, **Cert_Username_Password**, which includes a personal certificate as the first factor, and username and password as the second factor.

To create a new multi-factor login option that includes certificates:

1. Open the gateway object.
2. Select **Mobile Access** > **Authentication**.
3. In the **Multiple Authentication Clients Settings** table, click **Add** to create a new option.
4. Click **New**.
5. In the **Multiple Login Options** window, enter the Login Option's **Name** and **Display Name**.

   The **Display Name** represents this Login Option to the user upon login and can be a descriptive name.
6. Under **Authentication Methods**, click **Add** to add the first factor.
   a. In the Authentication Factor window, select **Personal Certificate**. Note that Personal Certificate must be the first authentication factor.
   b. Configure the Authentication settings.
   c. Click **OK**.
7. Under **Authentication Methods**, click **Add** to add the second factor.
   a. In the Authentication Factor window, select RADIUS, SecurID, DynamicID or Username and Password.
   b. Configure the Authentication settings, if necessary.
   c. Click **OK**.
8. To apply this Login Option only to the Mobile Access Portal or only to Capsule Workspace on mobile devices, under **Usage in Gateway**, select one or both client types.
9. Click **OK**.
10. Install policy.

To use the built-in default Login Option Cert_Username_Password:

1. Open the gateway object.
2. Select **Mobile Access** > **Authentication**.
3. In the **Multiple Authentication Clients Settings** table, click **Add**.
4. Select **Cert_Username_Password** from the list.
5. To apply this Login Option only to the Mobile Access Portal or only to Capsule Workspace on mobile devices:
   a. In the **Multiple Authentication Clients Settings** table, select **Cert_Username_Password** and click **Edit**.
   b. Under **Usage in Gateway**, select one or both client types.
6. Click **OK**.
7. Install policy.

Note - The Login Options configured in the Multiple Authentication Clients Settings list are only available to clients that support multiple login options. To see which clients support the new multiple login options, see sk111583.

Use Case: Users Selecting a Login Option on R80.x Gateways

When more than one Login Option is configured, and users connect with clients that support Multiple Login Options, users select a Login Option to use when they log in.

In the Mobile Access Portal, in the login page, users see a drop-down list with all available login options, shown by their Display Name.

In the Capsule Workspace mobile application, users select the Login Option on the first connection to the gateway. On subsequent connections, the same login option is shown automatically.

Policy Installation Targets

What can I do here?

Use this window to select installation targets for the policy.

Getting Here - SmartConsole > Install Policy > Policy Targets button

Working with Policy Packages

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

- **Access Control** - consists of these types of rules:
  - Firewall
  - NAT
  - Application & URL Filtering
  - Content Awareness
- **QoS** - Quality of Service rules for bandwidth management
- **Desktop Security** - the Firewall policy for endpoint computers that have the Endpoint Security VPN remote access client installed as a standalone client.
- **Threat Prevention** - consists of:
  - IPS - IPS protections continually updated by IPS Services
  - Anti-Bot - Detects bot-infected machines, prevents bot damage by blocking bot commands and Control (C&C) communications
  - Anti-Virus - Includes heuristic analysis, stops viruses, worms, and other malware at the gateway
  - Threat Emulation - Detects zero-day and advanced polymorphic attacks by opening suspicious files in a sandbox
  - Threat Extraction- Extracts potentially malicious content from e-mail attachments before they enter the corporate network
- **HTTPS Inspection** - Consists of rules to inspect traffic encrypted by the Transport Layer Security (TLS) protocol between internal browser clients and web servers.

Important - Legacy SmartDashboard does not show the QoS and Desktop policies when an administrator with read-only permissions is logged in, and the "Desktop Security" policy is enabled in the policy package.

The installation process:

- Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.

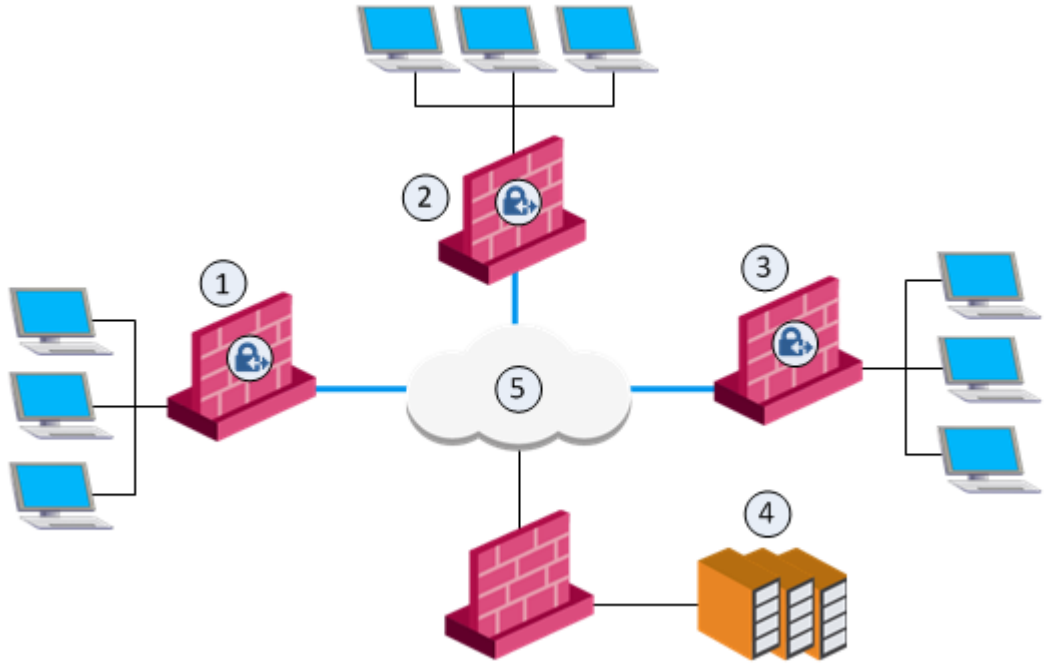
  If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

- Makes sure that each of the Security Gateways enforces at least one of the rules. If none of the rules are enforced, the default drop rule is enforced.
- Distributes the user database and object database to the selected installation targets.

You can create different policy packages for different types of sites in an organization.

Example

An organization has four sites, each with its own requirements. Each site has a different set of Software Blades installed on the Security Gateways:



Item	Security Gateway	Installed Software Blades
1	Sales California	Firewall, VPN
2	Sales Alaska	Firewall, VPN, IPS, DLP
3	Executive management	Firewall, VPN, QoS, and Mobile Access
4	Server farm	Firewall
5	Internet	

To manage these different types of sites efficiently, you need to create three different Policy Packages . Each Package includes a combination of policy types that correspond to the Software Blades installed on the site's Security Gateway. For example:

- A policy package that includes the Access Control policy type. The Access Control policy type controls the firewall, NAT, Application & URL Filtering, and Content Awareness Software Blades. This package also determines the VPN configuration.

  Install the Access Control policy package on *all* Security Gateways.

- A policy package that includes the QoS policy type for the QoS blade on Security Gateway that manages bandwidth.

  Install this policy package on the *executive management* Security Gateway.

- A policy package that includes the Desktop Security Policy type for the Security Gateway that handles Mobile Access.

  Install this policy package on the *executive management* Security Gateway.

Creating a New Policy Package

1. From the Menu, select **Manage policies and layers**.

   The **Manage policies and layers** window opens.

2. Click **New**.

   The **New Policy** window opens.

3. Enter a name for the policy package.

4. In the **General** page > **Policy types** section, select one or more of these policy types:

   - **Access Control & HTTPS Inspection**
   - **Threat Prevention**
   - **QoS**, select **Recommended** or **Express**
   - **Desktop Security**

   To see the **QoS**, and **Desktop Security** policy types, enable them on one or more Gateways:

   Go to gateway editor > **General Properties** > **Network Security** tab:

   - For QoS, select **QoS**
   - For Desktop Security, select **IPSec VPN** and **Policy Server Pol**

5. On the **Installation targets** page, select the gateways the policy will be installed on:

- **All gateways**
- **Specific gateways** - For each gateway, click the [+] sign and select it from the list.

To install Policy Packages correctly and eliminate errors, each Policy Package is associated with a set of appropriate installation targets.

6. Click **OK**.
7. Click **Close**.

   The new policy shows on the **Security Policies** page.

Adding a Policy Type to an Existing Policy Package

1. From the Menu, select **Manage policies and layers**.

   The **Manage policies and layers** window opens.
2. Select a policy package and click the **Edit** button.
3. The **New Policy** package window opens.
4. On the **General** > **Policy types** page, select the policy type to add:
   - **Access Control& HTTPS Inspection**
   - **Threat Prevention**
   - **QoS**, select **Recommended** or **Express**
   - **Desktop Security**
5. Click **OK**.

Installing a Policy Package

1. On the Global Toolbar, click **Install Policy**.

   The **Install Policy** window opens and shows the installation targets (Security Gateways).
2. From the **Select a policy** menu, select a policy package.
3. Select one or more policy types that are available in the package.
4. Select the **Install Mode**:

- **Install on each selected gateway independently** - Install the policy on each target gateway independently of others, so that if the installation fails on one of them, it doesn't affect the installation on the rest of the target gateways.

  Note - If you select **For Gateway clusters install on all the members, if fails do not install at all**, the Security Management Server makes sure that it can install the policy on all cluster members before it begins the installation. If the policy cannot be installed on one of the members, policy installation fails for all of them.

- **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all the target gateways. If the policy fails to install on one of the gateways, the policy is not installed on other target gateways.

5. Click **Install**.

Installing the User Database

When you make changes to user definitions through SmartConsole, they are saved to the user database on the Security Management Server. User authentication methods and encryption keys are also saved in this database. The user database does **not** contain information about users defined externally to the Security Gateway (such as users in external User Directory groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the Security Management Server.

You must choose to install the policy or the user database, based on the changes you made:

- Install the policy, if you modified additional components of the Policy Package (for example, added new Security Policy rules) that are used by the installation targets
- Install the user database, if you only changed the user definitions or the administrator definitions - from the Menu, select **Install Database**

The user database is installed on:

- Security Gateways - during policy installation
- Check Point hosts with one or more Management Software Blades enabled - during database installation

You can also install the user database on Security Gateways and on a remote server, such as a Log Server, from the command line interface on the Security Management Server.

To install user database from the command line interface:

On the Security Management Server, run in the Expert mode:

```
fwm dbload <Main IP address of Name of Security Gateway Object>
```

For more information, see the *R81.10 CLI Reference Guide* - Chapter *Security Management Server Commands* - Section *fwm* - Sub-section *fwm dbload*.

Note - Check Point hosts that do not have active Management Software Blades do not get the user database installed on them.

Uninstalling the Access Control policy

You can uninstall the Access Control policy using the command line interface on the Security Gateway.

To uninstall the Access Control policy

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Run:

```
fw unloadlocal
```

Warning

- The "`fw unloadlocal`" command prevents all traffic from passing through the Security Gateway (Cluster Member), because it disables the IP Forwarding in the Linux kernel on the Security Gateway (Cluster Member).
- The "`fw unloadlocal`" command removes all policies from the Security Gateway (Cluster Member). This means that the Security Gateway (Cluster Member) accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

For more information, see the *R81.10 CLI Reference Guide* - Chapter *Security Gateway Commands* - Section *fw* - Sub-section *fw unloadlocal*.

For uninstalling other Security Policies, check the relevant Administration Guides.

Custom Rule Field Settings

What can I do here?

Use this window to give custom names to the fields in the summary tab.

Getting Here - Security Policies > Access Control > Policy > Summary tab > click the pencil icon.

Policies - Viewing All and Recent

What can I do here?

Use this window to view all the policies or recent policies.

Getting Here - Security Policies > click (+) tab > Manage Policies

Managing Policies and Layers

What can I do here?

Use this window to view, edit, delete policies or create new ones.

Getting Here - Menu > Manage policies and layers
Or:
Security Policies > click (+) tab > Manage Policies > Manage policies and layers link

Working with Policy Packages

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

- **Access Control** - consists of these types of rules:
  - Firewall
  - NAT
  - Application and URL Filtering
  - Content Awareness
- **QoS** - Quality of Service rules for bandwidth management
- **Desktop Security** - the Firewall policy for endpoint computers that have the Endpoint Security VPN remote access client installed as a standalone client.
- **Threat Prevention** - consists of:
  - IPS - IPS protections continually updated by IPS Services
  - Anti-Bot - Detects bot-infected machines, prevents bot damage by blocking bot commands and Control (C&C) communications

- Anti-Virus - Includes heuristic analysis, stops viruses, worms, and other malware at the gateway
- Threat Emulation - Detects zero-day and advanced polymorphic attacks by opening suspicious files in a sandbox
- Threat Extraction - Extracts potentially malicious content from e-mail attachments before they enter the corporate network

- HTTPS Inspection - Consists of rules to inspect traffic encrypted by the Transport Layer Security (TLS) protocol. between internet browser clients and web servers.

The installation process:

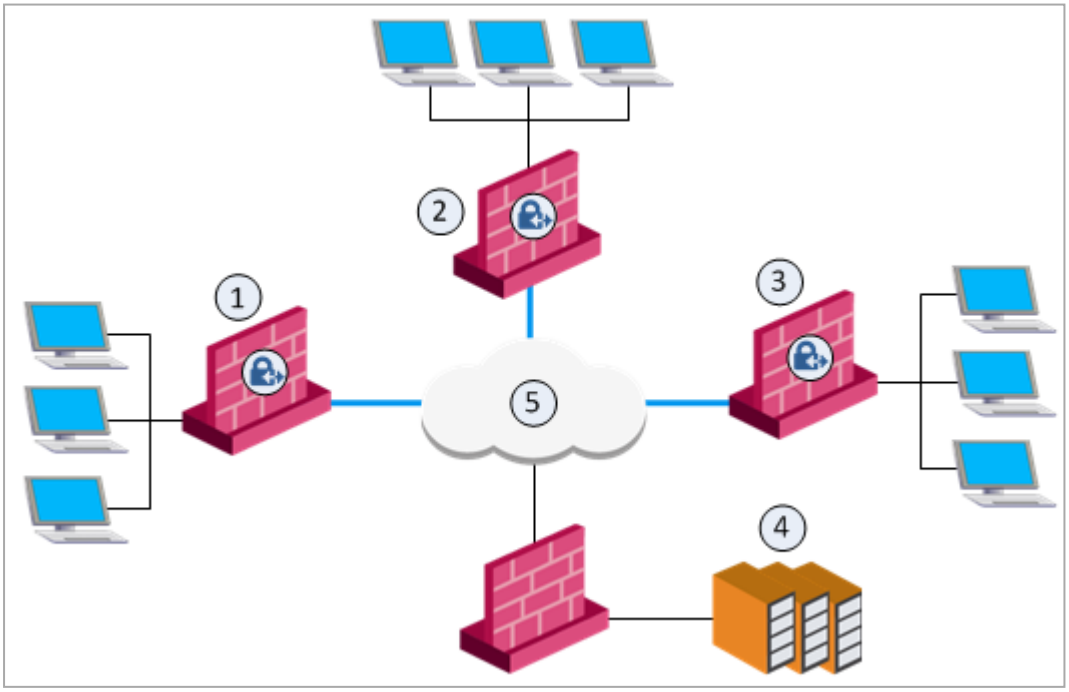
- Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.

  If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.
- Makes sure that each of the Security Gateways enforces at least one of the rules. If none of the rules are enforced, the default drop rule is enforced.
- Distributes the user database and object database to the selected installation targets.

You can create different policy packages for different types of sites in an organization.

Example:

An organization has four sites, each with its own requirements. Each site has a different set of Software Blades installed on the Security Gateways:



Item	Security Gateway	Installed Software Blades
1	Sales California	Firewall, VPN
2	Sales Alaska	Firewall, VPN, IPS, DLP
3	Executive management	Firewall, VPN, QoS, and Mobile Access
4	Server farm	Firewall
5	Internet	

To manage these different types of sites efficiently, you need to create three different Policy Packages. Each Package includes a combination of policy types that correspond to the Software Blades installed on the site's gateway. For example:

- A policy package that includes the Access Control policy type. The Access Control policy type controls the firewall, NAT, Application and URL Filtering , and Content Awareness Software Blades. This package also determines the VPN configuration.

  Install the Access Control policy package on *all* Security Gateways.

- A policy package that includes the QoS policy type for the QoS blade on gateway that manages bandwidth.

  Install this policy package on the *executive management* Gateway.

- A policy package that includes the Desktop Security Policy type for the gateway that handles Mobile Access.

  Install this policy package on the *executive management* Gateway.

Policy Packages

What can I do here?

Use this window to edit a policy package.

Getting Here - Security Policies > Access Control / Custom Threat Prevention / Autonomous Threat Prevention / HTTPS Inspection > Right-click Policy > Edit Policy
Or:
Menu > Manage polices and layers > New or Edit.

Installing a Policy Package

1. On the Global Toolbar, click **Install Policy**.

   The **Install Policy** window opens showing the installation targets (Security Gateways).

2. From the **Select a policy** menu, select a policy package.

3. Select one or more policy types that are available in the package.
4. Select the **Install Mode**:
   - **Install on each selected gateway independently** - Install the policy on each target gateway independently of others, so that if the installation fails on one of them, it doesn't affect the installation on the rest of the target gateways.

     Note - If you select **For Gateway clusters install on all the members, if fails do not install at all**, the Security Management Server makes sure that it can install the policy on all cluster members before it begins the installation. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all the target gateways. If the policy fails to install on one of the gateways, the policy is not installed on other target gateways.
5. Click **Install**.

Uninstalling a Policy Package

You can uninstall a policy package through a command line interface on the gateway.

To uninstall a policy package:

1. Open a command prompt on the Security Gateway.
2. Run: `fw unloadlocal`.

Warnings:

- The `fw unloadlocal` command prevents all traffic from passing through the Security Gateway, because it disables the IP Forwarding in the Linux kernel.
- The `fw unloadlocal` command removes all policies from the Security Gateway. This means that the Security Gateway accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

Creating a New Policy Package

1. From the Menu, select **Manage policies and layers**.

   The **Manage policies and layers** window opens.
2. Click **New**.

   The **New Policy** window opens.
3. Enter a name for the policy package.
4. In the **General** page > **Policy types** section, select one or more of these policy types:

- **Access Control** & **HTTPS Inspection**
- **Threat Prevention**
- **QoS**, select **Recommended** or **Express**
- **Desktop Security**

To see the **QoS**, and **Desktop Security** policy types, enable them on one or more Gateways:

Go to gateway editor > **General Properties** > **Network Security** tab:

- For QoS, select **QoS**
- For Desktop Security, select **IPSec VPN** and **Policy Server**

5. On the **Installation targets** page, select the gateways the policy will be installed on:
   - **All gateways**
   - **Specific gateways** - For each gateway, click the [**+**] sign and select it from the list.

   To install Policy Packages correctly and eliminate errors, each Policy Package is associated with a set of appropriate installation targets.
6. Click **OK**.
7. Click **Close**.

   The new policy shows on the **Security Policies** page.

Adding a Policy Type to an Existing Policy Package

1. From the Menu, select **Manage policies and layers**.

   The **Manage policies and layers** window opens.
2. Select a policy package and click the **Edit** button.
3. The **New Policy** package window opens.
4. On the **General** > **Policy types** page, select the policy type to add:
   - **Access Control** & **HTTPS Inspection**
   - **Threat Prevention**
   - **QoS**, select **Recommended** or **Express**
   - **Desktop Security**
5. Click **OK**.

QoS Policy Types

R81.10 includes two QoS Policy types:

- **Express** - Quickly create basic QoS Policies
- **Recommended** - Create advanced Policies with the full set of QoS features

This table shows the difference between the **Recommended** and **Express** policy types.

Features	Recommended	Express
IPv6 Support	✓	✓
Weights	✓	✓
Limits (whole rule)	✓	✓
Logging	✓	✓
Accounting	✓	✓
Support for hardware acceleration	✓	
High Availability and Load Sharing	✓	✓
Guarantees (Per connection)	✓	
Limits (Per connection)	✓	
LLQ (controlling packet delay in QoS)	✓	
DiffServ	✓	
Sub-rules	✓	
Matching by URI resources	✓	
Matching by DNS string	✓	
SecureXL support	✓	
CoreXL support	✓	
SmartLSM clusters	✓	

To select a QoS Policy type:

1. In SmartConsole menu, click **Manage policies and layers**.
2. In the Manage Policies window, click **New** or select an existing Policy and then click **Edit**.

3. Select **QoS**, and then select **Recommended** or **Express**.

Install Policy

What can I do here?

Use this window to install access control and threat prevention policies on one or more gateways.

- Click the **View Changes** button to see which revisions will be installed
- Click **Policy Targets** to select installation targets

> **Getting Here** - SmartConsole Install Policy button
> Or:
> Ctrl + Shift + Enter

Installing the Access Control Policy

1. On the Global Toolbar, click **Menu** > **Install Policy**.

   The **Install Policy** window opens showing the Security Gateways.

2. If there is more than one Policy package: From the **Policy** drop-down list, select a policy package.
3. Select **Access Control**. You can also select other Policies.
4. If there is more than one gateway: Select the gateways on which to install the Policy.
5. Select the **Install Mode**:

   - **Install on each selected gateway independently** - Install the policy on each target gateway independently of others, so that if the installation fails on one of them, it doesn't affect the installation on the rest of the target gateways.

     Note - If you select **For Gateway Clusters, if installation on a cluster member fails, do not install on that cluster**, the Security Management Server makes sure that it can install the policy on all cluster members before it begins the installation. If the policy cannot be installed on one of the members, policy installation fails for all of them.

   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all the target gateways. If the policy fails to install on one of the gateways, the policy is not installed on other target gateways.

6. Click **Install**.

Concurrent Policy Install

Starting from R81, one administrator or more can run *different* policy installation tasks on multiple gateways at the same time. In earlier versions, you can only run the *same* policy installation task on multiple gateways at the same time.

Concurrent Install Policy only supports the Access Control and Threat Prevention policies. It does not support the Desktop and QoS policies.

The maximum number of policy installation tasks (of different policies) that can run at the same time is 5. If more than 5 policy installation requests are sent, any request beyond the first 5 gets in a queue.

The running and the queued tasks appear in the **Recent Tasks** window at the bottom left of your screen.

Note - In the first installation, you cannot install both the Access Control and Threat Prevention policies on the same gateway at the same time. You must install one and then the other.

Accelerated Policy Install

R81 introduces the Accelerated Install Policy feature for the Access Control policy. When the Access Control policy installation is accelerated, the installation duration is decreased significantly.

Policy installation is accelerated depending on the changes that were made to the Access Control policy since the last installation.

For example, creating a Host object and adding it to an Access Control rule triggers *accelerated* policy installation.

For more information about accelerated install policy and a detailed list on the events that trigger accelerated policy installation, see sk169096.

Installing the Threat Prevention Policy

The IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction Software Blades have a dedicated Threat Prevention policy. You can install this policy separately from the policy installation of the Access Control Software Blades. Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways.

To install the Threat Prevention policy:

1. From the Global toolbar, click **Install Policy**.

   The **Install Policy** window opens showing the installation targets (Security Gateways).
2. Select **Threat Prevention**.
3. Select **Install Mode:**

- **Install on each selected gateway independently** - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.

  If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.

- **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.

4. Click **OK**.

Installing QoS and Desktop Security Policies

1. From the Global toolbar, click **Install Policy**.

   The **Install Policy** window opens showing the installation targets (Security Gateways).

2. In the **Policy** drop-down box, select the relevant policy.
3. In the **Install Mode** area, select one of these:

   - **Install on each selected gateway independently** - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.

     If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.

   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.

4. Click **OK**.

History

What can I do here?

Use this window to see all published changes to the layer. You can see:

- The status of each session after the change was published
- The session name and tags
- The administrator who published the changes
- The time and date of the changes

You can:

- Launch SmartConsole in read-only mode to see the selected session
- Revert to the selected session

Getting Here - Security Policies > Access Control > Policy > Actions > History

Implied Object

What can I do here?

Click on an implied object to see information about it.

Getting Here - Security Policies > Access Control > Policy > Actions > Implied Rules

Install Policy Settings

What can I do here?

Use this window to set installation targets and select an install mode

- To install on each selected gateway independently or
- Install on all selected gateways

Getting Here - Security Policies > Threat Prevention > Custom Policy Tools > Updates > IPS Schedule Update > On successful update perform Install Policy > Configure

Verify Access Control Policy

What can I do here?

Use this window to select an access control policy for verification.

Getting Here - Menu > Verify Access Control Policy

Heuristic Verification

Verify policy evaluates the rules for possible conflicts and redundancy

The installation process runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.

If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

Policy Verification - Task Details

What can I do here?

Use this window to see the results of a policy verification.

Getting Here - Menu > Verify Access Control Policy > Task window > Details link for the task

Task Details - Show More

What can I do here?

Use this window to view all the details generated by a task.

Getting Here - Task window > Details link for the task > Show more

Export List

What can I do here?

Use this window to see exported CSV files. An exported CSV file can show:

- The rules in the rule base of a policy
- Available IPS protections
- Objects in Object Explorer
- A list of Gateways and Servers

Getting Here - Security Policies > Access Control > Policy > Actions > Export
Or:
Security Policies > Threat Prevention > Policy/IPS/Threat Prevention > Actions > Export
Or:
Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Actions > Export
Or:
Object Explorer Actions > Export
Or:
Gateways & Servers > Actions > Export

Legacy User Access at Location

What can I do here?

Use this window to specify user groups in particular locations as the source of an access rule.

Getting Here - Security Policies Access Control > Policy > Source column - right-click > Add legacy user access

Directional Match Condition

What can I do here?

Use this window to configure directional VPN enforcement -- allow VPN connections in one direction only.

Getting Here - Security Policies Access Control > Policy > VPN Column > Directional Match Condition.

Understanding Directional VPN

Configurable Objects in a Direction

The table below shows all the objects that can be configured in a direction, including three new objects created for Directional VPN:

Name of Object	Description
Remote Access	Remote Access VPN community
Site to Site VPN	Regular Star or Mesh VPN community
Any Traffic	Any traffic
All_GwToGw	All Site to Site VPN communities

Name of Object	Description
All_Communities	All Site to Site and Remote Access VPN communities
External_clear	For traffic outside the VPN community
Internal_clear	For traffic between local domains within the VPN community

Note - Clear text connections originating from these objects are not subject to enforcement:

- **Any Traffic**
- **External_clear**
- **Internal_clear**

There is *no limit* to the number of VPN directions that you can configure in a single rule. In general, if you have many directional enforcements, consider replacing them with a standard bidirectional condition.

Directional Enforcement between Communities

VPN Directional Enforcement can take place between two VPN communities. In this case, one gateway must be configured as a member of both communities and the enforcement point between them. Every other peer gateway in both communities must have a route entry to the enforcement point gateway in its `$FWDIR/conf/vpn_route.conf` file.

To add a route entry to the enforcement point gateway:

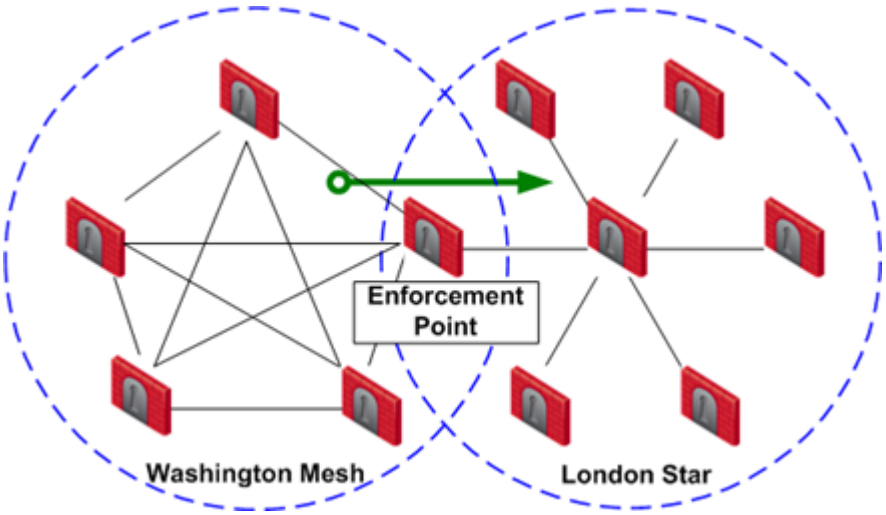
On the management module of each gateway in the community (except for the enforcement point gateway), add an entry in the `$FWDIR/conf/vpn_route.conf` file:

Destination	Next hop router interface	Install on
`< destination_community_obj>`	`< enforcement_point_gw>`	`< managed_FW_object>`

These are the variables in the entry:

- `destination_community_obj` - a network object for the combined encryption domain of the community
- `enforcement_point_gw` - the gateway that is a member of both communities and transfers the encrypted traffic between them
- `managed_FW_object` - all community members that are managed by the management module

In the example below, Washington is a Mesh community, and London is a VPN Star.



The directional VPN rule below must be configured for the enforcement point gateway in the Access Control Policy Rule Base:

Source	Destination	VPN	Services & Applications	Action
*Any	*Any	Washington => London	*Any	Accept

The rule is applied to all VPN traffic that passes through the enforcement point gateway between the Washington and London communities. If a connection is opened from a source in the Washington Mesh, and the destination is in the London Star, the connection is allowed. Otherwise, the connection is denied.

Note - The Directional Enforcement applies only to the first packet of a connection. If the connection is permitted, the following packets of this connection are also permitted, including the packets in the opposite direction.

Application - General

What can I do here?

Use this window to see a description of the application's primary category, risk and match settings.

Getting Here - Access Control > Policy > Services & Applications Column > Select Application > Edit object > General.

Application - Match Settings

What can I do here?

Use this window to see the services recommended for the application, or customize the application by adding new services.

Getting Here - Access Control > Policy > Services & Applications Column > Select Application > Edit object > Match Settings

Category - General

What can I do here?

Use this window to see the category's match settings and related blades.

Getting Here - Access Control > Policy > Services & Applications Column > Select Category > Edit object > General.

Category - Match Settings

What can I do here?

Use this window to see the services recommended for the category, or customize the category by adding new services.

Getting Here - Access Control > Policy > Services & Applications Column > Select Category > Edit object > Match Settings

Service with Resource

What can I do here?

Use this window to select a service and a resource. The applications layer checks defined in the resource are applied to the service.

Getting Here - Access Control > Policy > Services & Applications Column > Right-click in cell > Add Service with Resource

Understanding Services with Resources

Resources are used to match a specific kind of application layer content, in other words, to specify what content you are looking for, and to perform some action on the content.

Resources are used with security servers. By default, the enabled security servers are HTTP, FTP, SMTP, Rlogin and Telnet. Only the services that can be used with these security servers are displayed here.

In addition, there is a generic TCP security server that can be used with any TCP service. Every TCP Service has a property called **Enable for TCP Resource** in the **Advanced TCP Service Properties** window that allows the service to be used with the generic TCP security server. If that property is enabled, that service(s) appears in the list. Services do not have this property enabled by default.

Action Settings

What can I do here?

Use this window to configure UserCheck options and set an action for the access rule.

Getting Here - Security Policies > Access Control > Policy > Action column > More

Actions

Action	Description
Accept	Accepts the traffic
Drop	Drops the traffic. The Firewall does not send a response to the originating end of the connection and the connection eventually does a time-out. If no UserCheck object is defined for this action, no page is displayed.
Ask	Asks the user a question and adds a confirmatory check box, or a reason box. Uses a UserCheck object.
Inform	Sends a message to the user attempting to access the application or the content. Uses a UserCheck object.

To see these actions, right-click and select More:

Reject	Rejects the traffic. The Firewall sends an RST packet to the originating end of the connection and the connection is closed.
UserCheck Frequency	Configure how often the user sees the configured message when the action is ask, inform, or block.

Action	Description
Confirm UserCheck	Select the action that triggers a UserCheck message: ■ **Per rule** - UserCheck message shows only once when traffic matches a rule. ■ **Per category** - UserCheck message shows for each matching category in a rule. ■ **Per application/Site** - UserCheck message shows for each matching application/site in a rule. ■ **Per Data type** - UserCheck message shows for each matching data type.
Limit	Limits the bandwidth that is permitted for a rule. Add a Limit object to configure a maximum throughput for uploads and downloads.
Enable Identity Captive Portal	Redirects HTTP traffic to an authentication (captive) portal. After the user is authenticated, new connections from this source are inspected without requiring authentication.

Important - A rule that drops traffic, with the **Source** and **Destination** parameters defined as **Any**, also drops traffic to and from the Captive Portal.

Data Type

What can I do here?

Use this window to edit properties of the data type.

Getting Here - Security Policies > Access Control > Policy > Content column > Double-click a data type.
Or:
Menu > New Object > More Object Types > Data Type

Data Type Group

What can I do here?

Use this window to create or edit a data type group.

Getting Here - Security Policies > Access Control > Policy > Content column > add new items > New > Data Type Group
Or:
Menu > New Object > More Object Types > Data Type > New Data Type Group

Data Type - General Properties

- **Name** - Name of the data type representation.
- **Comment** - Optional comments and notes.
- **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.

Group Data Type Fields

The Content Awareness engine matches files to the Group Data Type if the *File Type* and the *Content Type* are matched.

File Type

- At least one file type must be matched. You can select *Any*. *Any* includes files, emails and web posts. *Any File* is only for files.

Content Type

- At least one content type must be matched. You can select *Any*.

Data Type - Any file

What can I do here?

In this window you can see the properties of the "Any File" Data Type. This Data Type matches any file type. You cannot change its properties.

> **Getting Here** - Security Policies > Access Control > Policy > Content column > add new items > Search for "Any File"

Data Type - General Properties

- **Name** - Name of the data type representation.
- **Comment** - Optional comments and notes.
- **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.

Keyword Data Type

What can I do here?

Use this window to create or edit a keyword data type. This is a list of words.

Data that is matched for this list of words and the threshold that you set here is logged as a Data Loss Prevention incident and handled according to the action of the rule.

Getting Here - Security Policies > Access Control > Policy > Content column > add new items > New > Keywords
Or:
Menu > New Object > More Object Types > Data Type > Data Type > New Keywords

Data Type - General Properties

- **Name** - Name of the data type representation.
- **Comment** - Optional comments and notes.
- **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.

Keywords Data Type Fields

Search List

- **Specify keywords or phrases to search for** - Click **+** to add the keyword to the list of this data type.

Threshold

This data will be matched only if it contains:

- **All keywords and phrases** - Select if the data will be matched to the rule only if all the words in the list appear in the data contents. Clear if any of the words may appear.
- **At least <number> keywords or phrase** - Define how many of the words in the list must appear in the contents of the data to match the rule.

If some of the words are more important than others (the rule should be matched if certain words of the list appear, and if all appear), consider using a Weighted Keyword data type rather than the simple Keyword type.

Weighted Keyword Data Type

What can I do here?

Use this window to create or edit a weighted keyboard data type. Use this type of data when different words have different importance.

For example, if "price list" is used in conjunction with other words such as "current", "reseller", "discount", it should be suspicious; but the other words may be fine, even together, without "price list".

Getting Here - Security Policies > Access Control > Policy > Content column > add new items > New > Weighted Keywords
Or
Menu > New Object > More Object Types > Data Type > Data Type > New Weighted Keywords

Data Type - General Properties

- **Name** - Name of the data type representation.
- **Comment** - Optional comments and notes.
- **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.

Weighted Keywords Data Type Fields

- **Weighted Keywords or Phrases** - Click **+** to add a new keyword or phrase.
- **Threshold** - Define the number of appearances, by weight, of all the keywords that, beyond this threshold, the data containing this list of words or phrases will be recognized as data to be protected.

Weighted Keywords or Phrases

What can I do here?

Use this window to create or edit a weighted keyword or phrase.

Getting Here - Security Policies > Access Control > Policy > Content column > add new items > New > Weighted Keywords > Weighted keywords or phrases > click +
Or:
Menu > New Object > More Object Types > Data Type > Data Types > New Weighted keywords > Weighted keywords or phrases

Weighted Keyword Data Type Fields

Keyword

Enter the weighted keyword.

Weight

- **Each appearance of this word contributes the following weight <number>** - Enter a number to represent the importance of this word in recognizing the data as matching the data type.
- **The weight of this word is limited to <number>** - Set a ceiling for the sum of keywords in one message or file.

Regular Expression

- **This keyword is a Regular Expression** - Select to have the weighted keyword analyzed as a pattern, rather than text. Use Check Point supported regular expressions.

Traditional Data Type Group

What can I do here?

Use this window to create or edit a group data type.

> **Getting Here** - Security Policies > Access Control > Policy > Content column > add new items > More > Traditional Data Type Group
> Or:
> Menu > New Object > More Object Types > Data Type > More > New Traditional Data Type Group

Data Type - General Properties

- **Name** - Name of the data type representation.
- **Comment** - Optional comments and notes.
- **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.

Traditional Group Data Type Fields

Traditional Data type groups are matched on OR. If data matches any of the data types in the group, the data type group is matched.

Members

- Click **+** to add a data type.
- Double-click a selected item to edit it. Changes are applied to all the member data type

and all data types and rules that use it.

- Click **X** to remove a selected item from the group. This does not delete it.

File Attribute Data Type

What can I do here?

Use this window to create or edit a file attribute data type.

> **Getting Here** - Security Policies > Access Control > Policy > Content column > add new items > New > File Attributes
> Or:
> Menu > New Object > More Object Types > Data Type > Data Type > New File Attributes

Data Type - General Properties

- **Name** - Name of the data type representation.
- **Comment** - Optional comments and notes.
- **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.

File Attribute Data Type Fields

Select the conditions that should be checked on files in data transmissions (including zipped email attachments, as well as other transmissions). A transmitted file must match all selected conditions for the File data type to be matched.

- **The file belongs to one of these file groups** - Click **+**, and select a files type from the list.
- **The file name contains** - Enter a string or regular expression to match against file names.
- **The file size is larger than** - Enter the threshold size in KB.

Compound Data Type

What can I do here?

Use this window to create or edit a compound data type.

> **Getting Here** - Security Policies > Access Control > Policy > Content column > add new items > New > Compound Data Type Group
> Or:
> Menu > New Object > More Object Types > Data Type > More > New compound Data Type Group

Data Type - General Properties

- **Name** - Name of the data type representation.
- **Comment** - Optional comments and notes.
- **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.

Compound Data Type Fields

A Compound Data Type is based on multiple data types. The relationship between the data types may be:

- AND (all the data types must be present to match traffic),
- NOT (if none of the data types are present, the traffic matches),
- A combination of AND and NOT (if traffic has all data types in the first list, and none of the data types in the second list, it matches this data type).

Members

You must add at least one data type to at least one of the lists.

- **Each one of these data types must be matched** - Select existing data types to add. Traffic must match all the data types of this group to match a rule using this compound data type.
- **Each one of these data types must not be matched** - Select existing data types to add to the definition. Traffic that does not contain any data matching the types in this list will match this compound data type.

  Notes:

  - If you edit the properties of a selected data type. Any changes you make apply to the data type itself.
  - If you remove the selected data type from the compound data type. This action does not affect the data type itself.

Patterns (RegEx)

What can I do here?

Use this window to create or edit pattern (RegEx) data types.

Getting Here - Menu > New Object > More Object Types > Data Type > Data Type > New Patterns (RegEx)

Data Type - General Properties

- **Name** - Name of the data type representation.
- **Comment** - Optional comments and notes.
- **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.

Pattern (RegEx) Fields

Pattern List

- **Type a pattern** - When you start to type the regular expression, the **+** is enabled. Click **+** to add the pattern to the list of this data type.

Threshold

- **Number of occurrences <number>** - Define how many times the patterns must appear to be considered data to be protected. If you want to set different occurrences for different patterns, consider using **Weighted Keywords** as the data type.

Track Settings

What can I do here?

Use this window to configure Track Settings.

Getting Here - Security Policies > Access Control > Policy > Track Column > More

Tracking Options

Select these options in the **Track** column of a rule:

- **None** - Do not generate a log.
- **Log** -This is the default **Track** option. It shows all the information that the Security Gateway used to match the connection. At a minimum, this is the Source, Destination, Source Port, and Destination Port. If there is a match on a rule that specifies an application, a session log shows the application name (for example, Dropbox). If there is a match on a rule that specifies a Data Type, the session log shows information about the files, and the contents of the files.
- **Accounting** - Select this to update the log at 10 minutes intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.

Note - When upgrading from R77.xx or from R80 to R81.10, there are changes to the names of the options in the **Track** column. To learn more see sk116580.

Advanced Track options

Detailed Log and **Extended Log** are only available if one or more of these Blades are enabled on the Layer: *Application & URL Filtering*, *Content Awareness*, or *Mobile Access*.

- **Detailed Log** -Equivalent to the *Log* option, but also shows the application that matched the connections, even if the rule does not specify an application. **Best Practice** -Use for a cleanup rule (Any/Internet/Accept) of an Applications and URL Filtering Policy Layer that was upgraded from an R77 Application Control Rule Base.
- **Extended Log** -Equivalent to the *Detailed* option, but also shows a full list of URLs and files in the connection or the session. The URLs and files show in the lower pane of the **Logs** view.

Log Generation

- **per Connection** - Select this to show a different log for each connection in the session. This is the default for rules in a Layer with only *Firewall* enabled. These are basic firewall logs.
- **per Session** - Select this to generate one log for all the connections in the same session. This is the default for rules in a Layer with *Applications and URL Filtering* or *Content Awareness* enabled. These are basic Application Control logs.
  - **Enable Firewall Sessions** - If **per session** is enabled, a session log will be generated. If you want to log only sessions with applications (without the firewall session) then disable **Enable Firewall Sessions**. Note - this is only for layers with application control.

Alert:

For each alert option, you can define a script in **Menu** > **Global Properties** > **Log and Alert** > **Alerts**.

- **None** - Do not generate an alert.
- **Alert** - Generate a log and run a command, such as: Show a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in the **Global Properties**.
- **SNMP** - Send an SNMP alert to the SNMP GUI, or run the script defined in the **Global Properties**.
- **Mail** - Send an email to the administrator, or run the mail alert script defined in the **Global Properties**.
- **User Defined Alert** - Send one of three possible customized alerts. The alerts are defined by the scripts specified in the **Global Properties**.

Log Sessions

A session is a user's activity at a specified site or with a specified application. The session starts when a *user* connects to an *application* or to a *site*. The Security Gateway includes all the activity that the user does in the session in one session log.

To search for log sessions:

In the **Logs** tab of the **Logs & Monitor** view, search for `type:Session`

To see details of the log session:

In the **Logs** tab of the **Logs & Monitor** view, select a session log.

In the bottom pane of the **Logs** tab, click the tabs to see details of the session log:

- **Connections** - Shows all the connections in the session. These show if **Per connection** is selected in the **Track** option of the rule.
- **URLs** - Shows all the URLs in the session. These show if **Extended Log** is selected in the **Track** option of the rule.
- **Files** - Shows all the files uploaded or downloaded in the session. These show if **Extended Log** is selected in the **Track** option of the rule, or if a Data Type was matched on the connection.

To see the session log for a connection that is part of a session:

1. In the **Logs** tab of the **Logs & Monitor** view, double-click on the log record of a connection that is part of a session.
2. In the **Log Details**, click the session icon (in the top-right corner) to see the session log.

To configure the session timeout:

By default, after a session continues for three hours, the Security Gateway starts a new session log. You can change this in SmartConsole from the **Manage & Settings** > **Blades** > **Application and URL Filtering** > **Advanced Settings** > **General** > **Connection unification**.

For sessions that are blocked by the Access Control Policy, the Security Gateway starts a new session log after 30 seconds. A blocked session log include all the connections that are blocked in this period.

New User Auth

What can I do here?

Use this window to define User Authentication properties for the Rule:

- How to handle the user when the allowed location of the user is different than the location allowed to the user in the Rule.
- Access to HTTP servers

Getting Here - Security Policies > Access Control > Policy > Action column > More > In the Actions Settings window select User Auth > click pencil icon:



Note - The User Auth option is available for layers that only have the firewall blade enabled.

User Auth Options

Source/Destination

- **Intersect with User Database** - The more restrictive access privileges of the rule and the user account properties are applied. If the **User Properties** > **Location** for a user does not allow this location, the user will be denied. If the rule blocks the user, the user will be denied, even if the Location is allowed.
- **Ignore User Database** - Access is given or denied according to the rule. The user account properties are ignored.

HTTP

- **Allow Predefined Servers Only** - Activates the Reauthentication options defined for the HTTP servers, and allows users to access only the servers in **Global Properties** > **Security Servers** > **HTTP servers**.
- **Allow All Servers** - Ignores Reauthentication options. If you are in transparent mode, it is not necessary to define the servers.

Best Practice - Use *Allow All Servers* with caution. It allows users to continue to any port.

Client Auth

What can I do here?

Use this window to define:

- How to handle a Client Authentication user when the allowed location in the User definition is different than the location allowed to the user in the Rule.
- The Sign On method
- Tracking for successful authentications.

Getting Here - Security Policies > Access Control > Policy > Action column > More > In the actions settings window select Client Auth > click pencil icon:



Note - The Client Auth option is available for layers that only have the firewall blade enabled.

Understanding Client Authentication

Client Authentication can be used to authenticate any service. It allows access from a specific IP address for an unlimited number of connections. The user working on a client performs the authentication by successfully meeting an authentication challenge, but it is the client machine that is granted access.

Client authentication can be used with any one of five different sign on methods. These sign on methods provide a choice of Authentication Methods for authenticated and other services. For all sign on methods other than Manual Client Authentication, the Check Point Security Gateway is transparent to the user. This means that the user authenticates directly to the destination host.

There is one other choice to make with Client Authentication: whether to use Standard Sign On or Specific Sign On.

At the end of the session, the user can sign off. When a user signs off, he or she is signed off from all services, and the connection is closed by the remote host.

Client Auth - General Options

Source and **Destination**

- *Intersect with User Database* means that if a user who successfully authenticates is at a source or trying to reach a destination which is allowed to the user according to the rule, but the **User Properties** for that user do not allow this location, the user will be denied.
- *Ignore User Database* - Users who would otherwise denied as a result of the allowed source or destination defined in the **User Properties** are allowed anyway.

Due to the nature of Client Authentication, it is not possible for the Client authentication process to know where the client may be connecting *to* when the **Required sign On** is set to **Standard** , so the user's allowed destinations cannot be checked.

- **Apply Rule Only if Desktop Configuration Options are Verified** controls the Secure Client Verification (SCV) for SecureClient connections. These connections can be either encrypted, for clients connecting via remote access, or unencrypted, where the SecureClient is on a LAN. If a user is successfully Client authenticated, they are only allowed access if the client machine is verified to be secure.

Sign On

- **Standard** allows the user to log in and be automatically authorized for all services that the rule allows, without having to perform authentication for each service.
- **Specific** requires the user to individually authorize each service and each host he/she will be trying to contact.

Sign On Method

- **Manual** - Manual Sign on is available for any service, as long as it is specified in the Client Authentication rule.

  In Manual Sign On, the user must first connect to the gateway in order to authenticate (in other words, the authentication is not transparent). The user must authenticate in one of the two ways:

  - A TELNET session to the gateway on port 259.
  - An HTTP connection to the gateway on port 900, through a Web browser. The requested URL must include the gateway name and the port number, such as http://gateway:900

- **Partially Automatic** - If the service is RLOGIN, Telnet, HTTP, or FTP, User Authentication can be used to perform a Standard Sign On. Other services cannot be authenticated in this way.

  As part of the configuration, make sure that port 80 is accessible on the gateway machine.

- **Fully Automatic** - Fully Automatic Sign On is available for any service, as long as the required service are specified in the Client Authentication rule.

  If the user attempts a connection to a remote host using an authenticated service (TELNET, FTP, HTTP, and RLOGIN), he or she are asked to authenticate by means of User Authentication. If the user attempts a connection to a remote host using any other service, he or she are asked to authenticate by means of the Session Authentication agent, which must be properly installed.

  As part of the configuration, make sure that port 80 is accessible on the gateway machine.

- **Agent Automatic Sign On** - Agent Automatic Sign On is available for any service, as long as the required service are specified in the Client Authentication rule, and as long as the Session Authentication agent is properly installed. If the user attempts a connection to a remote host using any service, he or she are asked to authenticate by means of the Session Authentication agent.

- **Single Sign On** - Single Sign On is available for any service, as long as the required service are specified in the Client Authentication rule. UserAuthority must be installed. Single Sign On is the Check Point address management feature that provides transparent network access. In this method, the Check Point Security Gateway consults the user IP address records to determine which user is logged on at a given IP address. If a connection matches a Single Sign On enabled rule, the Check Point Security Gateway sends a query to the UAS (UserAuthority server) with the packet's source IP. The UAS returns the name of the user who is registered to the IP. If the user's name is authenticated, the packet is accepted; if not, it is dropped.

Successful Authentication Tracking

- **None** means nothing is logged when a user authenticates successfully against this rule.
- **Log** generates a log entry upon successful authentication.
- **Alert** sends the Alert defined in the **Global Properties** .

Client Auth - Limits

What can I do here?

Use this window to set:

- Client authentication timeout
- Permitted number of Client Authentication sessions.

> **Getting Here** - Security Policies > Access Control > Policy > Action column > More > In the actions settings window select Client Auth > click pencil icon > Limits
> **Note** - The Client Auth option is available for layers that only have the firewall blade enabled.

Client Authentication - Limit Options

Authorization Timeout

The Authorization Timeout specifies the length of time after the client is authenticated, during which the specified service will be available to all sessions from the source IP address specified under **Source** in the relevant rule in the Rule Base.

- **Indefinite** means that either the user must explicitly sign off, or the Check Point Security Gateway administrator must stop and start the Security Gateway in order for the user to no longer be permitted.
- **Hours** and **Minutes** allows a time limited authorization timeout to be defined.
- **Refreshable Timeout** means the Authorization Timeout period is reset with every new connection authorized by the rule.

Number of Sessions Allowed

Number of Sessions Allowed refers to the number of individual connections the user is allowed to make through the firewall before the authentication expires.

- **Infinite** does not restrict the number of sessions.

Note - With HTTP (or any service that makes many individual connections), the default five connections are quickly used.

Encrypt

What can I do here?

Use this window to configure the encryption schemes and methods of integrity used by this rule during the second phase of IKE.

Getting Here - Security Policies > Access Control > Policy (Traditional mode) > Action column > More > Encrypt > Edit

Encrypt - Transform Options

Specify the methods negotiated in IKE phase 2 and used in IPsec connections. For example, if AES-128 and SHA1 are agreed upon in phase 2, all IPsec connections matching the **Encrypt** security rule are built using these methods.

- **Encryption Algorithm** - Selects one of the algorithms from the drop-down list.
- **Data Integrity** - Selects the cryptographic checksum method to be used for ensuring data integrity.
- **Compression Method** - Selects the compression method to use.
- The encrypted connection can be configured to compress data using the deflate compression method. This reduces bandwidth needs and costs.
- **Allowed Peer Gateway** - Selects the Security Gateways that are allowed to accept encrypted connections.
- **Use Perfect Forward Secrecy**- Select this option, if you need high security.

  By default, although IPsec encryption keys are replaced every Phase 2 renegotiation, the older key material has some impact on the new key. If higher security level is required, it is possible to use Perfect Forward Secrecy (PFS) and have fresh key material each time. To enable, select **Use Perfect Forward Secrecy**. This mode of operation requires another Diffie-Hellman key, and the Diffie-Hellman group is configurable.

  You can determine how often to renegotiate the IPsec SA - how often to repeat IKE phase 2. By default the SA is valid for one hour.

- **Use DH Group** - Selects the Diffie-Hellman group for the new encryption key.
- **Perform IP Pool NAT** - Allows range of IP addresses to be routable to the Security Gateway.

  An IP Pool is a range of IP addresses (an **Address Range**, a **Network** or a **Group** of one of these objects) routable to the Security Gateway.

  IP Pool NAT ensures proper routing for two connection scenarios:

  - SecuRemote/SecureClient to a MEP (Multiple Entry Point) Gateway connections.
  - Gateway to a MEP Gateway connections.

  To use IP Pools, you must first enable IP Pool NAT in SmartConsole > **Menu** > **Global properties** > **NAT** > **Network Address Translation**. There you can set tracking options for address exhaustion and for address allocation and release.

Client Encrypt

What can I do here?

Use this window to define User Encryption Action properties for the Rule. If the allowed location in the rule is different to the location allowed in the **User Properties** , the settings here take precedence.

Getting Here - Security Policies > Access Control > Policy (Traditional mode) > Action column > More > Client Encrypt > Edit

Understanding Client Encrypt

Users on remote clients can be required to authenticate before they can connect to servers behind the Security Gateway.

To require remote users to authenticate in a traditional mode policy, define the Client encrypt rule.

Source	Destination	Service	Action	Track
All_Users@alaska	Net_A	My_Services	Client Encrypt	log

The table shows a typical remote access rule in a traditional mode Policy. User Access is defined in the **Source** column of the rule, and **Client Encrypt** in the **Action** column.

Client Encrypt - Options

- **Source** and **Destination**in the **User Encryption Action Properties** window have two options:

- *Intersect with User Database* - If the user who successfully authenticates is coming from a source or destination which is allowed to the user according to the rule, if the **User Properties** for that user do not allow this location, the user will actually be denied.
- *Ignore User Database* - Users who would otherwise denied as a result of the allowed source or destination defined in the **User Properties** are allowed anyway, (as long as they authenticate successfully).

- **Apply Rule Only if Desktop Configuration Options are Verified** controls Secure Client Verification for SecureClient connections. These connections can be either encrypted, for clients connecting via remote access, or unencrypted, where the SecureClient is on a LAN. If a user is successfully client-authenticated, they are only allowed access if the client machine is verified to be secure.

Threat Prevention

What can I do here?

Use this window to configure a Custom Threat Prevention policy.

Getting Here - Security Policies > Threat Prevention > Custom Policy

The Custom Threat Prevention Policy

The Custom Threat Prevention policy determines how the system inspects connections for bots and viruses. The primary component of the policy is the Rule Base. The rules use the Malware database and network objects.

If you enable Identity Awareness on your gateways, you can also use Access Role objects as the scope in a rule. This lets you easily make rules for individuals or different groups of users.

There are no implied rules in the Rule Base. All traffic is allowed unless it is explicitly blocked.

The columns of a rule define the traffic that it matches and what is done to that traffic.

- **Predefined Rule** - When you enable the IPS or one of the Threat Prevention Blades, a predefined rule is added to the Rule Base. The rule defines that all traffic for all network objects, regardless of who opened the connection, (the protected scope value equals any) is inspected for all protections according to the recommended profile. By default, logs are generated and the rule is installed on all Security Gateways that have the Threat Prevention Blade enabled.

- **Exception Rule** - An exception lets you set a protection or protections to detect or prevent for a specified protected scope. For example, if you want to prevent specified protections for a specific user in a rule with a profile that only detects protections. Another example, if you want to detect all protections in an R and D lab network in a rule with a prevent profile.

Rule Columns

Item	Description
No	The rule number. The sequence is important. The first rule that matches traffic according to a protected scope and profile is applied. For example, if rules 1 and 2 share the same protected scope and a profile in rule 1 is set to *detect* protections with a medium confidence level and the profile in rule 2 is set to *prevent* protections with a medium confidence level, then protections with a medium confidence level will be *detected* based on rule 1.
Name	The name of the rule. Give the rule a descriptive name. A name can include spaces.
Protected Scope	Threat Prevention inspects traffic to and/or from all objects specified in the Protected Scope, even when the specified object did not open the connection. You can set the Protected Scope parameter to Any. This option lets Threat Prevention inspect traffic based on the direction and interface type as defined by the Profile assigned to the applicable rule. By default, the predefined Recommended Rule sets the Protection Scope to Any.
Source	The source of the connection
Destination	The connection's destination
Protection/Site/File/Blade	Shows the protections for the policy. The Custom Threat Prevention policy includes the Anti-Bot, Threat Emulation, and Anti-Virus protections. For **Rules**, this field is always set to **N/A**and cannot be changed. Protections for Rule Base rules are defined in the configured profile (in the Action column). For rule exceptions and exception groups, this field can be set to one or more specified protections.
Services	Adds services

Item	Description
Action	Action shows how the traffic is inspected. For Rules, this is defined by the profile. The profile contains the configuration options for different confidence levels and performance impact. For rule exceptions and exception groups, the action can be set to Ask, Prevent, Detect, or Inactive.
Track	Shows if the traffic is logged or triggers various notifications, traps, or alerts. **Packet capture** allows the packets relevant to the connection to be captured for analysis. The packet capture can be viewed from the event in the Logs & Monitor > Logs view. This can be configured only for rules (not rule exceptions). To configure packet capture, select any tracking action other than None and then select Packet capture.
Install On	Select a gateway for the policy

Custom Threat Prevention Layer - New or Edit

What can I do here?

Use this window to create or edit a Custom Threat Prevention layer.

Getting Here - Security Policies > Threat Prevention > Right-click Policy > Edit Policy > In the Custom Threat Prevention section > click the (+) icon >
Or:
Menu > Manage Polices > New or Edit > In the Threat Prevention section > click the (+) icon.
Or:
Connect SmartConsole to the Global Domain > Security Policies Click (+) to open the Manage Policies tab > Click the Manage Policies link > click New > Select the Threat Prevention option > In the Custom Threat Prevention section click the (+) icon.

Custom Threat Prevention Policy Layers

You can create a Custom Threat Prevention Rule Base with multiple Policy Layers. Policy Layers help you organize your Rule Base to best suit your organizational needs. You can divide the Policy Layers by services or networks. Each Policy Layer calculates its action separately from the other Layers. In case of one Layer in the policy package, the rule enforced is the first rule matched. In case of multiple Layers:

- If a connection matches a rule in only one Layer, then the action enforced is the action in that rule.
- When a connection matches rules in more than one Layer, the gateway enforces the strictest action and settings.

Important - When the Threat Prevention blades run in MTA mode, the gateway enforces the automatic MTA rule, which is created when MTA is enabled on the gateway.

Action Enforcement in Multiple-Layered Security Policies

These examples show which action the gateway enforces when a connection matches rules in more than one Policy Layers.

Example 1

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect

Enforced action: Prevent

Example 2

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect
Exception for protection X	Inactive	-

Enforced action for protection X: Detect

Example 3

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect
Override for protection X	Detect	-
Exception for protection X	Inactive	-

Exception is prior to override and profile action. Therefore, the action for the Data Center Layer is Inactive.

The action for the Corporate LAN Layer is Detect.

Enforced action for protection X: Detect.

Example 4

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Deep Scan all files	Process specific file type families: Inspect doc files and Drop rtf files.

Enforced action : Deep Scan doc files and Drop rtf files.

Example 5

MIME nesting level and Maximum archive scanning time

The strictest action is :

Block combined with the minimum nesting level/scanning time, or

Allow combined with the maximum nesting level/scanning time, or

If both Block and Allow are matched, the enforced action is Block.

Example 6

UserCheck

	HR Layer	Finance Layer	Data Center Layer 3
Rule matched	Rule 3	Rule 1	Rule 4
Profile action	Detect	Prevent	Prevent
Configured page	Page A	Page B	Page C

The first Layer with the strictest action is enforced.

Enforced Action : Prevent with UserCheck Page B.

Threat Prevention Layers in Pre-R80 Gateways

In pre-R80 versions, the IPS Software Blade was not part of the Threat Prevention Policy, and was managed separately. In R80.XX versions, the IPS Software Blade is integrated into the Threat Prevention Policy.

When you upgrade SmartConsole to R80.XX from earlier versions, with some Security Gateways upgraded to R80.XX, and other Security Gateways remaining in previous versions:

- For pre-R80 gateways with IPS and Threat Prevention Software Blades enabled, the policy is split into two parallel layers: IPS and Threat Prevention.

  To see which Security Gateway enforces which IPS profile, look at the **Install On** column in the IPS Layer.

- R80.XX gateways are managed separately, based on the R80 or higher Policy Layers.

Best Practice - For better performance, we recommend that you use the **Optimized** profile when you upgrade to R80 or higher from earlier versions.

Threat Prevention Layer - Permissions

What can I do here?

Use this window to select profiles that can edit the Threat Prevention layer.

Getting Here - Security Policies > Threat Prevention > Right-click Policy > Edit Policy > In the Custom Threat Prevention section > click the (+) icon > Select Layer > Permissions
Or:
Menu > Manage Polices > New or Edit > In the Custom Threat Prevention section > click the (+) icon > Select Layer > Permissions
Or:
Connect SmartConsole to the Global Domain > Security Policies Click (+) to open the Manage Policies tab > Click the Manage Policies link > click New > Select the Custom Threat Prevention option > In the Threat Prevention section click the (+) icon > Select Layer > Permissions

Autonomous Policy

What can I do here?

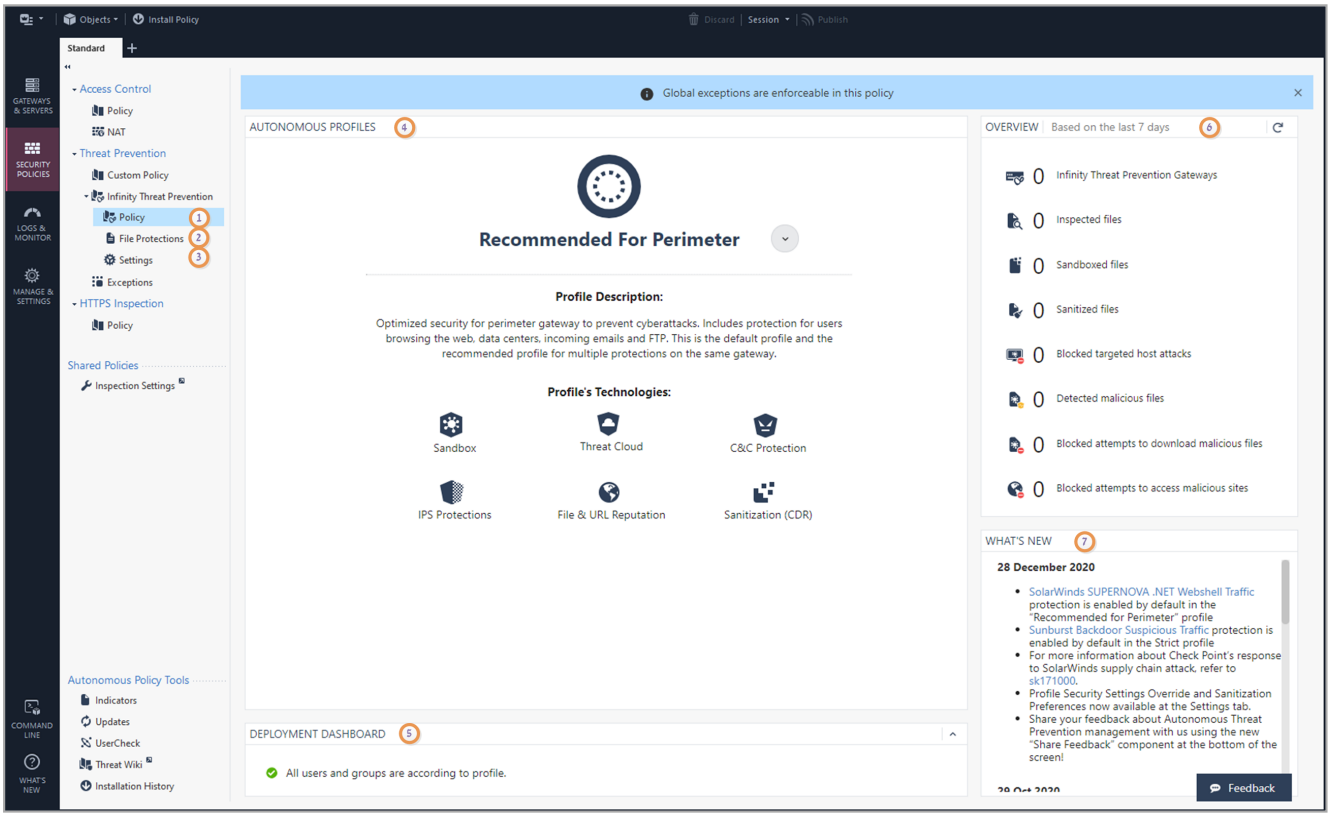
Use this window to configure Autonomous Threat Prevention.

Getting Here - Security Policies > Threat Prevention > Autonomous Threat Prevention > Policy
Or:
Security Policies > Threat Prevention > Autonomous Threat Prevention > Policy

Understanding Autonomous Threat Prevention

Autonomous Threat Prevention is an innovative Threat Prevention management model that:

- Provides zero-maintenance protection from zero-day threats, and continuously and autonomously ensures that your protection is up-to-date with the latest cyber threats and prevention technologies.
- Empowers administrators with a one-click classification of the gateway role using out-of-the-box policy profiles based on your business and IT security needs.
- Streamlines configuration and deployment of policy profiles across your gateways.
- Provides simple and powerful customizations to best serve your organization's needs.



No.	Item	Description
1	**Autonomous Threat Prevention Policy**	This is where you manage the Autonomous Threat Prevention Policy.
2	**File Protections**	See the protected files for each profile and customize as necessary.
3	**Settings**	Advanced settings.
4	**Autonomous Threat Prevention Profiles**	Select your profile.

No.	Item	Description
5	**Overview**	See statistical information about actions done on files.
6	**What's New**	See the updates introduced to Autonomous Threat Prevention.
7	**Deployment Dashboard**	Advanced configuration.

Note - For **offline** Threat Extraction Engine Release Updates, refer to sk167109.

Autonomous Threat Prevention Profiles

These are the 5 profiles supported by Autonomous Threat Prevention:

- **Recommended for Perimeter Profile**

  Optimized security for perimeter gateway to prevent cyberattacks. Includes protection for users browsing the web, data centers, incoming emails, and FTP. This is the default profile and the recommended profile for multiple protections on the same gateway (for example, when both Perimeter protection and Internal network protection are needed).

  Recommended for Perimeter is the most similar profile to the Optimized profile in the Custom Threat Prevention policy.

- **Strict Security for Perimeter Profile**

  Maximum security for perimeter gateways to prevent cyberattacks. Includes protection for users browsing the web, data centers, incoming emails and FTP.

- **Cloud/Data Center Profile**

  Optimized security to prevent cyberattacks on data centers. Includes extensive protection over servers and east-west traffic.

- **Internal Network Profile**

  Maximum security to prevent cyberattacks over internal traffic between internal users and internal servers.

- **Recommended for Guest Network Profile**

  ”Detect mode” security profile to monitor cyberattacks attempts through a guest network (Wi-Fi) non-intrusively.

Each profile consists of a wide range of industry-leading protections. This table summarizes the technologies used by each profile:

	IPS Protections	File & URL Reputation	ThreatCloud	Sandbox	Sanitization (CDR)	C&C protection
Recommended for Perimeter Profile	✓	✓	✓	✓	✓	✓
Cloud/Data Center Profile	✓	✓	✓	✓	–	✓
Internal Network Profile	✓	✓	✓	✓	–	✓
Strict Security for Perimeter Profile	✓	✓	✓	✓	✓	✓
Recommended for Guest Network Profile	✓	✓	✓	✓	–	✓

Here is a short explanation about each technology:

- **IPS Protections** - Integrated Intrusion Prevention System with leading performance and unlimited scaling. IPS implements advanced protections from network-based attacks and protects all IT systems, including servers, endpoints, industrial systems and IoT.
- **File & URL Reputation** - Files and URLs are checked through the ThreatCloud repository for reputation.
- **ThreatCloud** - A cloud-based real-time global threat intelligence using Check Point worldwide network of threat sensors.
- **Sandbox** - Prevents unknown, zero-day and advanced polymorphic attacks by executing suspicious files in evasion-resistant sandbox and applying advanced AI techniques.
- **Sanitization (CDR)** - Provides pro-active prevention of unknown attacks from day zero, by sanitizing incoming files before delivering them to users.
- **C&C protection** - Detects infected and compromised devices on the network. It blocks attacks and prevents damages by blocking malware Command & Control (C&C) communications.

For more information, see the *R81.10 Threat Prevention Administration Guide*.

File Protections

What can I do here?

Use this window to configure Autonomous Threat Prevention file protections.

Getting Here - Security Policies > Threat Prevention > Autonomous Threat Prevention > File Protections

Understanding Autonomous Threat Prevention File Protections

In the **File Protections** page, you can:

- View the protected file types and protection types for the selected Autonomous Threat Prevention profile.
- Override the recommended file protections according to profile and select different protections.

To configure file protections

1. Go to **Threat Prevention** > **Autonomous Threat Prevention** > **File Protections**
2. Click on the **+** sign and configure the required protection.

   These are the available protections:

   - **Inspect** - These technologies are operated: File Reputation, ThreatCloud and Sandbox. You can see Sandbox is enabled in the **Sandbox** column.
   - **Inspect & Clean** - These technologies are operated: File Reputation, ThreatCloud, Sandbox and Sanitization (CDR). You can see Sandbox is enabled in the **Sandbox** column.
   - **Block** - Block the file.
   - **Bypass** - Do not inspect the file.

   You cannot override the protections for file types which are not on the list. File types which are not on the list will be inspected in all profiles.

Settings

What can I do here?

Use this window to configure Autonomous Threat Prevention settings.

Getting Here - Security Policies > Threat Prevention > Autonomous Threat Prevention > Settings

Understanding Autonomous Threat Prevention Settings

Sanitized File Settings - By default, this option is selected:

- **Allow end-users to access the original files that are not malicious according to Sandbox** - After a file is cleaned/sanitized, a banner with a link to original file is added to the document. An access to original file will be allowed only if the original file is found to be benign by all Threat Prevention engines, including Sandbox. If you clear this option, you will not be able to access the original file even if it is determined as non-malicious.
- **Modify the name of the cleaned file** - Select this option to modify the name of the cleaned file.

Advanced Settings - If needed, you can turn off Sandbox and/or Sanitization and/or Archives deep scan. We recommend to keep Sandbox, Sanitization and Archives deep scan On.

Exceptions

What can I do here?

Use this window to create exceptions to the Threat Prevention policy.

Getting Here - Security Policies> Threat Prevention > Exceptions

Exception Rules

If necessary, you can add an **exception** directly to a rule. An exception sets a different **Action** to an object in the **Protected Scope** from the Action specified Threat Prevention rule. In general, exceptions are designed to give you the option to reduce the level of enforcement of a specific protection and not to increase it. For example: The Research and Development (R&D) network protections are included in a profile with the **Prevent** action. You can define an exception which sets the specific R&D network to **Detect**. For some Anti-Bot and IPS signatures only, you can define exceptions which are stricter than the profile action.

You can add one or more exceptions to a rule. The exception is added as a shaded row below the rule in the Rule Base. It is identified in the **No** column with the rule's number plus the letter E and a digit that represents the exception number. For example, if you add two exceptions to rule number 1, two lines will be added and show in the Rule Base as E-1.1 and E-1.2.

You can use exception groups to group exceptions that you want to use in more than one rule. See the Exceptions Groups Pane.

You can expand or collapse the rule exceptions by clicking on the minus or plus sign next to the rule number in the **No**. column.

To add an exception to a rule:

1. In the **Policy** pane, select the rule to which you want to add an exception.
2. Click **Add Exception**.
3. Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4. Enter values for the columns. Including these:
   - **Protected Scope** -Change it to reflect the relevant objects.
   - **Protection** - Click the plus sign in the cell to open the Protections viewer. Select the protection(s). Click **OK**.
5. In SmartConsole, install the policy.

Note - You cannot set an exception rule to an inactive protection or an inactive blade.

Disabling a Protection on One Server

Scenario: The protection Backdoor.Win32.Agent.AH blocks malware on windows servers. How can I change this protection to **detect** *for one server only?*

In this example, create this Threat Prevention rule, and install the Threat Prevention policy:

Name	Protected Scope	Protection/Site	Action	Track	Install On
Monitor Bot Activity	`* Any`	`- N/A`	A profile based on the **Optimized** profile. Edit this profile > go to the **General Policy** pane> in the **Activation Mode** section, set every **Confidence** to **Prevent**.	Log	Policy Targets
Exclude	Server_1	`Backdoor.Win32.Agent.AH`	**Detect**	Log	Server_1

To add an exception to a rule:

1. In SmartConsole, click Threat Prevention > **Policy** > **Layer**.
2. Click the rule that contains the scope of Server_1.
3. Click the **Add Exception** toolbar button to add the exception to the rule. The gateway applies the first exception matched.
4. Right-click the rule and select **New Exception**.
5. Configure these settings:
   - **Name** - Give the exception a name such as **Exclude**.
   - **Protected Scope** -Change it to **Server_1** so that it applies to all detections on the server.
   - **Protection/Site** - Click **+** in the cell. From the drop-down menu, click the category and select one or more of the items to exclude.

Note - To add EICAR files as exceptions, you must add them as whitelist files (see *"Adding a File to the Whitelist" on page 383*). When you add EICAR files through Exceptions in Policy rules, the gateway still blocks them, if archive scanning is enabled.

- **Action** - Keep it as **Detect**.
- **Track** - Keep it as **Log**.
- **Install On** - Keep it as **Policy Targets** or select specified gateways, on which to install the rule.

1. In SmartConsole, install the policy.

Blade Exceptions

You can also configure an exception for an entire blade.

To configure a blade exception:

1. In the **Policy**, select the Layer rule to which you want to add an exception.
2. Click **Add Exception**.
3. Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4. In the **Protection/Site** column, select **Blades** from the drop-down menu.
5. Select the blade you want to exclude.
6. In SmartConsole, install the policy.

Creating Exceptions from Logs or Events

In some cases, after evaluating a log or an event in the **Logs & Monitor** view, it may be necessary to update a rule exception in the SmartConsole Rule Base. You can do this directly from within the **Logs & Monitor** view. You can apply the exception to a specified rule or apply the exception to all rules that show under Global Exceptions.

To update a rule exception or global exception from a log:

1. Click **Logs & Monitor** > **Logs** tab.
2. Right-click the log and select **Add Exception**.
3. Configure the settings for the exception.
4. Click **OK**.
5. In the New Exception Rule window:
   - To show the exception in the policy, click **Go to**
   - Otherwise, click **Close**
6. In SmartConsole, install the policy.

New Exceptions Group

What can I do here?

Use this window to create a Threat Prevention exception group.

Getting Here - Security Policies > Threat Prevention > Exceptions > New

Exception Groups

An exception group is a container for one or more exceptions. You can attach an exception group to all rules or only to some rules. With exception groups, you can manage your exceptions more easily, because you can attach the same exception group to multiple rules, instead of manually define exceptions for each rule.

The Exception Groups pane shows a list of exception groups that were created, the rules that use them, and any comments related to the defined group. The Exceptions Groups pane contains these options:

Option	Meaning
New	Creates a new exception group.
Edit	Modifies an existing exception group.

Option	Meaning
Delete	Deletes an exception group.
Search	Search for an exception group.

Global Exceptions

The system comes with a predefined group named Global Exceptions. Exceptions that you define in the Global Exceptions group are automatically added to every rule in the Rule Base. For other exception groups, you can decide to which rules to add them.

Exception Groups in the Rule Base

Global exceptions and other exception groups are added as shaded rows below the rule in the Rule Base. Each exception group is labeled with a tab that shows the exception group's name. The exceptions within a group are identified in the **No** column using the syntax: `E - <rule number>.<exception number>`, where `E` identifies the line as an exception. For example, if there is a Global Exceptions group that contains two exceptions, all rules show the exception rows in the Rule Base **No** column as E-1.1 and E-1.2. Note that the numbering of exception varies when you move the exceptions within a rule.

To view exception groups in the Rule Base:

Click the plus or minus sign next to the rule number in the **No**. column to expand or collapse the rule exceptions and exception groups.

Creating Exception Groups

When you create an exception group, you create a container for one or more exceptions. After you create the group, add exceptions to them. You can then add the group to rules that require the exception group in the Threat Prevention Rule Base.

To create an exception group:

1. In SmartConsole, select **Security Policies** > **Threat Prevention** > **Exceptions**.
2. In the **Exceptions** section, click **New**.
3. In Apply On, configure how the exception group is used in the Threat Prevention policy.
    - **Manually attach to a rule** - This exception group applies only when you add it to Threat Prevention rules.

- **Automatically attached to each rule with profile** - This exception group applies to all Threat Prevention rules in the specified profile.
- **Automatically attached to all rules** - This exception group applies to all Threat Prevention rules.

4. Click **OK**.
5. Install the Threat Prevention policies.

Adding Exceptions to Exception Groups

To use exception groups, you must add exception rules to them.

To add exceptions to an exception group:

1. In SmartConsole, select **Security Policies** > **Threat Prevention** > **Exceptions**.
2. In the **Exceptions** section, click the exception group to which you want to add an exception.
3. Click **Add Exception Rule**.
4. Configure the settings for the new exception rule.
5. Install the Threat Prevention policy.

Adding Exception Groups to the Rule Base

You can add exception groups to Threat Prevention rules. This only applies to exception groups that are configured to **Manually attach to a rule**.

To add an exception group to the Rule Base:

1. Click **Security Policies** > **Threat Prevention** > **Policy**.
2. Right-click the rule and select **Add Exception Group** > **<group name>**.
3. Install the Threat Prevention policies.

IPS Core Protections

What can I do here?

Use this window to change settings for the Core protections enforced by a profile.

The IPS protections are divided into two main types:

- **Core protections** - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy.

- **ThreatCloud protections** - Updated from the Check Point cloud. These protections are part of the Threat Prevention policy.

Getting Here - Security Policies > Threat Prevention > Policy > IPS > Action Column > change profile.

Tracking Options

These tracking options are available for Threat Prevention.

Threat Prevention Track Options

- **None** - Do not generate an alert.
- **Alert** - Generate a log and run a command, such as display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in the **Menu > Global Properties > Log and Alert > Alerts**.
- **Packet Capture** - Adds raw IPS, Anti-Virus, Anti-Bot, Threat Emulation and Threat Extraction packet data to the Threat Prevention logs. Only blocked packets are added.
- **Forensics** - Adds fields to the Threat Prevention logs. The extra information gives you a deeper understanding of an attack.

HTTPS Inspection

What can I do here?

Use this window to edit the HTTPS Inspection Rulebase on which the HTTPS Inspection Policy is built.

Getting Here - Security Policies > HTTPS Inspection

Understanding HTTPS Inspection

You can enable HTTPS traffic inspection on Security Gateways to inspect traffic that is encrypted by the TLS protocol. TLS secures communication between internet browser clients and web servers. It supplies data privacy and integrity by encrypting the traffic, based on standard encryption ciphers.

The TLS protocol is widely implemented in public resources that include: banking, web mail, user forums, and corporate web resources.

There are two types of HTTPS inspection:

- **Inbound HTTPS inspection** - To protect internal servers from malicious requests originating from the internet or an external network.

- **Outbound HTTPS inspection** - To protect an organization from malicious traffic being sent by an internal client to a destination outside of the organization.

The Security Gateway acts as an intermediary between the client computer and the secure web site. The Security Gateway behaves as the client with the server and as the server with the client using certificates.

To optimize performance, inbound HTTPS traffic is inspected only if the policy has rules for HTTPS. For example, if the IPS profile does not have HTTP/HTTPS-related protections activated, HTTPS Inspection is not started.

All data is kept private in HTTPS Inspection logs. This is controlled by administrator permissions. Only administrators with HTTPS Inspection permissions can see all the fields in a log. Without these permissions, some data is hidden.

HTTPS Inspection Policy

The HTTPS Inspection policy determines which traffic is inspected. The primary component of the policy is the Rule Base. The rules use the categories defined in the Application and URL Filtering Database, network objects and custom objects (if defined).

The HTTPS inspection Rule Base lets you inspect the traffic on these network blades:

- Anti-Bot
- Anti-Virus
- Application Control
- Content Awareness
- Data Loss Prevention
- IPS
- Threat Emulation
- URL Filtering

The HTTPS Inspection Rule Base has these fields:

No

The sequence of rules is important because the first rule that matches is applied.

For example, if the predefined rule inspects all HTTPS traffic from any category and the next rule bypasses traffic from a specified category, the first rule that inspects the traffic is applied.

Name

A descriptive name for the rule. The name can include spaces.

Source

Network object that defines where the traffic starts. The default is **Any**.

Important - A rule that blocks traffic, with the **Source** and **Destination** parameters defined as Any, also blocks traffic to and from the Identity Awareness Captive Portal.

Destination

Network object that defines the destination of the traffic.

The default is the **Internet**, which includes all traffic with the destination of DMZ or external. If you delete the destination value, the rule changes to **Any**, which applies to traffic going to all destinations.

Important - A rule that blocks traffic, with the Source and Destination parameters defined as Any, also blocks traffic to and from the Identity Awareness Captive Portal.

Services

By default, HTTPS traffic on port 443 and HTTP and HTTPS proxy on port 8080 is inspected. You can include more services and ports in the inspection by adding them to the services list.

To select other HTTPS/HTTP services, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of services and select a service. Other services, such as SSH are not supported.

Category / Custom application

The Site Category column contains the categories for sites and applications that users browse to and you choose to include. One rule can include multiple categories of different types.

Important - ◦To perform categorization correctly, a single connection to a site must be inspected in some cases regardless of the HTTPS inspection policy. This maps the IP address of a site to the relevant domain name.

You can also include custom applications, sites, and hosts. You can select a custom defined application or site object with the Custom button or create a new host or site with the New button at the bottom of the page.

To add categories/applications to a rule

- Put your mouse in the column and a plus sign shows. Click the plus sign to open the Category viewer. For each category, the viewer shows a description and if there are applications or sites related with it.
- To filter the Available list by categories or custom-defined sites, click the specified button in the toolbar of the viewer. The Available list opens in the left column and then you can add items to the rule.
- To add a category object to the rule, click the check box in the Available list.
- To see the details of category without adding it to the rule, put the cursor on the name of the item in the Available list.
- You can only select a category to add to the rule from the Available list.
- If a category is already in a rule, it will not show in the Category viewer.
- If you know the name of a category, you can search for it. The results will show in the Available list

Action

The action is what is done to the traffic. Click in the column to see the options and select one to add to the rule.

- **Inspect** - The traffic is inspected on the blades set in the Blades column.
- **Bypass** - The traffic of source and destination traffic in rules that include the bypass action are not decrypted and inspected. You can bypass HTTPS Inspection for all Network objects. This is recommended for Anti-Virus, URL Filtering, and IPS updates. Other HTTPS protections that already operate on traffic will continue to work even when the HTTPS traffic is not decrypted for inspection.

Track

Choose if the traffic is logged in the **Logs** tab of the SmartConsole **Logs & Monitor** view, and if it triggers other notifications. Click in the column and the options open. The options include:

- **None** - Does not record the event.
- **Log** - Records the details in the Logs tab of the SmartConsole Logs & Monitor view. This option is useful for obtaining general information on your network traffic. There is one or more log for each session depending on the suppression option.
- **Alert** - Logs the event and executes a command, such as display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in the SmartConsole **Menu > Global Properties > Log and Alert > Alert Commands**.

- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in the SmartConsole **Menu > Global Properties > Log and Alert > Alert Commands**.
- **SNMP Trap** - Sends a SNMP alert to the SNMP GUI, or runs the script defined in the SmartConsole **Menu > Global Properties > Log and Alert > Alert Commands**.
- **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in the SmartConsole **Menu > Global Properties > Log and Alert > Alert Commands**.

Blade

Choose the blades that will inspect the traffic. Click in the column and the options open. The options include:

- Anti-Bot
- Anti-Virus
- Application Control
- Data Loss Prevention
- IPS
- URL Filtering
- Content Awareness (Data Awareness)
- Threat Emulation

Install On

Select which Security Gateways the rule will be installed on. The default is **All**, which means all Security Gateways that have HTTPS Inspection enabled. Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available Security Gateways and select.

Certificate

Choose the certificate that is applicable to the rule. The Security Gateway uses the selected certificate for communication between the Security Gateway and the client.

For outbound HTTPS Inspection - Select the **Outbound Certificate** object (default) that reflects the CA certificate you created/imported and deployed on the client machines in your organization.

For inbound HTTPS Inspection - Select the server certificate applicable to the rule. Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available server certificates and select one. When there is a match to a rule, the Security Gateway uses the selected server certificate to communicate with the source client.

HTTPS Inspection - Layer Editor

What can I do here?

Use this window to

- Share the HTTPS Inspection layer with multiple policies and rules.
- Create multiple HTTPS Inspection Layers

Getting Here - Security Policies > HTTPS Inspection > right-click > Edit Layer > General tab > HTTPS Inspection > Drop-down button > Edit layer

To create multiple HTTPS Inspection Layers

1. Open **Security Policies** > **HTTPS Inspection**.
2. Right-click on **HTTPS Inspection Default Shared Layer**.

   The policy editor opens.
3. On the **General** tab, in the **HTTPS Inspection** row, click the drop-down button and select **Select Layer**.
4. Click the drop-down button and then **New Layer**.

HTTPS Tools - Additional Settings

What can I do here?

Use this window to open additional HTTPS inspection settings in SmartDashboard. In SmartDashboard you can edit settings for:

- Trusted CA
- HTTPS Validation
- Server certificates

Getting Here - Security Policies > HTTPS Inspection > Policy > HTTPS Tools > Additional Settings

Shared Policies

Use the Shared Policy area to configure:

- Mobile Access
- Data Loss Prevention
- Inspection Settings

Getting Here - SmartConsole > Security Policies > Shared Policies

Access Tools & Threat Policy Tools

Access Tools

Use the **Access Tools** to:

- Manage VPN Communities
- Configure Updates
- Configure UserCheck Settings
- Configure Client Certificates
- Access the Application Wiki
- View Installation History

Threat Policy Tools

- Use the **Custom Policy Tools** to:
  - Edit threat profiles
  - View IPS Protections
  - Create Whitelists
  - Add Threat Indicators
  - Configure updates
  - Configure UserCheck
  - Access the Threat Wiki
  - View Policy installation history
- Use the **Autonomous Policy Tools** to
  - Add Threat Indicators
  - Configure updates
  - Configure UserCheck
  - Access the Threat Wiki
  - View Policy installation history

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools
Or:
SmartConsole > Security Policies > Threat Prevention > Custom or Autonomous Policy > Custom or Autonomous Policy Tools

Manage Access Control, Threat Prevention and HTTPS Inspection Layers

What can I do here?

Use this pane to:

- Create, edit, and delete Access Control, Threat Prevention, and HTTPS Inspection layers
- View Layer Details

Getting Here - Menu > Manage policies and Layers > Layers.

Layer Properties - General

What can I do here?

Use this window to:

- Edit a layer or create a new one
- Select the Software Blades to which the rules of this Layer apply
- Set if multiple policies can share the layer
- Configure Proxy

Getting Here - Menu > Manage Policies and Layers > Layers > New or Edit > General

Layer - General

- **Software Blades** - Select to enable one or more Software Blades.
  - Firewall (Network Access Control)
  - Application and URL Filtering
  - Content Awareness
  - Mobile Access
- **Sharing** - Select this option to share this layer with other policies.

Note - You can share this layer with other policies as an Ordered Layer. If you use the layer as an In-line layer, policy installation will fail on pre-R80 gateways.

Layer Properties - Advanced

What can I do here?

Use this window to set the HTTP Proxy configuration and configure the implicit cleanup action of the Layer.

Getting Here - Menu > Manage Policies and Layers > Layers> Access Control / Threat Prevention > New or Edit > Advanced

Advanced Options

- **Implicit Cleanup Action** - The default rule that is applied if none of the rules in the Layer match. Every Layer has its own implicit cleanup rule. You can configure the rule to Accept or Drop in the Layer settings.

  Important - Always add an explicit Cleanup Rule at the end of each Layer, and make sure that its Action is the same as the Action of the Implicit Cleanup Rule. If there is no explicit Cleanup Rule, one of these messages will show under the last rule of the Layer:

  Missing cleanup rule - Unmatched traffic will be dropped and not logged.
  Missing cleanup rule - Unmatched traffic will be accepted and not logged.

- **Proxy Configuration** - Select to detect users located behind an HTTP proxy with an **X Forward-For** header.

Layer - Permissions

What can I do here?

Use this window to

- Set the permission profile or profiles that have permission to edit the layer
- Select additional profiles that can edit the layer

Getting Here - Menu > Manage Layers > New or Edit > Permissions

Layer Properties - Permissions

Add or remove Permission Profiles that have permissions to work with this Policy Layer.

The upper list shows those Permission Profiles that have default permissions for this Layer. You cannot change these defaults.

VPN Communities

What can I do here?

In this window you can add, edit, and delete VPN communities and change their gateway assignments.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities

Setting up Site-to-Site VPN between Gateways

Scenario: Two Check Point gateways are managed by the same Security Management Server. How do you create a site-to-site VPN between the two gateways so that they can communicate securely?

Overview of the Workflow:

1. Create the gateway objects in SmartConsole and make sure that IPsec VPN is enabled on each one.
2. Generate internal CA certificates for each gateway (done automatically).
3. Create the VPN Community.
4. Define the VPN Domain.
5. Make sure that the VPN will work with your configured routing, or change the routing or link selection settings as necessary.
6. Create rules for the traffic.
7. Install the Access Control Policy.

Enabling IPsec VPN on a Gateway

Site to Site VPN requires two or more gateways with the IPsec VPN Software Blade enabled. Other Software Blades can be enabled on the same gateway.

Make sure that Trusted Communication is established between all gateways and the Security Management Server.

To enable the IPsec VPN Software Blade on a gateway:

1. In SmartConsole, open a gateway object.
2. On the **General Properties** page, in the **Network Security** tab, select **IPsec VPN**.

3. Click **OK**.

   An internal CA certificate for the gateway is created automatically.

Defining the VPN Domain for a Gateway

The VPN Domain defines the networks and IP addresses that are included in the VPN community. It is also called the Encryption Domain. When you create a Check Point gateway object, the VPN Domain is automatically defined as all IP Addresses behind the gateway, based on the topology information.

You can manually define the VPN domain to include one or more networks. You must have a Network object or Network Group object that represents the domain.

To manually define the VPN Domain:

1. In SmartConsole, open a gateway object.
2. Open the **Network Management** > **VPN Domain** page.
3. Select **Manually defined** and:
   - Browse to the object list and select an object that represents the domain.
   - Browse to the object list and click **New** > **Group** or **Network** to define a new group of machines or network.
4. Click **OK**.

Creating a VPN Community

You can create a Meshed or Star VPN Community. The procedure below shows an example of a Star Community.

To create a new VPN community:

1. In SmartConsole > **Security Policies** tab, in the **Access Tools** area, click **VPN Communities**.
2. Click the **New** icon and select **Star Community**.

   A **New Star Community** window opens.
3. Enter a name for the VPN Community.
4. In the **Center Gateways** area, click the plus icon to add one or more gateways to be in the center of the community.
5. In the **Satellite Gateways** area, click the plus icon to add one or more gateways to be around the center gateway.
6. Click **OK**.

The Community uses the default encryption and VPN Routing settings.

7. Optional: Edit more settings for the VPN Community in the community object.

More VPN Community Settings

In addition to the gateway members, you can edit these settings for the VPN Community in the community object:

- **Encrypted Traffic** - Select **Accept all encrypted traffic** to encrypt and decrypt all traffic between the Security Gateways. If this is not selected, create rules in the Security Policy Rule Base to allow encrypted traffic between community members
- **Encryption** - Select encryption settings that include the **Encryption Method** and **Encryption Suite**. See VPN Community Object - Encryption Settings.
- **Tunnel Management** - Select settings VPN tunnels that include **Permanent Tunnels** and Tunnel Sharing. See Configuring Tunnel Features.
- **VPN Routing** -For Star Communities, select how VPN traffic is routed between the center and satellite gateways. By default this is always set to **To center only**. See Configuring Domain Based VPN.
- **MEP (Multiple Entry Points)** - For Star Communities, select how the entry gateway for VPN traffic is chosen. This only applies when you have multiple center gateways in the community. See Configuring MEP.
- **Excluded Services** - Add services that are **not** to be encrypted, for example Firewall control connections. VPN tunnels are not created for the Services included here.
- **Shared Secret** - Configure shared secret authentication to use for communication with external gateways that are part of a VPN community. See Configuring a VPN with External Security Gateways Using Pre-Shared Secret.
- **Wire Mode** - Select to define internal interfaces and communities as trusted and bypass the firewall for some communication. See Configuring Wire Mode.
- **Advanced** - Configure advanced settings related to IKE, IPsec, and NAT. You can also **Reset All VPN Properties** to revert all VPN Community settings to their default values. See Configuring Advanced IKE Properties.

Confirming VPN Routing

By default, IPsec VPN uses the main **IPv4 Address**, defined in the **General Properties** page of the Gateway, for the VPN tunnel connection.

If you want to use this IP address for the VPN communication, and it is an external interface, you do not need additional routing.

If the main IP address is an internal interface, or if you want VPN communication on a different interface, make sure that:

- The **Link Selection** settings for the gateway are configured. Choose which gateway links are used by VPN to route traffic correctly.
- VPN Routing is configured to allow the connections.

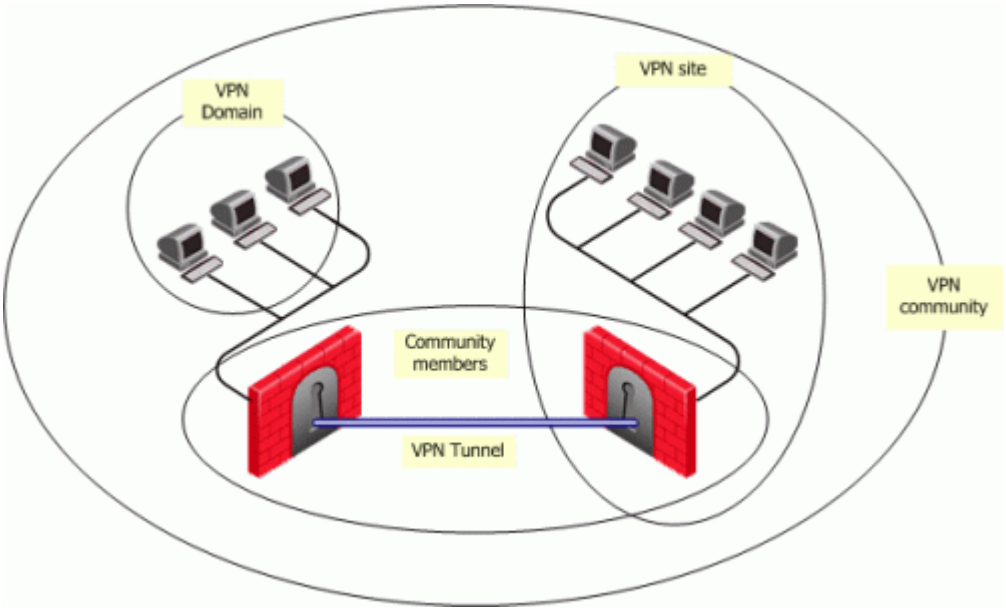
Understanding VPN Communities

VPN Communities

Creating VPN tunnels between Security Gateways is made easier through the configuration of VPN communities. A VPN community is a collection of VPN enabled gateways capable of communicating via VPN tunnels.

To understand VPN Communities, a number of terms need to be defined:

- *VPN Community member*. Refers to the Security Gateway that resides at one end of a VPN tunnel.
- *VPN Domain*. Refers to the hosts behind the Security Gateway. The VPN domain can be the whole network that lies behind the Security Gateway or just a section of that network. For example a Security Gateway might protect the corporate LAN and the DMZ. Only the corporate LAN needs to be defined as the VPN domain.
- *VPN Site*. Community member plus VPN domain. A typical VPN site would be the branch office of a bank.
- *VPN Community*. The collection of VPN tunnels/links and their attributes.
- *Domain Based VPN*. Routing VPN traffic based on the encryption domain behind each Security Gateway in the community. In a star community, satellite Security Gateways can communicate with each other through center Security Gateways.
- *Route Based VPN*. Traffic is routed within the VPN community based on the routing information, static or dynamic, configured on the Operating Systems of the Security Gateways.



The methods used for encryption and ensuring data integrity determine the type of tunnel created between the Security Gateways, which in turn is considered a characteristic of that particular VPN community.

A Security Management Server can manage multiple VPN communities, which means communities can be created and organized according to specific needs.

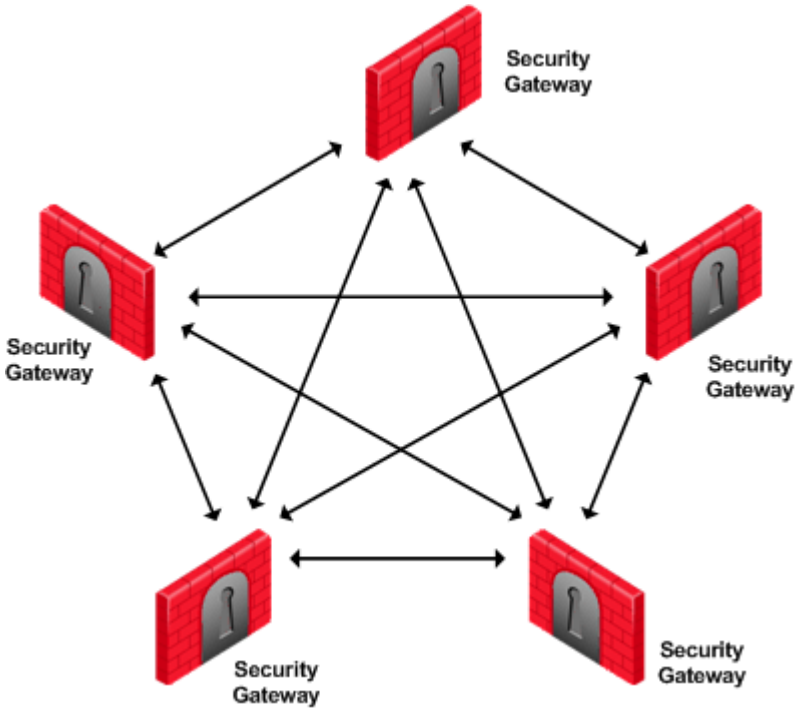
VPN Topologies

The most basic topology consists of two Security Gateways capable of creating a VPN tunnel between them. Security Management Server's support of more complex topologies enables VPN communities to be created according to the particular needs of an organization. Security Management Server supports two main VPN topologies:

- Meshed
- Star

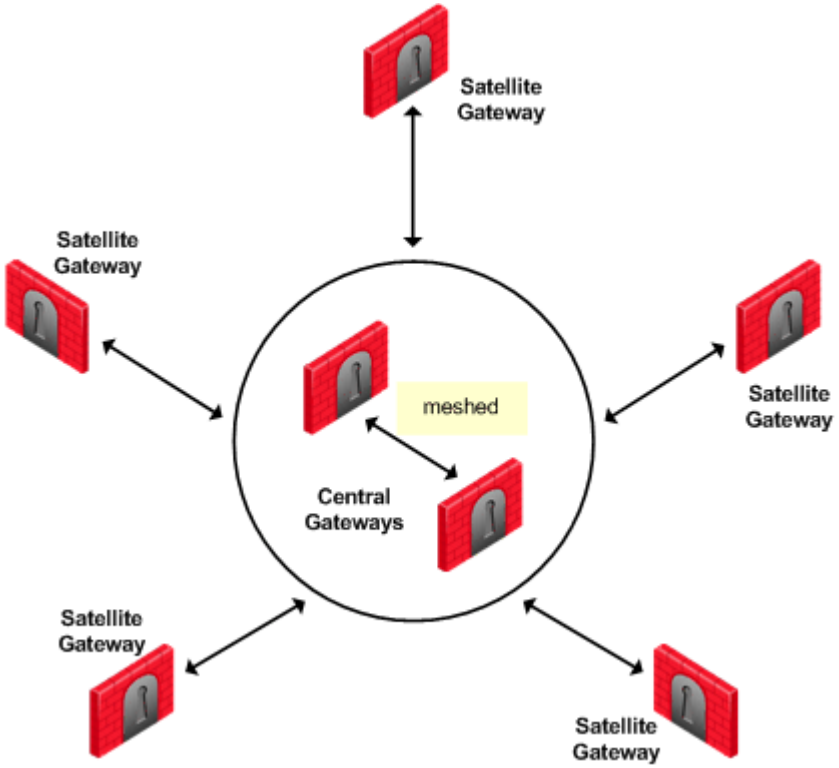
Meshed VPN Community

A Mesh is a VPN community in which a VPN site can create a VPN tunnel with any other VPN site in the community:



Star VPN Community

A star is a VPN community consisting of central Security Gateways (or "hubs") and satellite Security Gateways (or "spokes"). In this type of community, a satellite can create a tunnel only with other sites whose Security Gateways are defined as central.



A satellite Security Gateway cannot create a VPN tunnel with a Security Gateway that is also defined as a satellite Security Gateway.

Central Security Gateways can create VPN tunnels with other Central Security Gateways only if the **Mesh center Security Gateways** option has been selected on the **Central Security Gateways** page of the **Star Community Properties** window.

Access Control and VPN Communities

Configuring Security Gateways into a VPN community does not create a de facto access control policy between the Security Gateways. The fact that two Security Gateways belong to the same VPN community does not mean the Security Gateways have access to each other.

The configuration of the Security Gateways into a VPN community means that *if* these Security Gateways are allowed to communicate via an access control policy, then that communication is encrypted. Access control is configured in the Security Policy Rule Base.

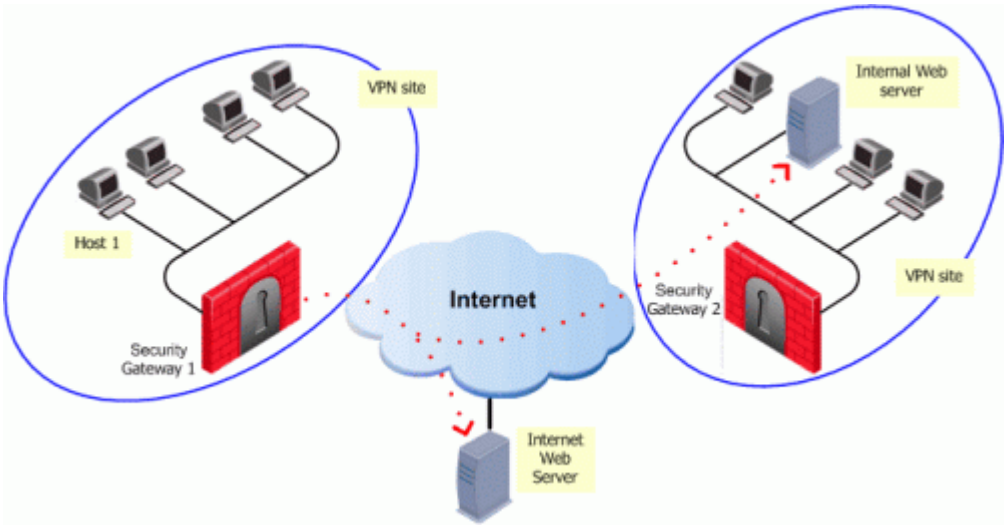
Using the VPN column of the Security Policy Rule Base, it is possible to create access control rules that apply *only* to members of a VPN community, for example:

Source	Destination	VPN	Services & Applications	Action
Any	Any	Community_A	HTTP	Accept

The connection is matched only if all the conditions of the rule are true, that is - it must be an HTTP connection between a source and destination IP address within VPN Community A. If any one of these conditions is not true, the rule is not matched. If all conditions of the rule are met, the rule is matched and the connection allowed.

It is also possible for a rule in the Security Policy Rule Base to be relevant for both VPN communities and host machines **not** in the community.

For example:



The rule in the Security Policy Rule Base allows an HTTP connection between any internal IP with any IP:

Source	Destination	VPN	Services & Applications	Action
Any_internal_ machine	Any	Any	HTTP	Accept

In both cases, the connection is simply matched to the Security Policy Rule; whether or not the connection is encrypted is dealt with on the VPN level. *VPN is another level of security separate from the access control level*.

Routing Traffic within a VPN Community

VPN routing provides a way of controlling how VPN traffic is directed.

There are two methods for VPN routing:

- Domain Based VPN
- Route Based VPN

VPN Community Options

- **New** > **Meshed Community** - Create a new Meshed Community. Opens the Meshed Community Properties window.
- **New** > **Star Community** - Create a new Star Community. Opens the Star Community Properties window.
- **Edit** - Change the selected community. Opens the Community Properties window.
- **Delete** - Delete the selected community.

Click a listed community to see the gateways that belong to it, and the encryption algorithms used in the VPN communications.

VPN Communities - Gateways

What can I do here?

Use this window to select the gateways of the Star or Meshed VPN community.

Note - For Global VPN Communities, see: *"VPN and Multi-Domain Security Management" on page 680*

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Gateways

Configuring a Meshed Community Between Internally Managed Gateways

To configure an internally managed VPN meshed community:

1. Install and configure the Security Gateways as described in the *R81.10 Installation and Upgrade Guide*.
2. In SmartConsole, double click on the Security Gateway object.
3. In the **General Properties** page:
   a. Enter the gateway **Name**.
   b. Enter the **IPv4 Address** and **IPv6 Address**.
   c. In the **Network Security** tab, Select **IPsec VPN**.
   d. Click **Communication** and establish trusted communication with the Gateway.
4. In the **Network Management** page, click **Get Interfaces**.

a. After the interfaces show in the table, click **Edit** to open the **Interface** window.

b. In the **Interface** window, define the general properties of the interface and the topology of the network behind it.

5. In the **Network Management** > **VPN Domain** page, define the VPN domain one of:

   - **All IP Addresses behind the Gateway based on Topology information**
   - **Manually defined** as an address range, a network, or a group that can be a combination of address ranges, networks, and even other groups.

     (There are instances where the VPN domain is a group which contains only the Security Gateway itself, for example where the Security Gateway is acting as a backup to a primary Security Gateway in an MEP environment.)

   The network Security Gateway objects are now configured, and need to be added to a VPN community.

   Note -There is nothing to configure on the **IPsec VPN** page, regarding certificates, because internally managed Security Gateways automatically receive a certificate from the internal CA.

6. Open the **Object Explorer** (CTRL+E), and select **VPN Communities**.

   a. Click **New** > **VPN Communities** > **Meshed Community**.

      The **New Meshed Community** window opens.

   b. In the **Encrypted Traffic** page, select **Accept all encrypted traffic** if you need all traffic between the Security Gateways to be encrypted. If not, then create applicable rules in the Security Policy Rule Base that allows encrypted traffic between community members (step 7).

   c. On the **Gateways** page, add the Security Gateways created in Step 1.

   A VPN tunnel is now configured.

   For information on other options, such as **Encryption**, **Shared Secret**, and **Advanced**, see: IPsec & IKE

7. If you did not select **Accept all encrypted traffic** in the **Encrypted Traffic** page of the Community, build an access control policy.

   For example:

Source	Destination	VPN	Service	Action
* Any	* Any	Meshed VPN Community	* Any	Accept

Where "Meshed VPN Community" is the VPN community you just defined.

Configuring a Star Community Between Internally Managed Gateways

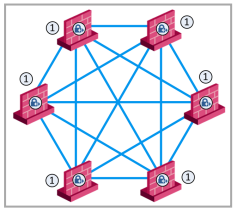
A star VPN community is configured in much the same way as a meshed community, the difference being the options on the **Star Community** window:

- On the **VPN Routing** page - Select **To center only**.
- On the Gateways page:
  - **Central Gateways** - Add the central Security Gateways.
  - **Central Gateways** - Select **Mesh central Security Gateways** if you want the central Security Gateways to communicate.
  - **Satellite Gateways** - Add the satellite Security Gateways.

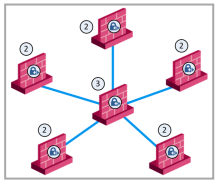
VPN Communities

A VPN Domain is a collection of internal networks that use Security Gateways to send and receive VPN traffic. Define the resources that are included in the VPN Domain for each Security Gateway. Then join the Security Gateways into a VPN community - collection of VPN tunnels and their attributes. Network resources of different VPN Domains can securely communicate with each other through VPN tunnels that terminate at the Security Gateways in the VPN communities.

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN tunnels between each pair of Security Gateway. In a Star community, each satellite Security Gateway has a VPN tunnel to the central Security Gateway, but not to other Security Gateways in the community.



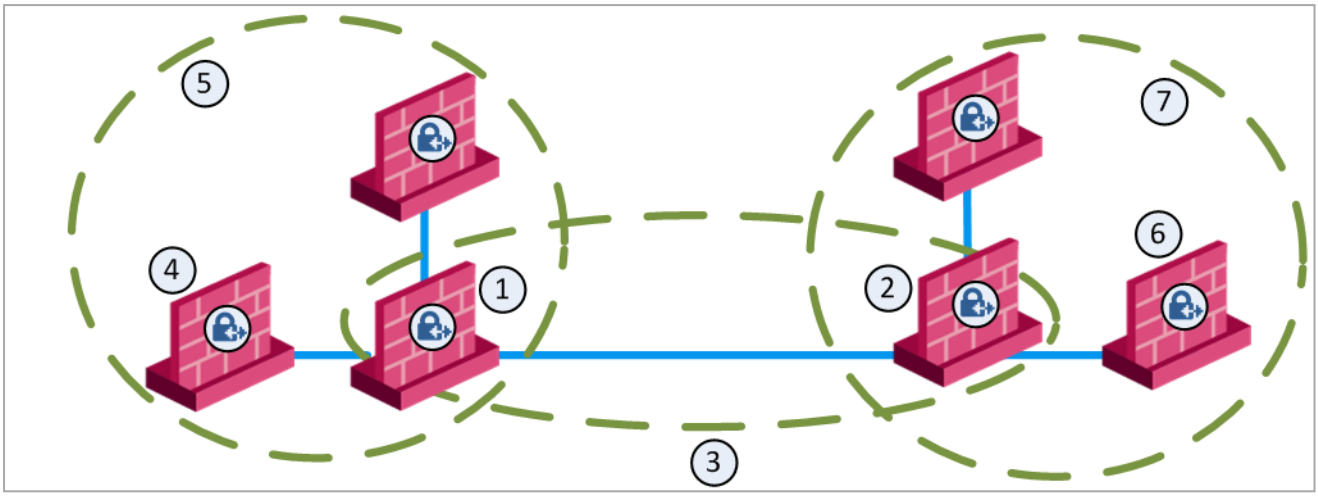
Mesh Topology



Star Topology

Item	Description
1	Security Gateway
2	Satellite Security Gateways
3	Central Security Gateway

Sample Combination VPN Community



Item	Description
1	London Security Gateway
2	New York Security Gateway
3	London - New York Mesh community
4	London company partner (external network)
5	London Star community
6	New York company partner (external network)
7	New York Star community

This deployment is composed of a Mesh community for London and New York Security Gateways that share internal networks. The Security Gateways for external networks of company partners do not have access to the London and New York internal networks. However, the Star VPN communities let the company partners access the internal networks of the sites that they work with.

VPN Domain Configuration

What can I do here?

Use this window to configure the VPN Domain of the Gateway.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Gateways > Add a gateway and double click on it.

VPN Communities - Encrypted Traffic

What can I do here?

Use this window to configure which gateways accept encrypted traffic.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Encrypted Traffic

Encrypted Traffic Options

- **Accept all encrypted traffic** adds a new rule to the Security Policy Rule Base. The rule encrypts all traffic between the Security Gateways.
- **Log Traffic** shows the logging option configured in **Global Properties > Log and Alert**.

VPN Communities - Encryption

What can I do here?

Use this window to set the Encryption Methods and Suites used by Community Members when exchanging keys or handling IPSec connections.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > Star/Mesh Community > Encryption

Selecting Encryption Methods

The methods selected depend on the organization's Security Policy, government regulations or other considerations such as encryption and integrity strength, or performance issues. Methods selected here apply to the whole community.

If different levels of encryption or different integrity methods are required between Security Gateways, consider defining additional communities, each with the relevant Security Gateways and methods.

Encryption Options

- **Encryption Method** - For IKE phase I and II.
  - **IKEv1 for IPv4 and IKEv2 for IPv6 only**.
  - **IKEv2 only** - Only support encryption using IKEv2. Security Gateways in this community cannot access peer gateways that support IKEv1 only.

- **Prefer IKEv2, support IKEv1** - If a peer supports IKEv2, the Security Gateway will use IKEv2. If not, it will use IKEv1 encryption. This is recommended if you have a community of older and new Check Point Security Gateways.

- **Encryption Suite** - The methods negotiated in IKE phase 2 and used in IPSec connections. Select the option for best interoperability with other vendors in your environment.
  - **Suite-B GCM-256** - (AES-GCM-256, SHA-384, EC Diffie-Hellman Group 20). See RFC 6379.
  - **VPN B** - (AES, AES-XCBC, Diffie-Hellman Group 14)). See RFC 4308.
  - **VPN-A** - (3DES, SHA-1, Diffie-Hellman Group 2). See RFC 4308.
  - **Suite-B GCM-128** - (AES-GCM-128, SHA-256, EC Diffie-Hellman Group 19). See RFC 6379
- **Custom Encryption Suite** - If you require algorithms other than those specified above. Select these properties for IKE Phase 1 and 2.

  IKE Security Association (Phase 1)
  - **Encryption Algorithm**
  - **Data Integrity**
  - **Diffie-Hellman Group**

  IKE Security Association (Phase 2)
  - **Encryption Algorithm**
  - **Data Integrity**

- **Use Perfect Forward Secrecy**

  The keys created by peers during IKE phase II and used for IPsec are based on a sequence of random binary digits exchanged between peers, and on the DH key computed during IKE phase I.

  The DH key is computed once, then used a number of times during IKE phase II. Since the keys used during IKE phase II are based on the DH key computed during IKE phase I, there exists a mathematical relationship between them. For this reason, the use of a single DH key may weaken the strength of subsequent keys. If one key is compromised, subsequent keys can be compromised with less effort.

  In cryptography, Perfect Forward Secrecy (PFS) refers to the condition in which the compromise of a current session key or long-term private key does not cause the compromise of earlier or subsequent keys. Security Gateways meet this requirement with a PFS mode. When PFS is enabled, a fresh DH key is generated during IKE phase II, and renewed for each key exchange.

  However, because a new DH key is generated during each IKE phase I, no dependency exists between these keys and those produced in subsequent IKE Phase I negotiations. Enable PFS in IKE phase II only in situations where extreme security is required. The DH group used during PFS mode is configurable between groups 1, 2, 5 and 14, with group 2 (1024 bits) being the default.

  Note - PFS mode is supported only between Security Gateways, not between Security Gateways and remote access clients.

Override Encryption for Externally Managed Gateways

The Encryption context, method, and suite can be overwrote for any externally managed gateway.

VPN Communities - Granular Encryption

What can I do here?

Use this window for override encryption for externally managed gateways.

> **Getting Here** - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > Star/Mesh Community > Encryption > Override Encryption for Externally Managed Gateways.

VPN Communities - Tunnel Management

What can I do here?

Use this window to set permanent VPN tunnels and VPN Tunnel Sharing.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Tunnel Management

Understanding VPN Tunnels

Overview of Tunnel Management

The VPN tunnel transports data securely. You can manage the types of tunnels and the number of tunnels with these features:

- **Permanent Tunnels** - Keeps VPN tunnels active to allow real-time monitoring capabilities.
- **VPN Tunnel Sharing** - Provides greater interoperability and scalability between Security Gateways. It also controls the number of VPN tunnels created between peer Security Gateways.

See the status of all VPN tunnels in SmartView Monitor. For details see *Monitoring Tunnels* in the *R81.10 Logging and Monitoring Administration Guide*.

Permanent Tunnels

As companies have become more dependent on VPNs for communication to other sites, uninterrupted connectivity has become more crucial than ever before. Therefore it is essential to make sure that the VPN tunnels are kept up and running. Permanent Tunnels are constantly kept active and as a result, make it easier to recognize malfunctions and connectivity problems. Administrators can monitor the two sides of a VPN tunnel and identify problems without delay.

Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

- Can be specified for an entire community. This option sets every VPN tunnel in the community as permanent.
- Can be specified for a specific Security Gateway. Use this option to configure specific Security Gateways to have permanent tunnels.
- Can be specified for a single VPN tunnel. This feature allows configuring specific tunnels between specific Security Gateways as permanent.

Permanent Tunnels in a MEP Environment

In a *Multiple Entry Point* (MEP) environment, VPN tunnels that are active are rerouted from the predefined primary Security Gateway to the backup Security Gateway if the primary Security Gateway becomes unavailable. When a Permanent Tunnel is configured between Security Gateways in a MEP environment where RIM is enabled, the satellite Security Gateways see the center Security Gateways as "unified." As a result, the connection will not fail but will fail over to another center Security Gateway on a newly created permanent tunnel.

Tunnel Testing for Permanent Tunnels

Check Point uses a proprietary protocol to test if VPN tunnels are active, and supports any site-to-site VPN configuration. Tunnel testing requires two Security Gateways, and uses UDP port 18234. Check Point tunnel testing protocol does not support 3rd party Security Gateways.

Dead Peer Detection

In addition to Tunnel Testing, *Dead Peer Detection* (DPD) is a different method to test if VPN tunnels are active. *Dead Peer Detection* does support 3rd party Security Gateways and supports permanent tunnels with interoperable devices based on IKEv1/IKEv2 DPD (IKEv1 DPD is based on RFC 3706). It uses IPsec traffic patterns to minimize the number of messages required to confirm the availability of a peer.

The tunnel testing mechanism is the recommended keepalive mechanism for Check Point to Check Point VPN gateways because it is based on IPsec traffic and requires an IPsec established tunnel. DPD is based on IKE encryption keys only.

DPD Responder Mode

In this mode, the Check Pointgateway sends a DPD Vendor ID reply to a peer gateway that sent a DPD Vendor ID request. The Check Pointgateway does **not** send DPD Vendor ID requests. This mode is configured by default.

Use Case

Dead Peer Detection is configured by default to meet the minimum requirement for a Check Pointgateway to establish a VPN tunnel with a non-Check Pointgateway. Dead Peer Detection is **not** relevant for a VPN tunnel between Check Pointgateways that use the Check Point proprietary tunnel testing protocol.

Permanent Tunnel Mode Based on DPD

DPD can monitor remote peers with the permanent tunnel feature. All related behavior and configurations of permanent tunnels are supported.

Important - When configuring DPD with a third-party VPN gateway, you must include the Check Point Security Gateway's external interface IP address in the encryption domain of the third-party VPN peer.

To configure DPD for a permanent tunnel, the permanent tunnel must be in the VPN community. After you configure the permanent tunnel, configure Permanent Tunnel mode Based on DPD. There are different possibilities for permanent tunnel mode:

- **tunnel_test** (default) - The permanent tunnel is monitored by a tunnel test (as in earlier versions). It works only between Check Point Security Gateways. Keepalive packets are always sent.
- **dpd** - The active DPD mode. A peer receives DPD requests at regular intervals (10 seconds). DPD requests are only sent when there is no traffic from the peer.
- **passive** - The passive DPD mode. Peers do not send DPD requests to this peer. Tunnels with passive peers are monitored only if there is IPsec traffic and incoming DPD requests.

  Note: To use this mode for only some gateways, enable the `forceSendDPDPayload` registry key on Check Point remote peers.

To enable DPD monitoring:

On each VPN gateway in the VPN community, configure the **tunnel_keepalive_method** property, in *Database Tool (GuiDBEdit Tool)* or dbedit (see sk13301). This includes 3rd Party gateways. (You cannot configure different monitor mechanisms for the same gateway).

1. In Database Tool (GuiDBEdit Tool), go to **Network Objects** > **network_objects** > **<*Name of Security Gateways object*>** > **VPN**.
2. For the **Value**, select a permanent tunnel mode.
3. Save all the changes.
4. Install the Access Control Policy.

Optional Configuration:

- **IKE Initiation Prevention** - By default, when a valid IKE SA is not available, a DPD request message triggers a new IKE negotiation. To prevent this behavior, set the property **dpd_allowed_to_init_ike** to **false**.

  Edit the property in *Database Tool (GuiDBEdit Tool)* > **Network Objects** > **network_objects** > **<*Name of Security Gateways object*>** > **VPN**.
- **Delete IKE SAs for dead peer** - Based on RFC 3706, a VPN Gateway has to delete IKE SAs from a dead peer. This functionality is enabled, by default.

- To disable the feature, add this line to the *$CPDIR/tmp/.CPprofile.sh* file and then **reboot**:

  ```
  DPD_DONT_DEL_SA=0 ; export DPD_DONT_DEL_SA
  ```

  Note - It is not supported to change the value of this environment variable in the current shell session with the "**export DPD_DONT_DEL_SA=0**" command.

- To enable the feature (if you disabled it), remove the line with "`DPD_DONT_DEL_SA`" from the *$CPDIR/tmp/.CPprofile.sh* file and then **reboot**.

  Note - It is not supported to change the value of this environment variable in the current shell session with the "`export DPD_DONT_DEL_SA=1`"command.

VPN Tunnel Sharing

Tunnel test is a proprietary Check Point protocol used to see if VPN tunnels are active. Tunnel testing requires two Security Gateways and uses UDP port 18234. Third party gateways do not support tunnel testing.

VPN Tunnel Sharing provides interoperability and scalability by controlling the number of VPN tunnels created between peer Security Gateways.

There are three available settings:

- **One VPN tunnel per each pair of hosts**
- **One VPN tunnel per subnet pair**
- **One VPN tunnel per Security Gateway pair**

VPN Management Tunnel Options

Permanent Tunnels

Permanent Tunnels are VPN tunnels that are constantly kept active and as a result, make it easier to recognize malfunctions and connectivity problems. Administrators can monitor the two sides of a VPN tunnel, and identify problems without delay.

Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. Permanent Tunnels can only be established between Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

- **On all tunnels in the community** - This option sets every VPN tunnel in the community as permanent.
- **On all tunnels of specific Gateways** - Use this option to configure specific gateways to have permanent tunnels.

- **On specific tunnels in the community** - This feature allows configuring specific tunnels between specific gateways as permanent.

Enable Route Injection Mechanism (RIM)

The Route Injection Mechanism (RIM) is a feature of the VPN module used to:

- Route return packets through the correct link or gateway
- Overcome link down time.

For example, when a link becomes unavailable, an alternative path is added or "injected" to the local routing table on the gateway. If a dynamic routing protocol is then configured, this change is propagated to the network behind the gateway. Route injection can be integrated with MEP functionality, providing an alternative to IP pool NAT in situations where large numbers of static IP addresses are not available.

Tracking Options

Several types of alerts can be configured to keep administrators up to date on the status of the VPN tunnels. Choosing one of these alert types will enable immediate identification of the problem and the ability to respond to these issues more effectively. The Tracking Options are:

- **None** - No action is taken.
- **Log** - The connection or loss of connection is logged.
- **Popup Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.
- **Mail Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.
- **SNMP Trap Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.
- **User Defined Alert** - Three different User Defined Alerts can be configured in the **Alert Commands** page of the **Global Properties** window. The action taken follows the pre-defined configuration.

VPN Tunnel Sharing

Since various vendors implement IPSec tunnels in a number of different methods, administrators need to cope with different means of implementation of the IPSec framework.

There are three settings for controlling the number of VPN tunnels between peer gateways:

- **One VPN tunnel per each pair of hosts** - A VPN tunnel is created for every session initiated between every pair of hosts.

- **One VPN tunnel per subnet pair** - Once a VPN tunnel has been opened between two subnets, subsequent sessions between the same subnets will share the same VPN tunnel. This is the default setting and is compliant with the IPSec industry standard.
- **One VPN tunnel per Gateway pair** - One VPN tunnel is created between peer gateways and shared by all hosts behind each peer gateway.

Tunnel Management - Select Gateways

What can I do here?

Use this window to select gateways that will maintain permanent VPN tunnels with their peers in the VPN community.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Tunnel Management > Permanent Tunnels section > Select Gateways button

Tunnel Management - Permanent Tunnel Tracking

What can I do here?

Use this window to set tracking options for permanent tunnels.

Getting Here - SmartConsole > Security Policies > Policy > Access Tools > VPN Communities > New Star/Mesh Community > Tunnel Management > Permanent Tunnels section > Gateway's button > Gateway Tunnel Properties

Up and Down Track Options

Several types of alerts can be configured to keep administrators up to date on the status of the VPN tunnels.

Tell me about the fields...

The Tracking Options are:

- **None** - No action is taken.
- **Log** - The connection or loss of connection is logged.
- **Popup Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.
- **Mail Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.

- **SNMP Trap Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.
- **User Defined Alerts** - Three different User Defined Alerts can be configured in the **Alert Commands** page of the **Global Properties** window. The action taken follows the pre-defined configuration.

Select Permanent Tunnels

What can I do here?

Use this window to Select permanent tunnels.

Click inside the white box.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Mesh Community > Tunnel Management > Permanent Tunnels section > Select Permanent Tunnels button

Tunnel Management - Permanent Tunnel Tracking - Specific Tunnels

What can I do here?

Use this window to set permanent tunnels and their tracking options.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Mesh Community > Tunnel Management > Permanent Tunnels section > Select Permanent Tunnels button > Click inside white table cell

Configuring Permanent Tunnels

To designate a Permanent Tunnel between gateways:

1. Double-click in the cell that intersects the two gateways where a Permanent Tunnel is required.
2. The **Tunnel Properties** window opens.
3. Select **Set these tunnels to be permanent tunnels**.
4. Set Tracking options.

Tunnel Selection in Mesh VPN Communities

What can I do here?

Use this window to select gateways in the Mesh VPN community that have permanent tunnels configured between them.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Mesh Community > Tunnel Management > Permanent Tunnels section > Select Permanent Tunnels

Configuring Permanent Tunnels

To designate a Permanent Tunnel between gateways:

1. Double-click in the cell that intersects the two gateways where a Permanent Tunnel is required.
2. The **Tunnel Properties** window opens.
3. Select **Set these tunnels to be permanent tunnels**.
4. Set Tracking options.

Route Injection Mechanism (RIM)

What can I do here?

Use this window to configure RIM for gateways in a Meshed or Star VPN community.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star Community > Tunnel Management > Permanent Tunnels section > Enable Route Injection Mechanism > Settings

Understanding RIM

Overview of Route Injection

Route Injection Mechanism (RIM) enables a Security Gateway to use dynamic routing protocols to propagate the encryption domain of a VPN peer Security Gateway to the internal network. When a VPN tunnel is created, RIM updates the local routing table of the Security Gateway to include the encryption domain of the VPN peer.

Note - Route Injection is not currently supported for IPv6.

RIM can only be enabled when permanent tunnels are configured for the community. Permanent tunnels are kept alive by tunnel test packets. When a Security Gateway fails to reply, the tunnel is considered "down." As a result, RIM deletes the route to the failed link from the local routing table, which triggers neighboring dynamic routing enabled devices to update their routing information accordingly. This results in a redirection of all traffic destined to travel across the VPN tunnel, to a pre-defined alternative path.

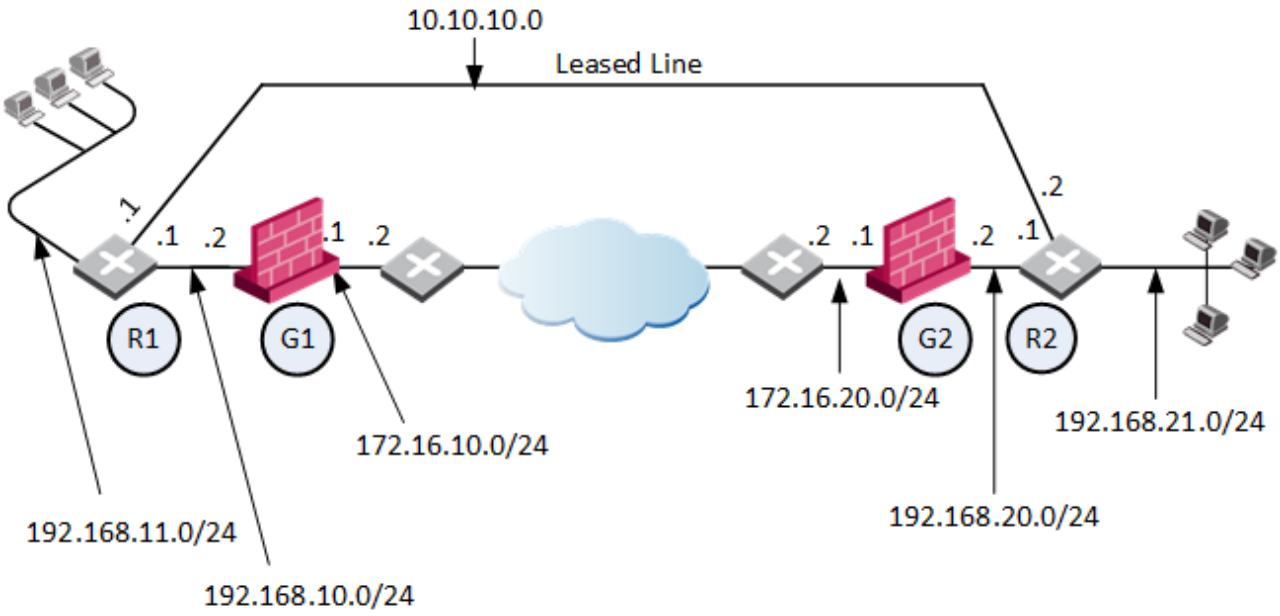
There are two possible methods to configure RIM:

- Automatic RIM - RIM automatically injects the route to the encryption domain of the peer Security Gateways.
- Custom Script - Specify tasks for RIM to perform according to specific needs.

Route injection can be integrated with MEP functionality, which sends return packets back through the same MEP Security Gateway.

Automatic RIM

In this scenario:



Label	Meaning
R1	Router 1
G1	Security Gateway 1
R2	Router 2
G2	Security Gateway 2

- RIM is enabled in the VPN community in which Security Gateway 1 and Security Gateway 2 participate.
- When the Security Gateways create a VPN tunnel, and the Permanent Tunnel status changes to "UP", RIM updates the routing tables:
  - The routing table on Security Gateway 1 gets the routes for the encryption domain of Security Gateway 2.
  - The routing table on Security Gateway 2 gets the routes for the encryption domain of Security Gateway 1.
- Security Gateway 1 has a dynamic routing neighborship with Router 1 and propagates RIM routes to Router 1.
- Security Gateway 2 has a dynamic routing neighborship with Router 2 and propagates RIM routes to Router 2.
- If the VPN tunnel becomes unavailable (Permanent Tunnel status with a peer changes to "DOWN"), then RIM removes routes from the routing tables of Security Gateway 1 and Security Gateway 2. The Security Gateways update their corresponding neighbors: Router 1 and Router 2. The routers start to send traffic over the leased line.

Below are the routing tables on the Security Gateways and Routers based on the diagram above. Entries in bold represent routes that RIM injected into the Security Gateway's local routing table:

For Security Gateway 1:

Destination	Netmask	Next Hop	Metric
0.0.0.0	0.0.0.0	172.16.10.2	1
192.168.21.0	**255.255.255.0**	**172.16.10.2**	**1**
192.168.11.0	255.255.255.0	192.168.10.1	1

Security Gateway 2:

Destination	Netmask	Next Hop	Metric
0.0.0.0	0.0.0.0	172.16.20.2	1
192.168.11.0	**255.255.255.0**	**172.16.20.2**	**1**
192.168.21.0	255.255.255.0	192.168.20.1	1

Router 1 (behind Security Gateway 1):

Destination	Netmask	Next Hop	Metric
0.0.0.0	0.0.0.0	192.168.10.2	1
192.168.21.0	**255.255.255.0**	**192.168.10.2**	**1**
192.168.21.0	255.255.255.0	10.10.10.2	2

Router 2 (behind Security Gateway 2):

Destination	Netmask	Next Hop	Metric
0.0.0.0	0.0.0.0	192.168.20.2	1
192.168.11.0	**255.255.255.0**	**192.168.20.2**	**1**
192.168.11.0	255.255.255.0	10.10.10.1	2

Custom Scripts

Custom scripts can be run on any Security Gateway in the community. These scripts are executed whenever a tunnel changes its state (example: goes "up" or "down"). Such an event, for example, can be the trigger that initiates a dial-up connection.

There is a script template **custom_rim** (with a **.sh** or **.bat** extension depending on the operating system) in the **$FWDIR/scripts/** directory.

Sample customized script:

```
#!/bin/sh

# This script is invoked each time a tunnel is configured with
the RIM option
# and the tunnel changed state.
#
# You may add your custom commands to be invoked here.

# Parameters read from command line.
RIM_PEER_GW=$1
RIM_NEW_STATE=$2
RIM_HA_STATE=$3
RIM_FIRST_TIME=$4
RIM_PEER_ENC_NET=$5

case "${RIM_NEW_STATE}" in
      up)
            # Place your action for tunnels that came up
            ;;
      down)
            # Place your action for tunnel that went down
            ;;
esac
```

Where:

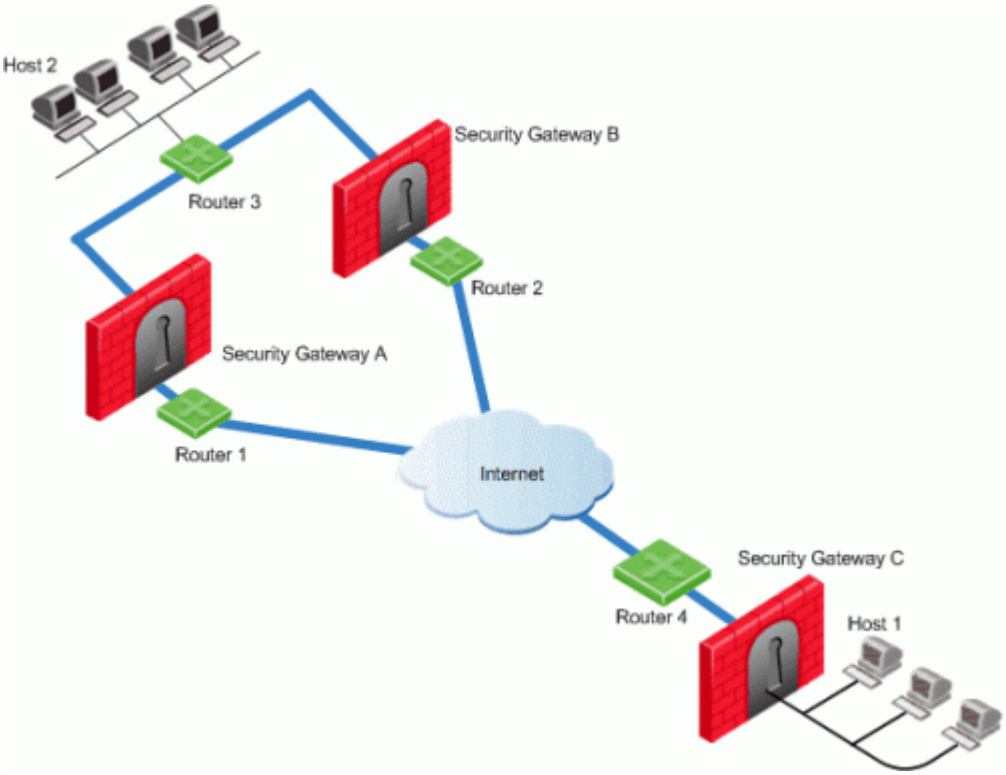
- `RIM_PEER_GW`: Peer Security Gateway
- `RIM_NEW_STATE`: Change in the state of the Security Gateway,(example: up or down).
- `RIM_HA_STATE`: State of a single Security Gateway in a cluster (example: standby or active).
- `RIM_FIRST_TIME`: The script is executed separately for each network in the peer's encryption domain. Though the script can be executed multiple times on a peer, this parameter is transferred to the script with the value of '1' only the first time the script runs on the peer. The value '1' indicates the first time this script is executed. The next time the script is executed, it is transferred with the value of '0' and the parameter is disregarded. For example, you can send an email alert to the system administrator the moment a tunnel goes down.
- `RIM_PEER_ENC_NET`: VPN domain of the VPN peer.

Injecting Peer Security Gateway Interfaces

You can inject the IP addresses of the peer Security Gateway into the routing tables, in addition to the networks behind the Security Gateway.

For example, after a VPN tunnel is created, RIM injects the encryption domain of the peer Security Gatewayinto the local routing tables of both Security Gateways.When RIM enabled Security Gateways communicate with a Security Gateway that has Hide NAT enabled, it is necessary to inject the peer's interfaces.

In this scenario:



- Security Gateways A and B are both RIM enabled and Security Gateway C has Hide NAT enabled on the external interface ("hiding" all the IP addresses behind it).
- Host 1, behind Security Gateway C, initiates a VPN tunnel with Host 2, through Security Gateway A.
- Router 3 holds routes to all the hosts behind Security Gateway C. Because Router 3 does not have the Hide NAT IP address of Security Gateway C, Router 3 cannot properly route packets back to Host 1.

To route back packets:

1. In SmartConsole:
    a. Click **Menu > Global properties**.
    b. Click **VPN Advanced Properties > Tunnel Management**.
    c. Select **RIM_inject_peer_interfaces**. This injects Router 3 with all of the IP addresses of Security Gateway C (this includes the Hide NAT address).
    d. Click **OK**.
    e. Install the Access Control Policy.
2. Configure the router not to propagate the information injected to other Security Gateways. For example, in the scenario shown above this could result in Security Gateway B routing traffic to Security Gateway C through Security Gateway A.

RIM - Options

For Star and Mesh communities, there are two possible ways to configure RIM:

- **Enable Automatic Route Injection Mechanism** - RIM automatically injects the route to the encryption domain of the peer gateways.
- **Enable customer editable script execution** - Specify tasks for RIM to perform according to specific needs. A script template **custom_rim** (with a **.sh** ot **.bat** extension depending on the operating system) is provided in the **$FDIR/Scripts**directory.

Tracking Options

- **None** - No action is taken.
- **Log** - The connection or loss of connection is logged.
- **Popup Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.
- **Mail Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.
- **SNMP Trap Alert** - The action specified in the **Alert Commands** page of the **Global Properties** window is taken.
- **User Defined Alerts** - Three different User Defined Alerts can be configured in the **Alert Commands** page of the **Global Properties** window. The action taken follows the pre-defined configuration.

VPN Communities - VPN Routing

What can I do here?

Use this window to configure VPN routing for satellites.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star Community > VPN Routing

Understanding VPN Routing

VPN Star Communities

A Star Community is a VPN Community composed of two types of members, Central and Satellite, where:

- Each central gateway can establish VPN tunnel with each satellite gateway
- Satellite gateways cannot establish VPN tunnels with each other
- Central gateways cannot establish VPN tunnel with each other by default, but this is configurable on the **Central Gateways** page

VPN Routing

VPN routing is a way of directing communication through a specific VPN tunnel in order to enhance existing connectivity or security. In addition VPN routing can be used to reduce connectivity costs. A star VPN Community supports VPN routing in the following way. The HUB (the machine through which the VPN communication is redirected) is defined as a central gateway, and the SPOKES (the endpoint machines that receive or initiate the VPN connection) as Satellites. A VPN tunnel is created between the central gateway and the satellite gateways. Packets sent by the SPOKES are routed through the HUB.

VPN Routing Options

- **To center only** . No VPN routing actually occurs. Only connections between the satellite gateways and central gateway go through the VPN tunnel. Other connections are routed in the normal way
- **To center and to other satellites through center** . Use VPN routing for connection between satellites. Every packet passing from a satellite gateway to another satellite gateway is routed through the central gateway. Connection between satellite gateways and gateways that do not belong to the community are routed in the normal way.

- **To center, or through the center to other satellites, to internet and other VPN targets** . Use VPN routing for every connection a satellite gateway handles. Packets sent by a satellite gateway pass through the VPN tunnel to the central gateway before being routed to the destination address.

In a star community, RDP packets are sent to the gateways and the first to respond is used for routing only when:

1. There is more than one center gateway, **and**
2. One of the following VPN routing options was selected:
   - **To center and to other satellites through center**
   - **To center, or through the center to other satellites, to internet and other VPN targets**

VPN Communities - MEP

What can I do here?

Use this window to configure

- Multiple Entry Points (MEP) to the core network
- Tracking options
- Return packet routing

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star Community > MEP

Multiple Entry Point

MEP Overview

Multiple Entry Point (MEP) is a feature that provides a High Availability and Load Sharing solution for VPN connections. The VPN module is installed on a Security Gateway that provides a single point of entry to the internal network. This Security Gateway makes the internal network "available" to peer Security Gateways. If the Security Gateway becomes unavailable, then peer Security Gateways cannot access the internal network.

A MEP environment has two or more Security Gateways that enable access to the same VPN domain. In a MEP environment, peer Security Gateways provide redundancy for uninterrupted access to the internal network.

VPN High Availability Using MEP or Clustering

Both MEP and Clustering are ways of achieving High Availability and Load Sharing.

However:

- Unlike the members of a ClusterXL Security Gateway Cluster, there is no physical restriction on the location of MEP Security Gateways. MEP Security Gateways can be geographically separated machines. In a cluster, the clustered Security Gateways need to be in the same location, directly connected via a *sync* interface.
- MEP Security Gateways can be managed by different Security Management Servers. Cluster members must be managed by the same Security Management Server.
- In a MEP configuration there is no "state synchronization" between the MEP Security Gateways. In a cluster, all of the Security Gateways hold the "state" of all the connections to the internal network. If one of the Security Gateways fails, the connection passes seamlessly over (performs *failover*) to another Security Gateway, and the connection continues. In a MEP configuration, if a Security Gateway fails, the current connection is lost and one of the backup Security Gateways picks up the *next* connection.
- In a MEP environment, the decision which Security Gateway to use is taken on the remote side; in a cluster, the decision is taken on the Security Gateway side.

Implementing MEP

MEP is implemented using RDP for Check Point Security Gateways and DPD for 3rd party Gateways / Cloud vendors.

- RDP is a proprietary Probing Protocol (PP) that sends special UDP RDP packets to port 259 to discover whether an IP is reachable. This protocol is proprietary to Check Point and does not conform to RDP as specified in RFC 908 / RFC 1151.
  Note - These UDP RDP packets are not encrypted, and only test the availability of a peer.
- DPD is a different method that discovers whether an IP is reachable. It supports 3rd party Security Gateways / Cloud vendors based on IKEv1/IKEv2.

Note - In an MEP environment, a Security Gateway determines which protocol to use automatically.

The peer continuously probes or polls all MEP Security Gateways in order to discover which of the Security Gateways are "up", and chooses a Security Gateway according to the configured selection mechanism. Since RDP/DPD packets are constantly being sent, the status of all Security Gateways is known and updated when changes occur. As a result, all Security Gateways that are "up" are known.

There are two available methods to implement MEP:

MEP Method	Description
Explicit MEP	Only Star communities with more than one central Security Gateway can enable explicit MEP. This MEP method provides multiple entry points to the network behind the Security Gateways. When available, Explicit MEP is the recommended method.
Implicit MEP	This MEP method is supported in all scenarios, where fully or partially overlapping encryption domains exist, or where Primary-Backup Security Gateways are configured.

Routing Return Packets

To make sure return packets are routed correctly, the MEP Security Gateway can make use of either of these:

- IP Pool NAT (Static NAT)
- Route Injection Mechanism (RIM)

Multiple Entry Point - Options

Use these options to configure entry to the core network.

- **Select the closest gateway to source (First to respond)**. If "first to respond" is the chosen mechanism, then the first MEPed gateway to respond to the satellites probing RDP packets becomes the chosen gateway. Subsequent connections pass through the chosen gateway
- **Select the closest gateway to destination (By VPN domain)** . An extension to the traditional Primary-backup MEP configuration. Before the MEP unification, the destination IP belonged to a particular VPN domain. The gateway of that domain becomes the chosen entry point. This gateway becomes the primary gateway while other gateways in the MEP become its backup gateways.
- **Random Selection (for Load distribution)** . To distribute the load, and prevent any one gateway from being flooded, connections can be evenly shared amongst all the gateways in the MEP configuration. When all gateways share equal priority (no primary) and are MEPed to the *same* VPN domain, a gateway is randomly chosen as the entry point to the network for each pair of source/destination IP addresses.
- **Manually set priority list (MEP rules)** . Which gateway will be chosen as the entry point to the core network can be controlled by manually setting a priority per source gateway. Each priority constitutes a MEP Rule. Click **Set...**to configure the rules

Tracking fields

From the drop-down box, select the type of tracking required.

Multiple Entry Point - Advanced

In some instances, more than one gateway is available in the center with no obvious priority between them. When this occurs, select how the gateway should be chosen, either by:

- First to respond
- Random Selection

Return Packet Routing

While MEP is used to determine which gateway to connect to, RIM (like IP Pool NAT) is used to correctly route return packets through the chosen gateway.

Return packets can be routed according to IP pool NAT, configured per gateway, or by using the route injection mechanism (RIM) configured in Tunnel Management.

IP Pool NAT

An IP Pool is a range of IP addresses (an Address Range, a network or a group of one of these objects) routable to the gateway or gateway cluster.

IP Pool NAT ensures proper routing for two connection scenarios:

- SecuRemote/SecureClient to MEPed (Multiple Entry Point) gateways.
- Gateway to MEP gateways.

Configuring IP Pool NAT

1. In **Global Properties** > **NAT** page, select **Enable IP Pool NAT**.
2. Set tracking options for address exhaustion and for address allocation and release. Then:
3. For each gateway, create a network object that represents the IP pool NAT addresses for that gateway. The IP pool can be a network, group, or address range. For example:
   - On the network objects tree, right-click **Network Objects**branch > **New > Address Range...** The **Address Range Properties** window opens.
   - On the **General** tab, enter the first IP and last IP of the address range.
   - Click **OK**. In the network objects tree, **Address Ranges** branch, the new address range appears.

4. On the gateway object where IP pool NAT translation is performed, **Gateway Properties** window, **NAT** > **IP Pool NAT** page, select either
   - **Allocate IP Addresses from**, and select the address range you created, OR
   - **Define IP Pool addresses on gateway interfaces** . If you choose this option, you need to define the IP Pool on each required interface, in the **Interface Properties** window, **IP Pool NAT** tab.
5. In the **IP Pool NAT** page, select either (or both):
   - **Use IP Pool NAT for VPN client connections**
   - **Use IP Pool NAT for gateway to gateway connections**
6. Click **Advanced.**
   - Decide after how many minutes unused addressees are returned to the IP pool.
   - Click **OK** twice.
7. Edit the routing table of each internal router, so that packets with an a IP address assigned from the NAT pool are routed to the appropriate gateway.

IP Pool NAT for Clusters

- In the Cluster object > **NAT > IP Pool NAT** page, choose the connection scenario.
- In the cluster member object > **IP Pool NAT**page, define the IP Pool on the cluster member. A separate IP pool must be configured for each cluster member. It is not possible to define a separate IP Pool for each cluster member interface.

MEP - Manual Priority List

What can I do here?

Use this window to set the order in which central gateways in a star community are chosen as the entry point to the core network. The central gateways are chosen in order of priority.

> **Getting Here** - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star Community > MEP > Manually set priority list option > Set

Understanding MEP Manual Priority

Which gateway will be chosen as the entry point to the core network can be controlled by manually setting a priority per source gateway. Each priority constitutes a MEP Rule.

The **MEP manual priority list** window is divided into the default rule, and rules which provide exceptions to the default rule. The default MEP rule takes effect when:

- No MEP rules are defined
- When the source of the connection cannot be found in the **Exception priority rules**

The **Exception priority rules**section contains three priority levels: primary, secondary, and tertiary. While there are only three priority levels,

- The same priority can be assigned to several central gateways
- The same rule can be assigned to several satellite gateways
- A priority level can be left blank

VPN Communities - Excluded Services

What can I do here?

Use this window to exclude services from the community. Excluded services are not encrypted and not matched to rules for the VPN community.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Excluded Services

Understanding Excluded Services

Services excluded from encryption are required for VPN control connections, such as a connection that installs a Security Policy. Control connections traversing the gateway on their way from the Security Management server to the remote enforcement point must not be modified (encrypted) by the gateway. Typically, these control connections are handled by *implied rules* in the Security Policy.

Although *implied rules* defined in the **Global Properties** resolve this issue, you may prefer to disable the implied rules and define special rules for control connections. In this instance, include these services in the list for services in the clear.

VPN Communities - Shared Secret

What can I do here?

Use this window to configure a shared secret (password) between all externally and internally managed members of the VPN community that do not use certificates for authentication.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Shared Secret

Understanding Shared Secrets

IKE supports Shared Secret authentication as well as certificates. Internally managed gateways have at least one certificate - the VPN certificate issued by the Internal CA. When a VPN is established between two internally managed gateways, VPN enforces the use of certificates for authentication. In situations where an externally managed gateway does not have a certificate, Shared Secret authentication is used.

Externally managed peer gateways that use Shared Secret authentication are listed in the window's table. To edit the shared secret, select the peer gateway and click the edit button. The same Shared Secret is used between the externally managed gateway and all the internally managed gateways.

Shared Secret - Editing

What can I do here?

Use this window to edit or enter a shared secret.

The secret must be at least six characters long, no more than 64 characters, and contain four different characters.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Mesh Community > Shared Secret > Select peer > Edit

VPN Communities - Wire Mode

What can I do here?

Use this window to allow encrypted traffic between wire mode interfaces to pass without inspection. Wire mode is configured in two places:

- On the community object
- On the gateway object

Enabling Wire Mode on the community allows information to pass through a VPN tunnel without state verification.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Wire Mode

Understanding Wire Mode

Overview of Wire Mode

The *Wire Mode* improves connectivity by allowing existing connections to fail over successfully by bypassing firewall enforcement. Traffic within a VPN community is, by definition, private and secure. In many cases, the firewall and the rule on the firewall concerning VPN connections is unnecessary. With the *Wire Mode*, the firewall can be bypassed for VPN connections by defining internal interfaces and communities as "trusted".

When a packet reaches a Security Gateway, the Security Gateway asks itself two questions regarding the packet(s):

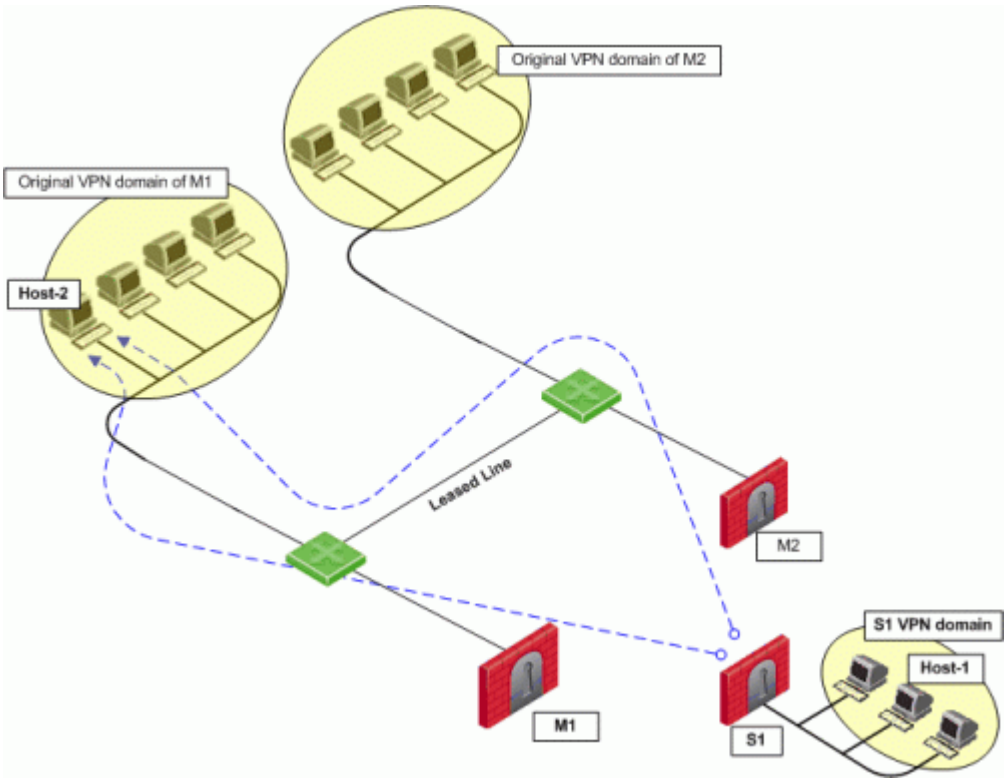
Is this information coming from a "trusted" source?

Is this information going to a "trusted" destination?

If the answer to both questions is yes, and the VPN Community to which both Security Gateways belong is designated as "*Wire Mode* enabled," stateful inspection is not enforced and the traffic between the trusted interfaces bypasses the firewall. Since no stateful inspection takes place, no packets can be discarded. The VPN connection is no different from any other connection along a dedicated wire. This is the meaning of "*Wire Mode*." Since stateful inspection no longer takes place, dynamic routing protocols (which do not survive state verification in non-wire mode configuration) can now be deployed. *Wire Mode* thus facilitates Route Based VPN.

Wire Mode in a MEP Configuration

In this scenario:

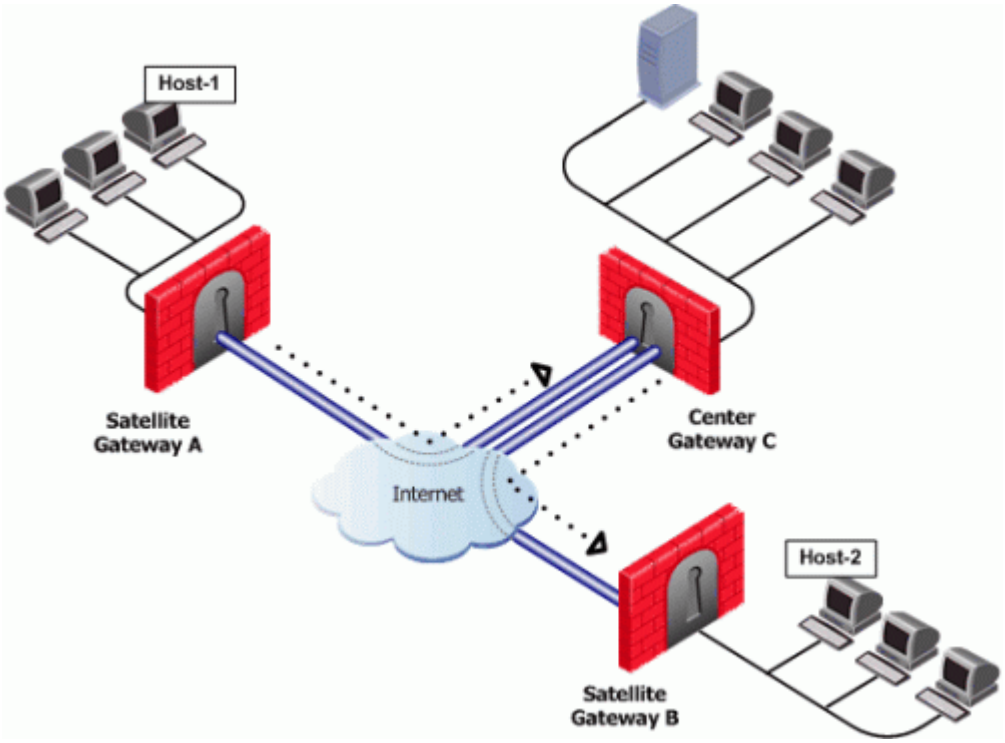


- Security Gateway **M1** and Security Gateway **M2** are both wire mode enabled and have trusted internal interfaces.
- The community where Security Gateway **M1** and Security Gateway **M2** reside, is wire mode enabled.
- Host 1, residing behind Security Gateway **S1** is communicating through a VPN tunnel with **Host 2** residing behind Security Gateway **M1** .
- MEP is configured for Security Gateway **M1** and Security Gateway M2 with Security Gateway **M1** being the primary Security Gateway and Security Gateway **M2** as the backup.

In this case, if Security Gateway **M1** goes down, the connection fails over to Security Gateway **M2**. A packet leaving **Host 2**will be redirected by the router behind Security Gateway **M1** to Security Gateway **M2** since Security Gateway **M2** is designated as the backup Security Gateway. Without wire mode, stateful inspection is enforced at Security Gateway **M2** and the connection is dropped. Packets that come into a Security Gateway whose session was initiated through a different Security Gateway, are considered "out-of-state" packets. Since Security Gateway **M2**'s internal interface is "trusted," and wire mode in enabled on the community, no stateful inspection is performed and Security Gateway **M2** will successfully continue the connection without losing any information.

Wire Mode with Route-based VPN

In this scenario:



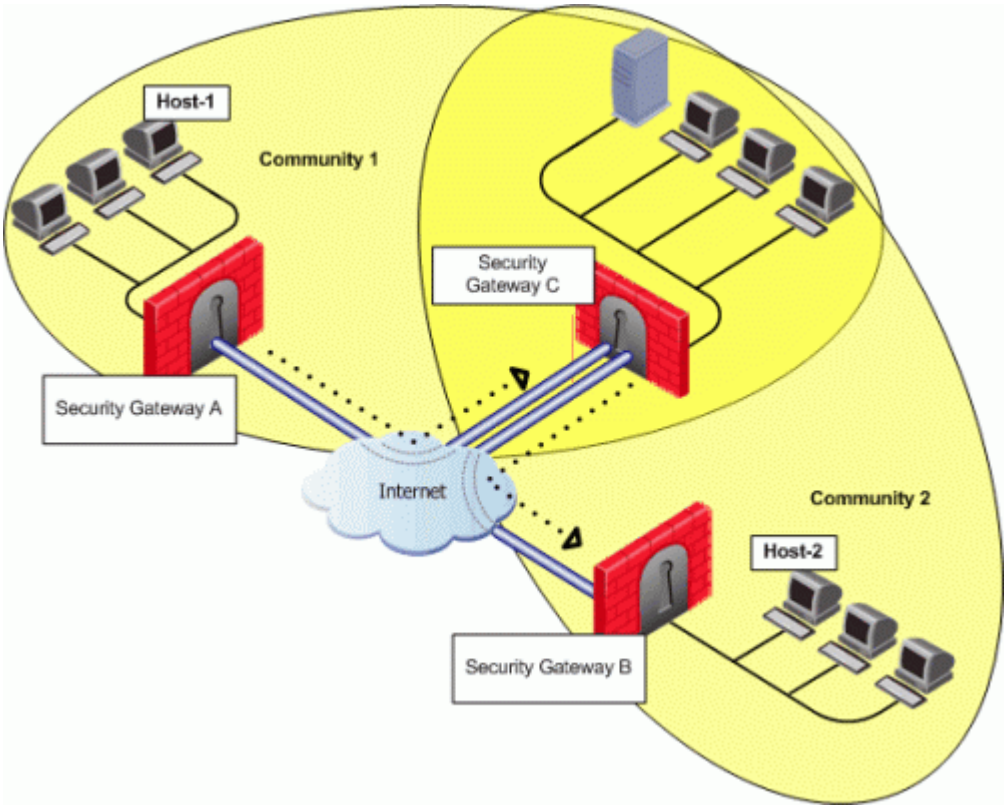
- Wire mode is enabled on Center Security Gateway C (without an internal trusted interface specified).
- The community is wire mode enabled.
- Host 1 residing behind Satellite Security Gateway A wishes to open a connection through a VPN tunnel with Host 2 behind Satellite Security Gateway B.

In a satellite community, Center Security Gateways are used to route traffic between Satellite Security Gateways within the community.

In this case, traffic from the Satellite Security Gateways is only rerouted by Security Gateway C and cannot pass through Security Gateway C's firewall. Therefore, stateful inspection does not need to take place at Security Gateway C. Since wire mode is enabled on the community and on Security Gateway C, making them trusted, stateful inspection is bypassed. Stateful inspection, however, does take place on Security Gateways A and B.

Wire Mode between two VPN Communities

In this scenario:



- Security Gateway A belongs to Community 1.
- Security Gateway B belongs to Community 2.
- Security Gateway C belongs to Communities 1 and 2.

- Wire mode is enabled on Center Security Gateway C (without an internal trusted interface specified).
- Wire mode is enabled on both communities.
- Host 1 residing behind Satellite Security Gateway A wishes to open a connection through a VPN tunnel with Host 2 behind Satellite Security Gateway B.

Wire mode can also be enabled for routing VPN traffic between two Security Gateways which are not members of the same community. Security Gateway C is a member of both communities and therefore recognizes both communities as trusted. When host 1 behind Security Gateway A initiates a connection to host 2 behind Security Gateway B, Security Gateway C is used to route traffic between the two communities. Since the traffic is not actually entering Security Gateway C, there is no need for stateful inspection to take place at that Security Gateway. Stateful inspection, however, does take place on Security Gateways A and B.

Configuring Wire Mode

Configuring Wire Mode

Wire mode is configured in two places:

- Community Properties (Meshed or Star)
- Security Gateway Properties

Enabling Wire Mode in a VPN Community

1. In SmartConsole, click the **Objects** menu > **Object Explorer**.
2. From the left tree, select the **VPN Communities**.
3. Open the VPN Community object.
4. From the left tree, click **Wire Mode**.
5. Select **Allow uninspected encrypted traffic between Wire mode interfaces of the Community members**.
6. To enable Wire Mode Routing, select **Wire Mode Routing - Allow members to route uninspected encrypted traffic in VPN routing configurations**.
7. Click **OK**.
8. Install the Access Control Policy.

Enabling Wire Mode on a specific gateway

1. In SmartConsole, from the left navigation panel, click **Gateways & Servers**.
2. Open the applicable Security Gateway object.
3. From the left tree, click **IPsec VPN** > **VPN Advanced**.
4. In the **Wire mode** section:
    a. Select **Support Wire Mode (and Wire mode routing - route uninspected encrypted traffic in VPN routing configurations)**.
    b. Click **Add**.
    c. Select the interfaces to be trusted by the selected Security Gateway.
    d. Click **OK**.
    e. Select **Log Wire mode traffic** to log the Wire Mode activity.
5. Click **OK**.
6. Install the Access Control Policy.

VPN Communities - Advanced

What can I do here?

Use this window to set IKE security associations and enable NAT inside the community.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > New Star/Meshed Community > Advanced

IKE and NAT inside the Community

IKE is the Internet Key Exchange protocol used in VPN for exchanging key-building material. Despite the name, keys are never actually exchanged. Only the material (random bits and mathematical data) used to build the keys are exchanged. IKE takes place in two phases.

IKE (Phase 1)

Change the default settings to alter the way the IKE Security Association is negotiated.

IPSEC (Phase 2)

Change the default settings to alter the way the IPSEC Security Association is negotiated.

Properties

Disable NAT Inside the VPN Community

Even if NAT is configured it is possible to disable NAT inside the VPN community. If NAT is disabled, when a host behind a community member opens a connection with another host behind a community member, the original IP addresses are used. Other connections use the translated address.

Use Aggressive mode

In aggressive mode, the Diffie-Hellman computation is performed parallel to authentication. A peer that is not yet authenticated can force processor intensive Diffie-Hellman computations on the other peer. Aggressive mode performs the IKE negotiation with three packets instead of six.

Support IP Compression

P compression is a process that reduces the size of the data portion of the TCP/IP packet. Such a reduction can cause significant improvement in performance. IPsec supports the Flate/DeflateIP compression algorithm. Deflate is a smart algorithm that adapts the way it compresses data to the actual data itself. Whether to use IP compression is decided during IKE phase II.

IP compression is not enabled by default. IP compression is important for SecuRemote / SecureClient users with slow links. For Example, dialup modems do compression as a way of speeding up the link. Security Gateway encryption makes TCP/IP packets appear "mixed up". This kind of data cannot be compressed and bandwidth is lost as a result. If IP compression is enabled, packets are compressed before encryption. This has the effect of recovering the lost bandwidth.

Remote Access Community - Participating Gateways

What can I do here?

Use this window to add gateways to the remote access VPN community.

Getting Here - SmartConsole > Security Policies > Policy > Access Tools > VPN Communities > Remote Access - Participating Gateways

Remote Access Community - Participating User Groups

What can I do here?

Use this window to add user groups to the remote access community. User groups can be defined in the internal database, or on LDAP servers.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > VPN Communities > Remote Access - Participating User Groups

UserCheck

What can I do here?

On the UserCheck page, you can create, edit, and preview UserCheck interaction objects and their messages.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > UserCheck

UserCheck Interactions in the Access Control Policy

UserCheck objects lets the Security Gateway communicate with users. Use them in the Rule Base to:

- Help users with decisions that can be dangerous to the organization's security.
- Share the organization's changing internet policy for Web applications and sites with users, in real-time.

If a UserCheck object is set as the action on in a policy rule, the user's browser redirects to the UserCheck web portal on port 443 or 80. The portal shows the notifications to the user.

UserCheck client adds the option to send notifications for applications that are not in a web browser. The UserCheck client can also work together with the UserCheck portal to show notifications on the computer itself when the notification cannot be displayed in a browser.

Configuring the Security Gateway for UserCheck

Enable or disable UserCheck directly on the Security Gateway. Make sure that the UserCheck is enabled on each Security Gateway in the network.

The Security Gateway has an internal persistence mechanism that preserves UserCheck notification data if the Security Gateway or cluster reboots. Records of a user answering or receiving notifications are never lost.

To configure UserCheck on a Security Gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The **Gateway Properties** window opens.

2. From the navigation tree, click U **serCheck**.

   The **UserCheck** page opens.

3. Make sure **Enable UserCheck for active blades** is selected

4. In the **UserCheck Web Portal** section:

In the **Main URL** field, enter the primary URL for the web portal that shows the UserCheck notifications.

If users connect to the Security Gateway remotely, make sure that the Security Gateway internal interface (in the **Network Management** page) is the same as the Main URL.

Note - The **Main URL** field must be manually updated if:

- The Main URL field contains an IP address and not a DNS name.
- You change a Security Gateway IPv4 address to IPv6 address, or the other way around.

5. **Optional:** Click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**.

   The aliases must be resolved to the portal IP address on the corporate DNS server

6. In the **Certificate** section, click **Import** to import a certificate that the portal uses to authenticate to the Security Management Server.

   By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority.

7. In the **Accessibility** section, click **Edit** to configure interfaces on the Security Gateway through which the portal can be accessed. These options are based on the topology configured for the Security Gateway. The topology must be configured.

   Users are sent to the UserCheck portal if they connect:

   - **Through all interfaces**
   - **Through internal interfaces**
     - **Including undefined internal interfaces**
     - **Including DMZ internal interfaces**
     - **Including VPN encrypted interfaces** - Interfaces used for establishing route-based VPN tunnels (VTIs)
   - **According to the Firewall policy** - Select this if there is a rule that states who can get an access to the portal.

   If the **Main URL** is set to an external interface, you must set the **Accessibility** option to one of these:

   - **Through all interfaces** - necessary in VSX environment
   - **According to the Firewall Policy**

8. In the **Mail Server** section, configure a mail server for UserCheck. This server sends notifications to users that the Gateway cannot notify using other means, if the server knows the email address of the user. For example, if a user sends an email which matched on a rule, the Gateway cannot redirect the user to the UserCheck portal because the traffic is not http. If the user does not have a UserCheck client, UserCheck sends an email notification to the user.
   - **Use the default settings** - Click the link to see which mail server is configured.
   - **Use specific settings for thisgateway** - Select this option to override the default mail server settings.
   - **Send emails using this mail server** - Select a mail server from the list, or click **New** and define a new mail server.
9. Click **OK**.
10. If there is encrypted traffic through an internal interface, add a new rule to the Firewall Layer of the Access Control Policy. This is a sample rule:

Source	Destination	VPN	Services & Applications	Action
Any	Security Gateway on which UserCheck client is enabled	Any	UserCheck	Accept

11. Install the Access Control Policy.

Blocking Applications and Informing Users

Scenario: I want to block pornographic sites in my organization, and tell the user about the violation. How can I do this?

To block an application or category of applications and tell the user about the policy violation:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Create a rule that includes these components:
   - **Services & Applications** - Select the **Pornography** category.
   - **Action** - **Drop**, and a UserCheck **Blocked Message** - **Access Control**.

     The message informs users that their actions are against company policy and can include a link to report if the website is included in an incorrect category.

- **Track** - Log

  Note - This Rule Base example contains only those columns that are applicable to this subject.

Name	Source	Destination	Services & Applications	Action	Track	Install On
Block Porn	Any	Internet	Pornography (category)	Drop Blocked Message	Log	Policy Targets

The rule blocks traffic to pornographic sites and logs attempts to access those sites. Users who violate the rule receive a UserCheck message that informs them that the application is blocked according to company Security Policy. The message can include a link to report if the website is included in an incorrect category.

> **Important** - A rule that blocks traffic, with the **Source** and **Destination** parameters defined as **Any**, also blocks traffic to and from the Captive Portal.

UserCheck for Access Control Default Messages

These are the default UserCheck messages in the **Access Tools** > **UserCheck** page of the Access Control Policy:

Name	Action Type	Description
Access Approval	Inform	
Access Notification	Inform	Shows when the action for the rule is inform. It informs users what the company policy is for that site.
Blocked Message - Access Control	Block	Shows when the action for the rule is Block, when a request is blocked.
Cancel Page - Access Control	Cancel	Shows after a user gets an Inform or Ask message and clicks Cancel.
Company Policy	Ask	Shows when the action for the rule is **ask**. It informs users what the company policy is for that site and they must click **OK** to continue to the site.

If the default UserCheck messages do not fit your needs, you can create a UserCheck Interaction Object.

For example, you can create a:

Message with Content Awareness Fields

If you define a custom UserCheck message, you can use predefined **Field** variables in the message.

Here is an example of a UserCheck message that you can define. This example uses some of the **Insert Field** variables for Application Control and Content Awareness rules:

```
According to the company policy, this action is intended for
work-related use only.
                Details:
                - File Name is classified as Data Types
                - Access to Application name
                - Category Category
[ ] I will use this site/application and data in accordance with
company policy.
Reference: Incident ID
```

You can show these UserCheck message previews:

- **Regular view** - Shows a preview of the UserCheck message on a computer.
- **Mobile** - Shows a preview of the UserCheck message on a mobile device.
- **Agent** - Shows a preview of the UserCheck message in the agent window.
- **Email** - Shows a preview of the UserCheck message in an email.

Creating a UserCheck Interaction Object

If the default UserCheck messages do not fit your needs, you can create a UserCheck Interaction object.

To create a UserCheck object that includes a message:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Click **Access Tools** > **UserCheck**.
3. Click **New**, and select one of these interaction modes:
    - **AskUserCheck** - Show a message to users that asks them if they want to continue with the request or not.
    - **Block UserCheck** - Show a message to users and block the application request.

- **Inform UserCheck** - Show an informative message to users. Users can continue to the application or cancel the request.

The **UserCheck Interaction** window opens on the **Message** page.

4. Enter a name for the UserCheck object and, optionally, a comment.
5. Select a language (English is the default) from the **Languages** tabs.
6. Enter the message content. You can:
   - Use the formatting toolbar to change text color, alignment, add or remove bullets.
   - Use the **Insert field** variables. These include fields for Content Awareness.

     Example Message with Content Awareness field

     If you define a custom UserCheck message, you can use predefined **Field** variables in the message.

     Here is an example of a UserCheck message that you can define. This example uses some of the **Insert Field** variables for Application Control and Content Awareness rules:

     ```
     According to the company policy, this action is intended
     for work-related use only.
                    Details:
                    - File Name is classified as Data Types
                    - Access to Application name
                    - Category Category
     [ ] I will use this site/application and data in
     accordance with company policy.
     Reference: Incident ID
     ```

7. In the **Settings** tab, configure optional settings. For example:
   - **Fallback Action** - For a *Block* action type, when UserCheck notification cannot be displayed, this action is taken.
   - **External Portal** - When selected, redirects the user to the specified **External Portal** (enter the URL), and the UserCheck message is not shown to the end-user Select **Add UserCheck Incident ID to the URL query**, to log the incident
8. Click **OK**.

   This creates the UserCheck object and web page notification for the portal.

Example UserCheck Message Using Field Variables

If you define a custom UserCheck message, you can use predefined **Field** variables in the message.

Here is an example of a UserCheck message that you can define. This example uses some of the **Insert Field** variables for Application Control and Content Awareness rules:

```
According to the company policy, this action is intended for work-
related use only.
               Details:
               - File Name is classified as Data Types
               - Access to Application name
               - Category Category
[ ] I will use this site/application and data in accordance with
company policy.
Reference: Incident ID
```

Localizing and Customizing the UserCheck Portal

After you set the UserCheck interaction object language, you can translate the Portal **OK** and **Cancel** buttons to the applicable language. For more information, see sk83700.

Some of the UserCheck predefined notifications are translated to more than one language. For example, **Access Notification** is translated to English, French, Spanish, and Japanese.

To support more languages:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Click **Access Tools** > **UserCheck**.
3. Double-click the UserCheck object to edit it.
4. In the **Message** page, click **Languages**.
5. Select the **Languages** from the list.

UserCheck Frequency and Scope

You can set the number of times that users get UserCheck messages for accessing applications that are not permitted by the policy. You can also set if the notifications are based on accessing the rule, application category, or application itself.

To set how often UserCheck notifications show :

1. Select the **Action** cell of a rule in the Access Control **Policy**, and click **More**.
2. In the **Action Settings** window, select the **UserCheck Frequency**.

   The options are:

   - **Once a day**
   - **Once a week**

- **Once a month**
- **Custom frequency**

3. Select **Confirm UserCheck**.

   Possible notifications are:

   - **Per rule**
   - **Per category**
   - **Per application**
   - **Per data type**

Example:

In a rule that contains:

Services & Applications	Action
Social Networking category	Inform

If you select a **UserCheck Frequency** of **Once a day**, and **Confirm UserCheck** of **Per rule**:

A user who accesses Facebook and then LinkedIn on the same day gets one **Inform** message.

If you select a **UserCheck Frequency** of **Once a day**, and **Confirm UserCheck** of **Per application**:

A user who accesses Facebook and then LinkedIn on the same day gets one **Inform** message for Facebook and one for LinkedIn.

In new installations, the **Confirm UserCheck Scope** default is **Per category**.

In upgrades from a version before R75.40, the **Confirm UserCheck** default is **Per Rule**.

UserCheck Settings

For each UserCheck interaction object you can configure these options from the **Settings** page UserCheck object:

- **Languages** - Set a language for the UserCheck message if the language setting in the user browser cannot be determined or is not implemented. For example:

  - If the browser native language is Spanish
  - The UserCheck message is in Japanese and French
  - You select Japanese as the default language

  Then the notification displays in Japanese.

- **Fallback Action** (For Action Types **Ask** and **Inform**) - Select an alternative action (allow or block) for when the UserCheck notification cannot be shown in the browser or application that caused the notification. If UserCheck determines that the notification cannot be shown in the browser or application, the behavior is:
  - If the **Fallback Action** is **Allow** (the default for Inform messages), the user is allowed to access the website or application, and the UserCheck client (if installed) shows the notification.
  - If the **Fallback Action** is **Block**, the gateway tries to show the notification in the application that caused the notification. If it cannot and the UserCheck client is installed, it shows the notification through the client. The website or application is blocked, even if the user does not see the notification.
- **External Portal - Redirect the user to External Portal** - Select this to redirect users to an external portal, not on the gateway.
  - **URL** - Enter the URL for the external portal. The specified URL can be an external system that obtains authentication credentials from the user, such as a user name or password. It sends this information to the gateway.
  - **Add UserCheck Incident ID to the URL query** - An incident ID is added to the end of the URL query.
- **Conditions** (For the Action Type **Ask**) - Select actions that must occur before users can access the application. Select one or more of these options:
  - **User accepted and selected the confirm checkbox** - This applies if the UserCheck message contains a checkbox (**Insert User Input** > **Confirm Checkbox**). Users must accept the text shown and select the checkbox before they can access the application.
  - **User filled some textual input** - This applies if the UserCheck message contains a text field (**Insert User Input** > **Textual Input**). Users must enter text in the text field before they can access the application. For example, you might require that users enter an explanation for use of the application.

UserCheck CLI

See the *R81.10 CLI Reference Guide* - Chapter *Security Gateway Commands* - Section *usrchk*.

Revoking Incidents

The Revoke Incidents URL can revoke a user's responses to UserCheck notifications. The URL is:

https://<IP Address of Security Gateway>/UserCheck/RevokePage

If users regret their responses to a notification and contact their administrator, the administrator can send users the URL.

After a user goes to the URL, all of the user's responses to notifications are revoked. The logs in the SmartConsole **Logs & Monitor** view **Logs** tab will show the user's activity, and that the actions were revoked afterwards.

Administrators can use the `usrchk` command of the CLI to revoke incidents for one user, all users, or a specified interaction object.

UserCheck Client

The UserCheck client is installed on endpoint computers to communicate with the gateway and show UserCheck interaction notifications to users.

It works with the **Data Loss Prevention** and **Content Awareness** Software Blades.

Notifications of incidents can be sent by email (for SMTP traffic) or shown in a popup from the UserCheck client in the system tray (for SMTP, HTTP and FTP).

UserCheck client adds the option to send notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck client can also work together with the UserCheck portal to show notifications on the computer itself when:

- The notification cannot be displayed in a browser, or
- The UserCheck engine determines that the notification will not be shown correctly in the browser.

Users select an option in the notification message to respond in real-time.

For Data Loss Prevention (DLP), administrators with full permissions or the View/Release/Discard DLP messages permission can also send or discard incidents from the SmartConsole **Logs & Monitor** > **Logs** view.

Workflow for installing and configuring UserCheck clients:

1. Configure how the clients communicate with the gateway and create trust with it.
2. Enable UserCheck and the UserCheck client on the gateway.
3. Download the UserCheck client MSI file.
4. Install the UserCheck client on the endpoint computers.
5. Make sure that the UserCheck clients can connect to the gateway and receive notifications.

UserCheck Requirements

See *UserCheck Client Requirements* in the *R81.10 Release Notes*.

Enabling UserCheck Client

Enable UserCheck and the UserCheck client on the gateway in the Properties window of the gateway object in SmartConsole. This is necessary to let clients communicate with the gateway.

To enable UserCheck and the UserCheck client on the gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **UserCheck**.
3. Select **Enable UserCheck for active blades**.

   This enables UserCheck notifications from the gateway.
4. In the **UserCheck Client** section, select **Activate UserCheck Client support**.

   This enables UserCheck notifications from the client.
5. Click **OK** and **Install Policy**.

Getting the MSI File

To get the MSI file:

1. In SmartConsole, in the **Gateways & Servers** view, open the **General Properties** window of the Security Gateway object.
2. From the navigation tree, select **UserCheck**.
3. In the **UserCheck Client** section, click **Download Client**.

   Important - Before you can download the client MSI file, the portal must be up. The portal is up only after a installation.

Distributing and Connecting Clients

After configuring the clients to connect to the gateway, install the clients on the user machines. You can use any method of MSI or EXE mass deployment and installation that you choose. For example, you can send users an email with a link to install the client. When a user clicks the link, the MSI file automatically installs the client on the computer.

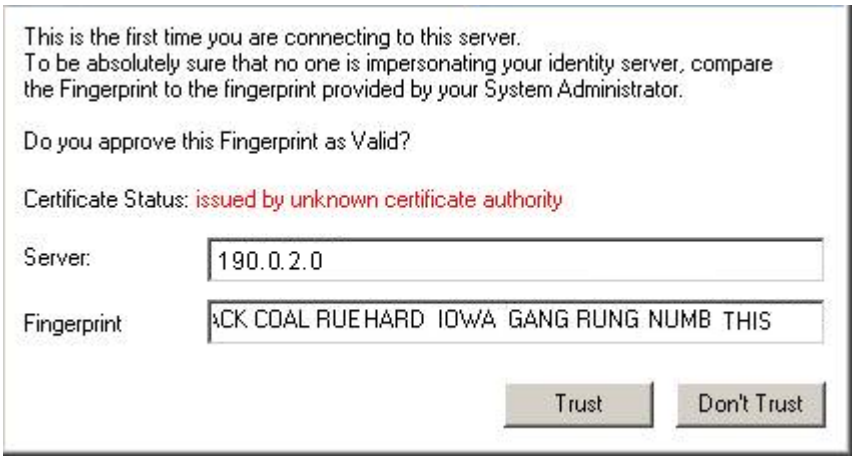
Alternatively, users can download the installation package from the regular DLP UserCheck notifications.

To install the client for all user accounts on a Windows computer, see sk96107.

The installation is silent and generally, no reboot is required.

When the client is first installed, the tray icon indicates that it is not connected. When the client connects to the gateway, the tray icon shows that the client is active.

The first time that the client connects to the gateway, it asks for verification from the user and approval of the fingerprint.



Best Practices:

- Let the users know this will happen.
- Use a server certificate that is trusted by the certificate authority installed on users' computers. Then users do **not** see a message that says: **Issued by unknown certificate authority**.

If UserCheck for DLP is enabled on the gateway, users are required to enter their username and password after the client installs.

Example of message to users about the UserCheck client installation (for DLP):

```
Dear Users,
Our company has implemented a Data Loss Prevention automation to
protect our confidential data from unintentional leakage. Soon you
will be asked to verify the connection between a small client that
we will install on your computer and the computer that will send
you notifications.
This client will pop up notifications if you try to send a message
that contains protected data. It might let you to send the data
anyway, if you are sure that it does not violate our data-security
guidelines.
When the client is installed, you will see a window that asks if
you trust the DLP server. Check that the server is SERVER NAME and
then click Trust.
In the next window, enter your username and password, and then
click OK.
```

Note - If the UserCheck client is not connected to the gateway, the behavior is as if the client was never installed. Email notifications are sent for SMTP incidents and the Portal is used for HTTP incidents

UserCheck and Check Point Password Authentication

You can see and edit Check Point users from **Users and Administrators** in the navigation tree.

To enable Check Point password authentication:

SmartConsole Configuration

1. Open SmartConsole and open the **Manage & Settings** view.
2. Click **Permissions & Administrators** > **Administrators**, and select an existing user or create a new user.
3. In the **General Properties** page of the user, make sure that an email address is defined.
4. In the **Authentication Properties** page of the user, set **Authentication Scheme** to **Check Point Password** and enter the password and password confirmation.
5. Click **OK**.

UserCheck Client Configuration

Ask your users to configure their UserCheck client:

1. On the UserCheck client computer, right-click the UserCheck icon in the Notification Area (next to the system clock).
2. Select **Settings**.
3. Click **Advanced**.
4. Select **Authentication with** Check Point user accounts defined internally in **SmartConsole**.

Helping Users

If users require assistance to troubleshoot issues with the UserCheck client, you can ask them to send you the logs.

To configure the client to generate logs:

1. Right-click the UserCheck tray icon and select **Settings**.

   The **Settings** window opens.
2. Click **Log to** and browse to a pathname where the logs are saved.
3. Click **OK**.

To send UserCheck logs from the client:

1. Right-click the UserCheck tray icon and select **Status**.

   The **Status** window opens.

2. Click **Advanced** and then click the **Collect information for technical support** link.

   The default email client opens, with an archive of the collected logs attached.

UserCheck for Access Control Default Messages

These are the default UserCheck messages in the **Access Tools** > **UserCheck** page of the Access Control Policy:

Name	Action Type	Description
Access Approval	Inform	
Access Notification	Inform	Shows when the action for the rule is inform. It informs users what the company policy is for that site.
Blocked Message - Access Control	Block	Shows when the action for the rule is Block, when a request is blocked.
Cancel Page - Access Control	Cancel	Shows after a user gets an Inform or Ask message and clicks Cancel.
Company Policy	Ask	Shows when the action for the rule is **ask**. It informs users what the company policy is for that site and they must click **OK** to continue to the site.

If the default UserCheck messages do not fit your needs, you can create a UserCheck Interaction object.

For example, you can create a message with Content Awareness fields.

If you define a custom UserCheck message, you can use predefined **Field** variables in the message.

Here is an example of a UserCheck message that you can define. This example uses some of the **Insert Field** variables for Application Control and Content Awareness rules:

```
According to the company policy, this action is intended for work-
related use only.
                Details:
                - File Name is classified as Data Types
                - Access to Application name
                - Category Category
[ ] I will use this site/application and data in accordance with
company policy.
Reference: Incident ID
```

You can show these UserCheck message previews:

- **Regular view** - Shows a preview of the UserCheck message on a computer.
- **Mobile** - Shows a preview of the UserCheck message on a mobile device.
- **Agent** - Shows a preview of the UserCheck message in the agent window.
- **Email** - Shows a preview of the UserCheck message in an email.

Application and URL Filtering UserCheck Page

Ask and **Inform** pages include a **Cancel** button that users can click to cancel the request.

For Threat Prevention and Application and URL Filtering , you can show these UserCheck message previews:

- **Regular view** - Shows a preview of the UserCheck message on a computer.
- **Mobile Device** - Shows a preview of the UserCheck message on a mobile device.

For DLP, you can also show these UserCheck message previews:

- **Email** - Shows a preview of the UserCheck message in an email.
- **Agent** - Shows a preview of the UserCheck message in the DLP agent window.

Localizing and Customizing the UserCheck Portal

After you set the UserCheck interaction object language, you can translate the Portal **OK** and **Cancel** buttons to the applicable language. For more information, see sk83700.

Some of the UserCheck predefined notifications are translated to more than one language. For example, **Access Notification** is translated to English, French, Spanish, and Japanese.

To support more languages:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Click **Access Tools** > **UserCheck**.
3. Double-click the UserCheck object to edit it.

4. In the **Message** page, click **Languages**.
5. Select the **Languages** from the list.

UserCheck - Message

What can I do here?

For DLP, Threat Prevention and Application Control: Edit or create a UserCheck object to create a custom message for users.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > UserCheck New > Ask/Block/Inform > Message
Or:
Menu > Object Explorer > New > UserCheck > Ask > Message

Creating a UserCheck Interaction Object

If the default UserCheck messages do not fit your needs, you can create a UserCheck Interaction object.

To create a UserCheck object that includes a message:

1. In the **Security Policies** view of SmartConsole, go to the **Access Control Policy**.
2. Click **Access Tools** > **UserCheck**.
3. Click **New**, and select one of these interaction modes:
   - **Ask UserCheck** - Show a message to users that asks them if they want to continue with the request or not.
   - **Block UserCheck** - Show a message to users and block the application request.
   - **Inform UserCheck** - Show an informative message to users. Users can continue to the application or cancel the request.

   The **UserCheck Interaction** window opens on the **Message** page.
4. Enter a name for the UserCheck object and, optionally, a comment.
5. Select a language (English is the default) from the **Languages** tabs.
6. Enter the message content. You can:

- Use the formatting toolbar to change text color, alignment, add or remove bullets.
- Use the **Insert field** variables. These include fields for Content Awareness.

  If you define a custom UserCheck message, you can use predefined **Field** variables in the message.

  Here is an example of a UserCheck message that you can define. This example uses some of the **Insert Field** variables for Application Control and Content Awareness rules:

```
According to the company policy, this action is intended
for work-related use only.
               Details:
               - File Name is classified as Data Types
               - Access to Application name
               - Category Category
[ ] I will use this site/application and data in
accordance with company policy.
Reference: Incident ID
```

7. In the **Settings** tab, configure optional settings. For example:
   - **Fallback Action** - For a *Block* action type, when UserCheck notification cannot be displayed, this action is taken.
   - **External Portal** - When selected, redirects the user to the specified **External Portal** (enter the URL), and the UserCheck message is not shown to the end-user.

     Select **Add UserCheck Incident ID to the URL query**, to log the incident.
8. Click **OK**.

   This creates the UserCheck object and web page notification for the portal.

UserCheck - settings

What can I do here?

Use this window to configure browser language, fallback action, conditions under which user data is sent, and external portal redirect.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > UserCheck New > Ask/Block/Inform > Settings
Or:
Menu > Object Explorer > New > UserCheck > Ask > Settings

UserCheck Setting Options

- **Languages**

  Set a language for the UserCheck message if the language setting in the user's browser cannot be determined. For example:

  - If the browser native language is Spanish
  - The UserCheck message is in Japanese and French
  - You select Japanese as the default language

  Then the notification displays in Japanese.

- **Fallback Action**

  Select an alternative action (**Accept** or **Drop**) for when the UserCheck notification cannot be shown in the browser or application that caused the notification. If UserCheck determines that the notification cannot be shown in the browser or application:

  - An **Accept** fallback action (the default for Inform messages) lets the user access the website or application, and the UserCheck client (if installed) shows the notification.
  - A **Drop** fallback action configures the gateway to show the notification in the application that caused the notification. If the gateway cannot, and the UserCheck client is installed, the notification shows in the client. The website or application is blocked, even if the user does not see the notification.

- **Conditions**

  User accepted and selected the confirm checkbox - This applies if the UserCheck message contains a checkbox. Users must accept the text shown and select the checkbox before they can access the application.

  User filled some textual input - This applies if the UserCheck message contains a text field. Users must enter text in the text field before they can access the application. For example, you might require that users enter an explanation for use of the application.

- **External Portal**

  - **Redirect to External Portal** -Select this to redirect users to an external portal, not on the gateway.
  - **URL** -Enter the URL for the external portal. The specified URL can be an external system that obtains authentication credentials from the user, such as a user name or password. It sends this information to the gateway.

- **Add UserCheck Incident ID to the URL query**

  An incident ID is added to the end of the URL query.

- **Confirmation sent to the gateway**

  The URL template field points to an XML file. This file should be placed on the external portal so that it can be sent back to the Security Gateway.

  The pre-shared secret authenticates the external portal to the Security Gateway.

Anti-Bot

What can I do here?

Use this window to configure UserCheck settings and suspicious mail detection settings for Anti-bot.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Anti-bot

Configuring Anti-Bot Settings

Here you can configure the Anti-Bot **UserCheck Settings**:

- **Prevent** - Select the UserCheck message that opens for a **Prevent** action
- **Ask** - Select the UserCheck message that opens for an **Ask** action

Blocking Bots

To block bots in your organization, install this default Threat Policy rule that uses the **Optimized** profile, or create a new rule.

Protected Scope	Action	Track	Install On
*Any	**Optimized**	Log Packet Capture	*Policy Targets

To block bots in your organization:

1. In SmartConsole, click **Gateways & Servers**.
2. Enable the **Anti-Bot** Software Blade on the Gateways that protect your organization. For each Gateway:

a. Double-click the Gateway object.

b. In the **Gateway Properties** page, select the **Anti-Bot** Software Blade.

The First Time **Activation** window opens.

c. Select **According to the Anti-Bot and Anti-Virus policy**.

d. Click **OK**.

3. Click **Security Policies** > **Threat Prevention** > **Policy** > **Threat Prevention**.

You can block bots with the out-of-the-box Threat Prevention policy rule with the default **Optimized** Profile.

Alternatively, add a new Threat Prevention rule:

a. Click **Add Rule**.

A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.

b. Make a rule that includes these components:

- **Name** - Give the rule a name such as **Block Bot Activity**.
- **Protected Scope** -The list of network objects you want to protect. By default, the **Any** network object is used.
- **Action** - The Profile that contains the protection settings you want. The default profile is **Optimized**.
- **Track** - The type of log you want to get when the gateway detects malware on this scope.
- **Install On** - Keep it as **Policy Targets** or select Gateways, on which to install the rule.

4. Install the Threat Prevention policy.

The IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction Software Blades have a dedicated Threat Prevention policy. You can install this policy separately from the policy installation of the Access Control Software Blades. Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways.

To install the Threat Prevention policy:

a. From the Global toolbar, click **Install Policy**.

The **Install Policy** window opens showing the installation targets (Security Gateways).

b. Select **Threat Prevention**.

c. Select **Install Mode:**

- **Install on each selected gateway independently** - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.

  If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.

- **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.

d. Click **OK**.

Monitoring Bot Activity

Scenario: I want to monitor bot activity in my organization without blocking traffic at all. How can I do this?

In this example, you will create this Threat Prevention rule, and install the Threat Prevention policy:

Name	Protected Scope	Action	Track	Install On
Monitor Bot activity	`*Any`	A profile that has **these** changes relative to the **Optimized** profile: Go to the **General Policy** pane > **Activation Mode** section, and set all **Confidence** levels to **Detect**.	`Log`	`*Policy Targets`

To monitor all bot activity:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. Create a new profile:
   a. From the **Custom Policy Tools** section, click **Profiles**.

      The **Profiles** page opens.

   b. Right-click a profile and select **Clone**.

c. Give the profile a name such as **Monitoring_Profile**.

d. Edit the profile, and under **Activation Mode**, configure all confidence level settings to **Detect**.

e. Select the **Performance Impact** - for example, **Medium or lower**.

This profile detects protections that are identified as an attack with low, medium or high confidence and have a medium or lower performance impact.

3. Create a new rule:

a. Click **Threat Prevention** > **Policy** > **Threat Prevention**.

b. Add a rule to the Rule Base.

The first rule that matches is applied.

c. Make a rule that includes these components:

- **Name** - Give the rule a name such as **Monitor Bot Activity**.
- **Protected Scope** -Keep **Any** so the rule applies to all traffic in the organization.
- **Action** - Right-click in this cell and select **Monitoring_Profile**.
- **Track** - Keep **Log**.
- **Install On** - Keep it as **Policy Targets** or choose Gateways, on which to install the rule.

4. Install the Threat Prevention policy.

The IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction Software Blades have a dedicated Threat Prevention policy. You can install this policy separately from the policy installation of the Access Control Software Blades. Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways.

To install the Threat Prevention policy:

a. From the Global toolbar, click **Install Policy**.

The **Install Policy** window opens showing the installation targets (Security Gateways).

b. Select **Threat Prevention**.

c. Select **Install Mode:**

- **Install on each selected gateway independently** - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.

  If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.

- **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.

d. Click **OK**.

Updates - Access Policy

What can I do here?

Use this window to update packages related to the Access policy.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > Updates

Application Control & URL Filtering

You can schedule an update or update now. Update now has three options:

- Update now
- Offline update
- Import applications

More Details - Threat Policy

What can I do here?

Use this window to see which gateways do not have updated Anti-Bot, Anti-Virus or Threat Emulation protections.

Getting Here - SmartConsole > Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > IPS > More details...(3 links)

Installation History

What can I do here?

Use this window to view the history of managed network objects.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > Installation History

Policy Installation History

In the Installation History you can choose a Gateway, a date and time when the Policy was installed, and:

- See the revisions that were installed on the Gateway and who installed the Policy.
- See the changes that were installed and who made the changes.
- Revert to a specific version, and install the last "good" Policy.

To work with the Policy installation history:

1. In SmartConsole, go to **Security Policies**.
2. From the **Access Tools** or the **Threat Prevention Tools**, select **Installation History**.
3. In the **Gateways** section, select a Gateway.
4. In the **Policy Installation History** section, select an installation date.
5. **To see the revisions that were installed and who made them**:

   Click **View installed changes**.

   To see the changes that were installed and who made them :

   Click **View**.

   To revert to a specific version of the Policy:

   Click **Install specific version**.

Updates - Status and Details

What can I do here?

Use this window to see the details and status of the update.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > Updates > Update Now > Details link in task window

Schedule Update

What can I do here?

Use this window to enable a scheduled update.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > Updates > Schedule Update

Updating the Application and URL Filtering Database

The Application and URL Filtering Database on the Security Gateway gets regular, automatic updates that make sure that you have the most current data and newly added applications and websites in the Application and URL Filtering Layer of the Access Control Policy.

By default, updates run on the Security Management Server and Security Gateways once a day. You can change the update schedule or choose to manually update the management server. The updates are stored in a few files on each Security Gateway.

To manually update the Application and URL Filtering Database on the management server:

1. In SmartConsole, click **Security Policies** > **Access Tools** > **Updates**.
2. In the **Application and URL Filtering** section, click **Update Now**.

To change the schedule for Application and URL Filtering Database updates on the management server:

1. In SmartConsole, click **Security Policies** > **Access Tools** > **Updates**.
2. Click **Schedule Update**.
3. Select **Enable Application Control & URL Filtering Scheduled Update**.
4. Click **Configure** to schedule when the updates will run. By default, a scheduled update runs once a day.

In Multi-Domain Security Management, update the database for all Domain Management Servers in the Global SmartConsole and not from Domain Management Servers.

Connecting to the Internet for Updates

The gateway or Security Management Server connects to the Internet to get the Application and URL Filtering Database updates. To make sure that it can get the updates successfully:

- Make sure that there is a DNS server configured.
- Make sure a proxy is configured for each gateway and the Security Management Server, if necessary.

Security Policies > **Access Tools** > **Updates** shows if the Security Management Server uses a proxy to connect to the Internet.

To configure a proxy for the Security Management Server:

1. Select **Security Policies** > **Access Tools** > **Updates**.
2. Click **Configure Proxy**.
3. In the **Proxy Configuration** window, in the **Use proxy** field, enter the domain name or IP address of the proxy, and the **Port** number.

To Configure IPv6 proxy support:

If the proxy uses an IPv6 address:

1. On the Windows computer, running SmartConsole client, go to **Start** menu and open **Control Panel > System and Security > System > Advanced System Settings**.
2. Open the **Advanced** tab > **Environment variables**.
3. Create a new **User Variable**.
4. Set the value to: `updates_over_IPv6=1`

Scheduling Updates

To change the update schedule from the default scheduled Application and URL Filtering Database updates:

1. Select **Security Policies** > **Access Control** > **Access Tools** > **Updates**.
2. Click **Schedule Update**.
3. Select the target for updates:
   - **Security Management Server**
   - **Security Gateway**
4. Click **Configure**.

   Configure the Security Management Server updates and the Security Gateway updates separately.
5. Set the **Time of Event**. Set the update interval, and a time of day for updates to occur.
6. Click **OK**.

If you have Security Gateways or Security Management Servers in different time zones, they will not be synchronized until all of them are updated.

Scheduled Update

What can I do here?

Use this window to schedule the update.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > Updates > Application and URL Filtering > Schedule Update > Security Management Server > Configure
Or:
SmartConsole > Security Policies > Threat Prevention > Custom Policy Tools > Updates > IPS > Scheduled Update > Configure (top button in window)

Schedule Update - Security Management Server - Configure

Use this window to schedule the package update.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > Updates > Application and URL Filtering > Schedule update > Security Management Server > Configure

Scheduled Update - Security Gateway - Configure

What can I do here?

Use this window to schedule the package update.

Getting Here - SmartConsole > Security Policies > Access Control > Policy > Access Tools > Updates > Application and URL Filtering > Schedule update > Security Gateway > Configure

Profiles

What can I do here?

Use this window to create and edit profiles.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles

Optimized Protection Profile Settings

The **Optimized** profile is activated by default, because it gives excellent security with good gateway performance.

These are the goals of the **Optimized** profile, and the settings that achieve those goals:

Goal	Parameter	Setting
Apply settings to all the Threat Prevention Software Blades	**Blades Activation**	Activate the profile for IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction.
Do not have a critical effect on performance	**Performance impact**	Activate protections that have a *Medium or lower* effect on performance.
Protect against important threats	**Severity**	Protect against threats with a severity of *Medium or above*.
Reduce false-positives	**Confidence**	Set to *Prevent* the protections with an attack *confidence* of *Medium* or *High*. Set to *Detect* the protections with a confidence of *Low*.

Profiles Pane

The pane shows a list of profiles that have been created, their confidence levels, and performance impact settings. The Profiles pane contains these options:

Option	Meaning
New	Creates a new profile.
View	Shows an existing profile.
Edit	Modifies an existing profile.
Clone	Creates a copy of an existing profile.
Delete	Deletes a profile.
Where Used	Shows you reference information for the profile.
Search	Searches for a profile.
Last Modified	Shows who last modified the selected profile, when and on which client.

Performance Impact

Performance impact is how much a protection affects the gateway performance. Some activated protections might cause issues with connectivity or performance. You can set protections to not be prevented or detected if they have a higher impact on gateway performance.

There are three options:

- High or lower
- Medium or lower
- Low

Severity

Severity of the threat. Probable damage of a successful attack to your environment.

There are three degrees of severity:

- Low or above
- Medium or above
- High or above

Activation Settings

- **Prevent** - The protection action that blocks identified virus or bot traffic from passing through the gateway. It also logs the traffic, or tracks it, according to configured settings in the Rule Base.
- **Detect** - The protection action that allows identified virus or bot traffic to pass through the gateway. It logs the traffic, or tracks it, according to configured settings in the Rule Base.
- **Inactive** - The protection action that deactivates a protection.

Confidence Level

The confidence level is how confident the Software Blade is that recognized attacks are actually virus or bot traffic. Some attack types are more subtle than others and legitimate traffic can sometimes be mistakenly recognized as a threat. The confidence level value shows how well protections can correctly recognize a specified attack.

Creating Profiles

You can choose from multiple pre-configured Profiles, but not change them. You can create a new profile or clone a profile. When you create a new profile, it includes all the Threat Prevention Software Blades by default.

When HTTPS inspection is enabled on the Security Gateway, Threat Emulation, Anti-Bot, and Anti-Virus can analyze the applicable HTTPS traffic.

To create a new Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Custom Policy Tools** section, click **Profiles**.

   The **Profiles** page opens.
3. Right-click a profile and select **New**.
4. Configure the settings for the profile.
5. Click **OK**.
6. Install the Threat Prevention policy.

Cloning Profiles

You can create a clone of a selected profile and then make changes. You cannot change the out-of-the-box profiles: **Basic**, **Optimized**, and **Strict**.

To clone a Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Custom Policy Tools** section, click **Profiles**.

   The **Profiles** page opens.
3. Right-click the profile and select **Clone**.
4. The **Name** field shows the name of the copied profile plus **_copy**.
5. Rename the profile.
6. Click **OK**.
7. Publish the SmartConsole session.

Editing Profiles

You can change the settings of the Threat Prevention profile according to your requirements.

To edit a profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Custom Policy Tools** section, click **Profiles**.

The **Profiles** page opens.

3. Right-click the profile and select **Edit**.

Deleting Threat Prevention Profiles

You can delete a profile, but you cannot delete the default Threat Prevention profiles.

To delete a profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Custom Policy Tools** section, click **Profiles**.

   The **Profiles** page opens.
3. Right-click the profile, and click **Delete**.

   A window opens and shows a confirmation message.
4. Click **Yes**.

   If the profile is used by another object, you cannot delete it. The error message is shown in the Tasks window.
5. In SmartConsole, install the policy.

To show the objects that use a profile:

1. From the **Profiles** page, select the profile.

   The Summary
2. From the **Where Used** section in the **Summary** tab, click **Where Used**.

   The **Where Used** window opens and shows the profile.
3. Right-click the rule and select **View in policy**.

Showing Changes to a Threat Prevention Profile

You can show the Audit log and see changes that were made to a Threat Prevention profile.

To show the Audit log for a Threat Prevention profile:

1. In SmartConsole, click Logs & Monitor.
2. Click the **Audit** tab, or press **CTRL + T** and click **Open Audit Logs View**.
3. In **Enter search query**, enter the name of the profile.
4. To refine the search:

a. Right-click the **Object Type** column heading and select **Add Filter**.

b. Enter **Threat Prevention Profile**.

c. Click the filter to add it to the search.

d. Click **OK**.

The search results are filtered to Threat Prevention profiles.

5. To see more information about the changes to a profile, double-click the Audit log.

New Threat Profile - Task Details

What can I do here?

Use this window to see the status of the profile creation operation.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > New profile > Task window > Details

Profile - General Policy

What can I do here?

Use this window to activate Threat Prevention blades, active protection, and activation modes.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > General Policy

Introducing Profiles

Check Point Threat Prevention provides instant protection based on pre-defined Threat Prevention **Profiles** . You can also configure a custom Threat Prevention profile to give the exact level of protection that the organization needs.

When you install a Threat Prevention policy on the Security Gateways, they immediately begin to enforce IPS protection on network traffic.

A Threat Prevention profile determines which protections are activated, and which Software Blades are enabled for the specified rule or policy. The protections that the profile activates depend on the:

- Performance impact of the protection.
- Severity of the threat.
- Confidence that a protection can correctly identify an attack.
- Settings that are specific to the Software Blade.

A Threat Prevention profile applies to one or more of the Threat Prevention Software Blades: IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction.

A *profile* is a set of configurations based on:

- *Activation settings* (prevent, detect, or inactive) for each *confidence level* of protections that the ThreatSpect engine analyzes
- IPS Settings
- Anti-Bot Settings
- Anti-Virus Settings
- Threat Emulation Settings
- Threat Extraction Settings
- Indicator configuration
- Malware DNS Trap configuration
- Links inside mail configuration

Without profiles, it would be necessary to configure separate rules for different activation settings and confidence levels. With profiles, you get customization and efficiency.

SmartConsole includes these default Threat Prevention profiles:

- **Optimized** - Provides excellent protection for common network products and protocols against recent or popular attacks
- **Strict** - Provides a wide coverage for all products and protocols, with impact on network performance
- **Basic** - Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance

Profile - Mail Settings

What can I do here?

Use this window to create a policy for malicious email on MTA gateways.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Mail > General

General

General

- **Emulate emails for malicious content (requires Threat Emulation)** - When this option and the Threat Emulation blade are enabled, the Threat Emulation blade scans SMTP traffic.
- **Scan emails for viruses (requires Anti-Virus)** - When this option and the Anti-Virus blade are enabled, the Anti-Virus blade scans SMTP traffic.
- **Extract potentially malicious attachments (requires Threat Extraction)** - When this option and the Threat Extraction blade are enabled, the Threat Extraction blade scans SMTP traffic.
- **Enable MTA Live Monitoring** - Shows the current status of the email traffic which passed through the MTA in the selected time frame.

Malicious Email Policy on MTA Gateways

In this section you can decide whether to block or allow an email which was found malicious.

If you allow the email, you can select any or all of these options:

- **Remove attachments and links** - This option is selected by default. You can replace a link or an attachment found malicious with a neutralized version of the links and attachments. The neutralized email version is sent to the recipient with a customizable template. Click **Configure** to edit the template:
  - **Malicious Attachments** - Replaced by a neutralized txt file. You can customize the message which the user receives. Click **Insert Field** to add more file-related information to your message (for example: file name or MD5 hash).
  - **Failed to Scan Attachments** - If the scanning of the attachment fails and fail mode is set to fail-close, the attachment is replaced with a txt attachment. If fail mode is set to fail-open, the original attachment is allowed. Click **Insert Field** to add more file-related information to your message (for example: file name or MD5 hash).
  - **Malicious Links** - Replaced by a neutralized link. Click **Insert Field** to add more link-related information to your message, for example, neutralized url.
- **Add an X-Header to the email** - Tag the email found malicious with an X-Header. The X-Header format is: "X-Check Point-verdict: <*verdict*>; *confidence: <confidence>*". For example: "X-Check Point-verdict: malicious; confidence: high". With this option, you can configure the MTA Next Hop to quarantine all emails with a specific X-Header.
- **Add a prefix to the email subject** - Adds a prefix to the subject of an email found malicious. For example: you can add a warning message that the email is malicious. Click **Configure** to edit the prefix.
- **Add customized text to the email body** - This option adds a section at the beginning of the email body, based on a customizable template, with an optional placeholder for the verdicts of the links and attachments found malicious or failed to be scanned. The links are given in their neutralized versions, and attachments are only given by file names. Click **Configure** to edit the template.

Send a copy to the following list - This option is available both if you allow or block the malicious email. With this option, the original email (with the malicious attachments and links) is attached to a new email, which contains: the verdict list with the neutralized links and attachment file names, and the SMTP envelope information. You can configure the email content on the gateway. You can use this option for research purposes. For example: The Incident Response Team needs to inquire the emails received in the organization for improved security and protection.

MIME Nesting

This is an optional configuration. In this section, you can configure the maximum number of MIME nesting levels to be scanned (A nesting level is an email within an email). These settings are the same for Anti-Virus, Threat Emulation and Threat Extraction.

- **Maximum MIME nesting is (levels)** - Set the maximum number of levels in the email which the engine scans.
- **When nesting level is exceeded (action on file)** - If there are more MIME nested levels than the configured amount, select to **Block** or **Allow** the email.

Attachment Configuration

What can I do here?

Use this window to configure a custom message for emails that have had attachments and links removed.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Mail > General > Remove attachments and links > Configure

Mail Subject Prefix Configuration

What can I do here?

Use this window to add a prefix to the mail subject.

Getting Here -Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > General > Malicious Email Policy on MTA Gateways > Add a prefix to the email subject

Configuring the Mail Subject

If you select to allow the original email, you can click **Configure Mail Subject** to add a message which warns not to open the email.

Best Practice - If an attachment is found to be malicious, we recommend not to open the original email.

Email Body Configuration

What can I do here?

Use this window to create custom text in the body of an email.

See also: *"Profile - Mail Settings" on page 324*

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Mail > General > Add customized text to the email body > Configure

Exceptions

What can I do here?

Use this window to configure exceptions to Threat Emulation and Threat Extraction.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Mail > Exceptions

Configuring Exceptions

You can exclude specific email addresses from the Threat Emulation or Threat Extraction protections.

To exclude emails from Threat Emulation:

1. In **Emulation Exceptions**, click **Configure**.
2. In the **Recipients** section, click the **+** button to enter one or more emails.

   Emails and attachments that are sent to these recipients will not be sent for emulation.
3. In the **Senders** section, click the **+** button to enter one or more emails.

   Emails and attachments that are received from these senders will not be sent for emulation.

   Note - You can use a wildcard character to exclude more than one email address from a domain.
4. Click **OK**.

Note - If you want to do emulation on outgoing emails, make sure that you set the Protected Scope to **Inspect incoming and outgoing files**.

To exclude emails from Threat Extraction:

1. In **Extraction Exclusion/Inclusion**:
   - Select **Scan all emails** (selected by default) and click **Exceptions**.

     Click the **+** button to exclude specific recipients, users, groups or senders.
   - Select **Scan mail only for specific users or groups** and click **Configure**.

     Click the Add button to exclude specific User Groups, Recipients or Senders.
2. Click **OK**.

Examples:

A *user* is an object that can contain an email address with other details.

A *group* is an AD group or an LDAP group of users

A *recipient* is an email address only.

Important : In the main SmartConsole menu > **Global Properties** > **User Directory**, make sure that you selected **Use User Directory for Security Gateways**.

Signed Email Attachments

Signed emails are not encrypted, but the mail contents are *signed* to authenticate the sender. If the received email differs from the email that was sent, the recipient gets a warning, and the digital signature is no longer valid.

Clean replaces the original attachment with an attachment cleaned of threats, or converts the attachment to PDF form. Both actions invalidate the digital signature. If the attachment does not include active content, the mail remains unmodified and the digital signature valid.

Allow does not change the email. The digital signature remains valid. Select this option to prevent altering digital signatures.

Threat Emulation - Excluded Mail Addresses

What can I do here?

Use this window to exclude email senders and recipients from scanning.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Mail > Exceptions > Emulation Exceptions > Configure

Excluding Emails

You can enter email addresses that are not included in Threat Emulation protection. SMTP traffic that is sent to or from these addresses is not sent for emulation.

Note - If you want to do emulation on outgoing emails, make sure that you set the Protected Scope to **Inspect incoming and outgoing files**.

To exclude emails from Threat Emulation:

1. In the **Recipients** section, you can click the Add button and enter one or more emails.

   Emails and attachments that are sent to these addresses will not be sent for emulation.

2. In the **Senders** section, you can click the Add button and enter one or more emails.

   Emails and attachments that are received from these addresses will not be sent for emulation.

   Note - You can also use a wildcard character to exclude more than one email address from a domain.

3. Click **OK** and close the Threat Prevention profile window.
4. Install the Threat Prevention policy.

Threat Extraction - Exceptions

What can I do here?

Use this window to exclusion emails from Threat Extraction scanning. Select **Recipients** and **Senders**.

See also *"Exceptions" on page 327*

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Mail > Exceptions > Scan all emails > Exceptions

Threat Extraction For Specific Users or Groups

What can I do here?

Use this window to limit Threat Extraction scanning to specific users or groups. Select **Recipients** and **Senders**.

See also *"Configuring Exceptions" on page 327*

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Mail > Exceptions > Scan mail only for specific users or group > Configure

Threat Prevention Mail Configuration

What can I do here?

In this window you can configure how Threat Prevention and Anti-Virus scan emails.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Mail > MIME Nesting

MIME Nesting

- **Maximum MIME nesting level is (levels)** - Set the maximum number of levels that will be scanned in a MIME email with nested contents. This controls how deeply into the nesting the ThreatSpect engine will scan.
- **When nesting level is exceeded (action on file)** - If there are more MIME nested levels in an email than the maximum configured level, you can configure to block or allow the file.

IPS - Additional Activation

What can I do here?

Use this window to activate/deactivate client and server protections.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Open Profile > IPS

Additional Activation Fields

For additional granularity, in the **Additional Activation** section of the **Profile** configuration window, you can select IPS protections to activate and to deactivate. The IPS protections are arranged into tags (categories) such as **Product**, **Vendor**, **Threat Year**, and others, for the ease of search. The gateways enforce activated protections, and do not enforce deactivated protections, regardless of the general profile protection settings.

- **Activate IPS protections according to the following additional properties** - When selected, the categories configured on this page modify the profile's IPS protections.
  - **Protections to activate** - The IPS protection categories in this section are enabled on the Security Gateways that use this Threat Prevention profile.
  - **Protections to deactivate** - The IPS protection categories in this section are NOT enabled on the Security Gateways that use this Threat Prevention profile.

  These categories only filter out or add protections that comply with the activation mode thresholds (Confidence, Severity, Performance).

For example, if a protection is inactive because of its Performance rating, it is not enabled even if its category is in **Protections to activate**.

IPS - Updates Policy

What can I do here?

Use this window to set newly downloaded protections to active or inactive.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > IPS section > Updates

Updates

There are numerous protections available in IPS. It takes time to become familiar with those that are relevant to your environment. Some are easily configured for basic security and can be safely activated automatically.

In the Threat Prevention profile, you can configure an updates policy for IPS protections that were newly updated. You can do this with the **IPS** > **Updates** page in the **Profiles** navigation tree. Select one of these settings for **Newly Updated Protections**:

- **Active - According to profile settings** -Selected by default. Protections are activated according to the settings in the **General** page of the Profile. This is the Check Point recommended configuration.

  Set activation as staging mode - Newly updated protections remain in staging mode until you change their configuration. The default action for protections in staging mode is Detect. You can change the action manually in the **IPS Protections** page.

  Click **Configure** to exclude specific protections from staging mode.

- **Inactive** -Newly updated protections are not activated

Best Practice - In the beginning, allow IPS to activate protections based on the IPS policy. During this time, you can analyze the alerts that IPS generates and how it handles network traffic, while you minimize the impact on the flow of traffic. Then you can manually change the protection settings to suit your needs.

IPS Staging Configuration

What can I do here?

Use this window to exclude protections from staging mode. The exclusion is based on their impact on performance and severity.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > IPS section > Updates Policy > Set activation as Staging mode > Configure

Pre R80 IPS Settings

What can I do here?

Use this window to see the Pre R80 IPS profile assigned to the Pre R80 gateway.

Note - The Pre R80 Gateways & Servers must have the IPS blade enabled.

Getting Here - Security Policies > Threat Prevention > Custom Policy Tools > Profiles > New > IPS >
Pre R80 Settings

Pre R80 Settings

The Pre-R80 Settings are relevant for the pre-R80 gateways only.

Protections Activation

Activate protections of the following types:

- **Client Protections** - Select to activate protections that protect only clients (for example, personal computers).
- **Server Protections** - Select to activate protections that protect only servers.

  If a network has only clients or only servers, you can enhance gateway performance by deactivation of protections. If you select Client Protections and Server Protections, all protections are activated, except for those that are:

  - Excluded by the options selected here
  - Application Controls or Engine Settings
  - Defined as Performance Impact - Critical

Excluded Protections Categories

Do not activate protections of the following categories - The IPS protection categories you select here are not automatically activated. They are excluded from the Threat Prevention policy rule that has this profile in the action of the Rule Base.

Anti-Virus

What can I do here?

Use this window to configure the Anti-Virus settings for the Threat Prevention profile.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Anti-Virus

Configuring Anti-Virus Settings

You can configure Threat Prevention to exclude files from inspection, such as internal emails and internal file transfers. These settings are based on the interface type (internal or external, as defined in SmartConsole) and traffic direction (incoming or outgoing).

Before you define the scope for Threat Prevention, you must make sure that your DMZ interfaces are configured correctly. To do this, follow the steps in the table below.

To check DMZ interface configuration

Step	Instructions
1	In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway. The gateway window opens and shows the **General Properties** page.
2	From the navigation tree, click **Network Management** and then double-click a DMZ interface.
3	In the **General** page of the **Interface** window, click **Modify**.
4	In the **Topology Settings** window, click **Override** and **Interface leads to DMZ**.
5	Click **OK** and close the Security Gateway editor. Perform this procedure for each interface that goes to the DMZ.

You can configure these Anti-Virus settings in the Anti-Virus page

- **Anti-Virus UserCheck Settings**:
  - **Prevent** - Select the UserCheck message that opens for a **Prevent** action.
  - **Ask** - Select the UserCheck message that opens for an **Ask** action.
- **Protected Scope**:
  - **Inspect incoming files from**:

    Sends **only incoming** files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:

    - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
    - **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
    - **All** - Inspect all incoming files from all interface types.

- **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.

- The **Protocols** that Anti-Virus scans:
  - **Web (HTTP/HTTPS)**
  - **FTP**
  - **SMB**
  - **Mail (SMTP or POP3)** - Click **Mail** to configure the SMTP traffic inspection. This links you to the **Mail** page of the Profile settings, (see *Configuring Mail Settings*).

- File Types:
  - **Process file types known to contain malware** - Select this option to scan the files configured by default. To see the default list of files, go to **Process specific file type families**, and click **Configure**.
  - **Process all file types** -Select **Enable deep inspection scanning**, if needed. Remember, it impacts performance.
  - **Process specific file types families**

- To configure the specific file type families:

Step	Instructions
1	Click **Configure**.
2	In the **File Types Configuration** window, for each file type, select the Anti-Virus action for the file type.
3	Click **OK** to close the **File Types Configuration** window.

- **Archives** - You can configure the Anti-Virus profile to enable **archive scanning**. (see *"Enabling Archive Scanning" on the next page*).

Enabling Archive Scanning

You can configure the Anti-Virus settings to enable archive scanning. The Anti-Virus engine unpacks archives and applies proactive heuristics. The use of this feature impacts network performance.

Select **Enable Archive scanning (impacts performance)** and click **Configure:**

Setting	Description
Stop processing archive after (seconds)	Sets the amount in seconds to stop processing the archive. The default is 30 seconds.
When maximum time is exceeded (action on file)	Sets to block or allow the file when the time for processing the archive is exceeded. The default setting is **Allow**.

Blocking Viruses

To block viruses and malware in your organization

Step	Instructions
1	In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
2	In the **General Properties** page, select the **Anti-Virus** Software Blade The **First Time Activation** window opens.
3	Select **According to the Anti-Bot and Anti-Virus policy**. Click **OK**.
4	Click **OK** to close the Security Gateway Properties window.
5	Publish the SmartConsole session.
6	Click **Security Policies > Threat Prevention > Custom Policy**.
7	Click **Add Rule**. A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
8	Make a rule that includes these columns: ■ **Name** Give the rule a name such as **Block Virus Activity**. ■ **Protected Scope** The list of network objects you want to protect. In this example, the **Any** network object is used. ■ **Action** The Profile that contains the protection settings you want (see *Profiles Pane*). The default profile is **Optimized**. ■ **Track** The type of log you want to get when detecting malware on this scope. In this example, keep **Log** and also select **Packet Capture** to capture the packets of malicious activity. You will then be able to view the actual packets in **SmartConsole > Logs & Monitor > Logs**. ■ **Install On** Keep it as **All** or choose specified Security Gateways, on which to install the rule.

Step	Instructions
9	Install the Threat Prevention Policy. The IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction Software Blades have a dedicated Threat Prevention policy. You can install this policy separately from the policy installation of the Access Control Software Blades. **Best Practice** - Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways.

Additionally Supported Protocols for Anti-Virus

In addition to HTTP, FTP, SMB and SMTP protocols, which you can select in the SmartConsole GUI, the Anti-Virus Software Blade also supports the IMAP and POP3 protocols.

Procedure to activate Anti-Virus inspection for IMAP and POP3 protocols

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to the Expert mode.
3	Back up the `$FWDIR/conf/malware_config` file: `cp -v $FWDIR/conf/malware_config{,_BKP}`
4	Edit the `$FWDIR/conf/malware_config` file: `vi $FWDIR/conf/malware_config`
5	Change the value of the applicable parameter: ■ To activate IMAP protocol support: In the "`[imap]`" section, change the value of the parameter "`imap_av_policy_on`" from "`0`" to "`1`". ■ To activate POP3 protocol support: In the "`[temp_for_av_profile]`" section, change the value of the parameter "`pop3_enabled`" from "`0`" to "`1`".
6	Save the changes in the file and exit the editor.
7	In SmartConsole, install Threat Prevention Policy.

Indicators

What can I do here?

Use this window to enable indicator scanning and select specific indicator actions for the Threat Prevention profile.

See also *Threat Indicators*

Getting Here - Security Policies > Threat Prevention > Policy > right-click a profile > Edit > Indicators

UserCheck Custom Frequency

What can I do here?

Use this window to set the number of times that users get UserCheck messages for accessing applications that are not permitted by the policy.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Anti-Bot / Anti-Virus > UserCheck Settings > Show: Custom Frequency > Configure

File Types

What can I do here?

In this window you can set the Security Gateway action for the file type.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Anti-Virus > Process specific file type families > Configure

File Types Configuration

- **Type** - The file extension
- **Description** - Describes the file extension family. For example, an archive or an executable
- **Action**
  - **Inspect** - Anti-Virus scans these files based on their MD5, file type, and signatures
  - **Block** - Anti-Virus blocks these files and they cannot enter the internal network

- **Bypass** - Anti-Virus allows these files and does not scan them for viruses. Files of this type are considered safe
- **Deep Scan** - Anti-Virus scans md5 and file type

Archive Scanning

What can I do here?

Configure how the ThreatSpect engine unpacks and scans file archives.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Double-click a profile > Anti-Virus Settings > Archives > Enable Archive scanning > Configure

Archive Scanning Configuration

- **Stop processing archive after X seconds** - The maximum number of seconds that the ThreatSpect engine scans an archive. The default value is 30 seconds.
- **When maximum time is exceeded** - If the ThreatSpect engine scans the archive for more than the maximum configured level, you can configure to block or allow the file archive.

Threat Emulation - General

What can I do here?

Use this window to configure general Threat Emulation settings.

Getting Here - Security Policies Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Threat Emulation - General

Configuring Threat Emulation Settings

Before you define the scope for Threat Prevention, you must make sure that your DMZ interfaces are configured correctly. To do this:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The gateway window opens and shows the **General Properties** page.

2. From the navigation tree, click **Network Management** and then double-click a DMZ interface.

3. In the **General** page of the **Interface** window, click **Modify**.

4. In the **Topology Settings** window, click **Override** and **Interface leads to DMZ**.
5. Click **OK** and close the gateway window.

Do this procedure for each interface that goes to the DMZ.

If there is a conflict between the Threat Emulation settings in the profile and for the Security Gateway, the profile settings are used.

To configure Threat Emulation settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Custom Policy Tools** section, click **Profiles**.

   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, go to Threat Emulation and configure these settings:
   a. Threat Emulation
   b. Emulation Environment
   c. Advanced Threat Emulation Settings.
5. Click **OK** and close the Threat Prevention profile window.
6. Install the Threat Prevention policy.

Threat Emulation General Settings

On the **Threat Emulation > General** page, you can configure these settings:

UserCheck Settings:

- **Prevent** - Select the UserCheck message that opens for a **Prevent** action
- **Ask** - Select the UserCheck message that opens for an **Ask** action

Protected Scope:

Select an interface type and traffic direction option:

- **Inspect incoming files from the following interfaces**:

  Sends **only incoming** files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:

  - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.

- **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
- **All** - Inspect all incoming files from all interface types.

- **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.

Protocols

Protocols to be emulated:

- **Web (HTTP and HTTPS**
- **FTP**
- **SMB**

Mail (SMTP or **POP3)** - Click **Mail** to configure the SMTP traffic inspection by the Threat Emulation blade. This links you to the **Mail** page of the Profile settings.

File Types

Here you can configure the Threat Emulation **Action** and **Emulation Location** for each file type scanned by the Threat Emulation blade. Select one of these:

- **Process all enabled file types** - This option is selected by default. Click the blue link to see the list of supported file types. Out of the supported file types, select the files to be scanned by the Threat Emulation blade.

  Note - you can find this list of supported file types also in **Manage & Settings** view > **Blades** > **Threat Prevention** > **Advanced Settings** > **Threat Emulation** > **File Type Support**.

- **Process specific file type families** - Click **Configure** to change the action or emulation location for the scanned file types.

  To change the emulation action for a file type, click the applicable action in the **Action** column and select one of these options:

  - **Inspect** - The Threat Emulation blade scans these files.
  - **Bypass** - Files of this type are considered safe and the Software Blade does not do emulation for them.

  To change the emulation location for a file type, click **Emulation Location** and select one of these options:

  - **According to gateway** - The **Emulation Location** is according to the settings defined in the **Gateway Properties** window of each gateway.

- **Locally** - Emulation for these file types is done on the gateway.
- **ThreatCloud** - These file types are sent to the ThreatCloud for emulation.

Archives

Block archives containing these prohibited file types. Click **Configure** to select the prohibited file types. If a prohibited file type is in an archive, the gateway drops the archive.

Emulation Environment

You can use the **Emulation Environment** window to configure the emulation location and images that are used for this profile:

- The **Analysis Locations** section lets you select where the emulation is done.

  Locations

  - **Check Point ThreatCloud** - Files are sent to the Check Point ThreatCloud for emulation. The emulation in the ThreatCloud is identical to a local emulation but it does not use CPU, RAM, and disk space on a local appliance. When you configure ThreatCloud emulation, a secure SSL connection is created between the company's Security Gateway and the ThreatCloud. Files are sent to the ThreatCloud over this secure connection for emulation. The results are sent back to the Security Gateway and the applicable action is done to the file.
  - **Local Threat Emulation appliance** - The Threat Emulation appliance that does the emulation and file analysis. Threat Emulation uses the CPU, RAM and disk space of the appliance to do the emulation.
  - **Other Threat Emulation appliance** - Enable Threat Emulation on a Security Gateway and select the Threat Emulation appliance that does the emulation.

  - To use the Security Gateway settings for the location of the virtual environment, click **According to the gateway**.
  - To configure the profile to use a different location of the virtual environment, click **Specify** and select the applicable option.

    Note - In the **Remote Emulation Appliances** option, for R80.10 gateways with R80.10 Jumbo Hotfix Accumulator and R77.20 gateways, you can select multiple appliances for remote emulation. For older gateways, you can select only one appliance for remote emulation.

- The **Environments** section lets you select the operating system images on which the emulation is run. If the images defined in the profile and the Security Gateway or Threat Emulation appliance are different, the profile settings are used.

  These are the options to select the emulation images:

- To use the emulation environments recommended by Check Point security analysts, click **Use Check Point recommended emulation environments**
- To select other images for emulation, that are closest to the operating systems for the computers in your organization, click **Use the following emulation environments**

Advanced Threat Emulation Settings

- **Emulation Connection Handling Mode**

  Emulation Connection Handling Mode lets you configure Threat Emulation to allow or block a connection while it finishes the analysis of a file. The handling mode you select affects the form of the file that the user receives and the timing at which the user receives it. This section explains the difference between the Threat Emulation handling modes and the interaction between the Threat Emulation and Threat Extraction components with regards to the handling mode selected.

  The first part of the section explains what happens when Threat Emulation works with Threat Extraction disabled and the second part explains how the Threat Emulationand the Threat Extraction components work together. You can also specify a different mode for SMTP and HTTP services. To configure the settings for the Threat Emulation handling mode, go to **Security Policies** > **Threat Prevention** > **Policy** > right-click a profile > **Threat Emulation** > **Advanced**.

  Selecting an Emulation connection handling mode when Threat Extraction is disabled

  If Threat Emulation reaches a verdict regarding a file within 3 seconds or less:

  - If the file is benign, the gateway sends the original file to the user.
  - If the file is malicious, the gateway blocks the page.

  If Threat Emulation takes longer than 3 seconds to check the file:

  - In **Rapid Delivery** mode - The gateway sends the original file to the user (even if it turns out eventually that the file is malicious).
  - In **Maximum Prevention** mode - The user waits for Threat Emulation to complete. If the file is benign, the gateway sends the original file to the user. If the file is malicious, the gateway presents a Block page and the user does not get access to the file. Maximum Prevention mode gives you more security, but may cause time delays in downloading files.

  In **Custom** mode- You can set a different handling mode for SMTP and HTTP. For example: you can set HTTP to Rapid Delivery and SMTP to Maximum Prevention.

Selecting an Emulation connection handling mode when Threat Extraction is enabled

With Threat Extraction, the gateway removes potentially malicious parts from downloaded/attached files and delivers them instantly to the user. Threat Emulation continues to run in the background, and examine the original files. Threat Extraction supports certain file types, primarily Microsoft Office files and PDFs, but not all file types, for example, executables.

- If Threat Emulation rules that the file is benign, the user gets access to the original file, using the link in the file itself or the email body banner, , without help desk overhead.
- If Threat Emulation rules that the file is malicious, the original file is blocked and the user only gets access to the cleaned file.

This way administrators can ensure maximum security, while not harming end-user productivity.

This behavior would be the same for both the Rapid Delivery and Maximum Prevention modes. Nevertheless, if you select Maximum Prevention, In CLI, you can configure an even more restrictive mode, such that:

- The user always waits for Threat Emulation to complete, even if the file is supported by Threat Extraction.
- The user receives the file only if the file is deemed benign, and if the file is supported by Threat Extraction, it will also be cleaned. To configure this mode, see sk146593.

When Threat Extraction is enabled, but the file is not supported by Threat Extraction, the user is not able to receive a cleaned version of the file. The behavior therefore, will be the same as when Threat Extraction is disabled. In Rapid Delivery mode, the user gets the original file and in Maximum Prevention mode, the user waits for the Threat Emulation verdict.

Best Practice:
If Threat Extraction is enabled, use Maximum Prevention as your handling mode (without the extra preventive CLI configuration). Because most files that users work with on a daily basis are documents, that are supported by Threat Extraction, the time penalty for waiting for the non-supported files is manageable. Users will be able to receive most files in a timely manner. If Threat Extraction is disabled, select the handling mode based on balancing your security needs versus time constraints.

If you use the **Prevent** action, a file that Threat Emulation already identified as malware is blocked. Users cannot get the file even in **Rapid Delivery** mode.

- **Static Analysis** optimizes file analysis by doing an initial analysis on files. If the analysis finds that the file is simple and cannot contain malicious code, the file is sent to the destination without additional emulation. Static analysis significantly reduces the number of files that are sent for emulation. If you disable it, you increase the percentage of files that are sent for full emulation. The Security Gateways do static analysis by default, and you have the option to disable it.
- **Logging** lets you configure the system to generate logs for each file after emulation is complete.

Prohibited File Types in Archives

What can I do here?

Use this window to block archives that contain specific file types.

Getting Here - Security Policies Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Threat Emulation > General > Archives > Configure

Prohibited File Type

What can I do here?

Use this window to see information about the selected file type that has been prohibited in archives.

Getting Here - Security Policies Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Threat Emulation > General > Archives > Configure > Select a file type > Double click on File type object

Threat Emulation Supported File Types

What can I do here?

Use this window to select the file types that the Security Gateway sends for emulation.

Getting Here - Security Policies Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Threat Emulation > General > File Types > Process specific file type families > Configure > Threat Emulation Supported File Types

File Type Settings

You can configure the Threat Emulation **Action** and **Emulation Location** for each file type scanned by the Threat Emulation blade.

In the File Types section, select one of these:

- **Process all enabled file types** - This option is selected by default. Click the blue link to see the list of supported file types. Out of the supported file types, select the files to be scanned by the Threat Extraction blade.

  Note -you can find this list of supported file types also in **Manage & Settings** > **Blades** > **Threat Prevention** > **Advanced Settings** > **Threat Extraction** > **Configure File Type Support**.

- **Process specific file type families** -Click **Configure** to change the action or emulation location for the scanned file types.

  To change the emulation action for a file type, click the applicable action in the **Action** column and select one of these options:

  - **Inspect** - The Threat Emulation blade scans these files.
  - **Bypass** - Files of this type are considered safe and the Software Blade does not do emulation for them.

  To change the emulation location for a file type, click **Emulation Location** and select one of these options:

  - **According to gateway** - The **Emulation Location** is according to the settings defined in the **Gateway Properties** window of each gateway.
  - **Locally** - Emulation for these file types is done on the gateway.
  - **ThreatCloud** - These file types are sent to the ThreatCloud for emulation.

Threat Emulation - Emulation environment

What can I do here?

Use this window to configure the Threat Emulation location and environment.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Threat Emulation > Emulation Environment

ThreatCloud Emulation

You can securely send files to the Check Point ThreatCloud for emulation. The ThreatCloud is always up-to-date with the latest Threat Emulation releases.

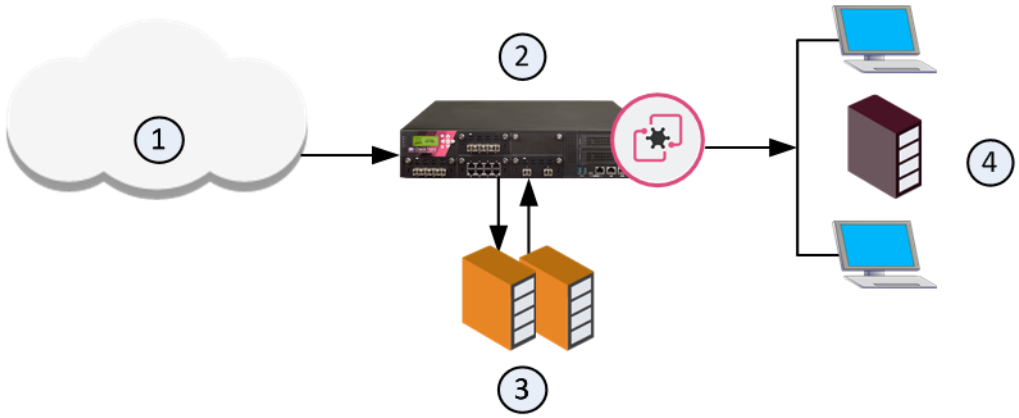
Sample ThreatCloud Emulation Workflow

1. The Security Gateway gets a file from the Internet or an external network.
2. The Security Gateway compares the cryptographic hash of the file with the database.

- If the file is already in the database, no additional emulation is necessary
- If the file is not in the database, it is necessary to run full emulation on the file

3. The file is sent over an SSL connection to the ThreatCloud.
4. The virtual computers in the ThreatCloud run emulation on the file.
5. The emulation results are sent securely to the Security Gateway for the applicable action.

Sample ThreatCloud Deployment



Item	Description
1	Internet and external networks
2	Perimeter Security Gateway
3	Check Point ThreatCloud servers
4	Computers and servers in the internal network

Threat Emulation Analysis Locations

You can choose a location for the emulation analysis that best meets the requirements of your company.

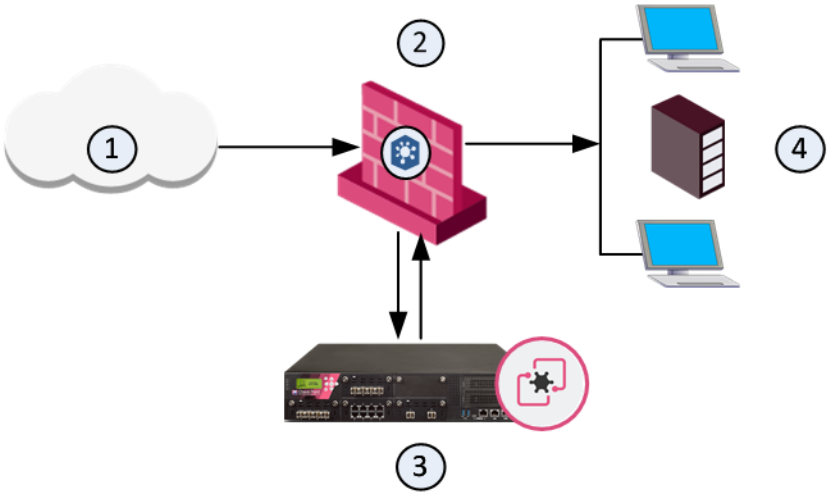
- **ThreatCloud** - You can send all files to the Check Point ThreatCloud for emulation. Network bandwidth is used to send the files and there is a minimal performance impact on the Security Gateway.
- **Private ThreatCloud Appliance in the Internal network** - You can use a Threat Emulation appliance to run emulation on the files.

Local or Remote Emulation

You can install a Threat Emulation appliance in the internal network.

Sample Workflow for Threat Emulation Appliance in a Local Deployment

1. The Threat Emulation appliance receives the traffic, and aggregates the files.
2. The Threat Emulation appliance compares the cryptographic hash of the file with the database.
   - The file is already in the database, no more emulation is necessary.
   - If the file is not in the database, the virtual computers in the Threat Emulation appliance run full emulation on the file.

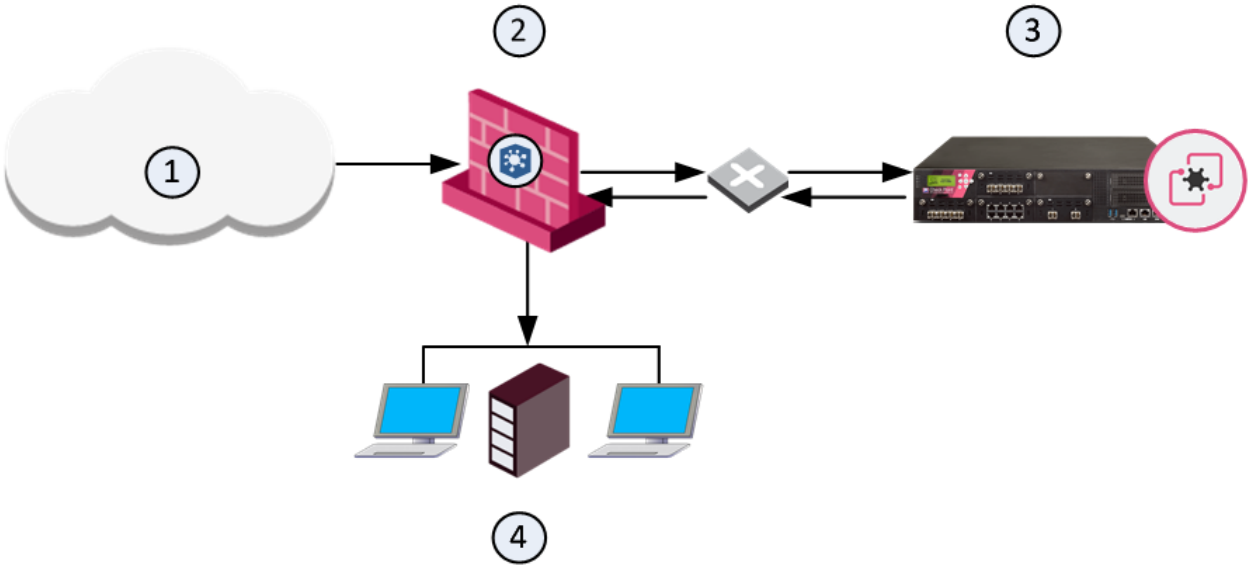


Item	Description
1	Internet and external networks
2	Perimeter Security Gateway
3	Threat Emulation appliance
4	Computers and servers in the internal network

Sample Workflow for Threat Emulation Appliance in a Remote Deployment

1. The Security Gateway aggregates the files, and the files are sent to the Threat Emulation appliance.

2. The Threat Emulation appliance compares the cryptographic hash of the file with the database.
   - The file is already in the database, no more emulation is necessary.
   - If the file is not in the database, the virtual computers in the Threat Emulation appliance run full emulation on the file.



Item	Description
1	Internet and external networks
2	Perimeter Security Gateway
3	Threat Emulation Private Cloud Appliance
4	Computers and servers in the internal network

Optimizing File Emulation

Files have unique cryptographic hashes, these file hashes are stored in a database after emulation is complete. Before emulation is run on a file, the appliance compares the file hash to the database:

- If the hash is not in the database, the file is sent for full emulation
- If the hash is in the database, then it is not necessary to run additional emulation on the file

This database helps to optimize emulation and give better network performance.

Selecting the Threat Emulation Deployment

What are my options to send traffic for emulation?

- Inline - Traffic is sent for emulation before it is allowed to enter the internal network. You can use the Threat Prevention policy to block malware.
- SPAN/TAP - You can use a mirror or TAP port to duplicate network traffic. Files are sent to the computer in the internal network. If Threat Emulation discovers that a file contains malware, the appropriate log action is done.
- MTA (Mail Transfer Agent) - SMTP traffic goes to the Security Gateway, and is sent for emulation. The MTA acts as a mail proxy, and manages the SMTP connection with the source. The MTA sends email files to emulation after it closes the SMTP connection. When the file emulation is completed, the emails are sent to the mail server in the internal network.

I want to use the Prevent action and be able to block malicious files, what are my deployment options?

- ThreatCloud - Files are sent to the ThreatCloud for emulation. When the emulation is complete, ThreatCloud sends a notification to the Security Gateway that the files are safe. Then they go to computers in the internal network.
- Threat Emulation appliance with inline deployment - The files are kept in the Threat Emulation appliance and after emulation, safe files go to the computer in the internal network.

This table summarizes how Threat Emulation sends traffic for emulation:

	Block Malware
Inline	Yes
SPAN/TAP	No
MTA	Recommended with Prevent action for emails

Inline Deployments (Prevent and Ask)

Use the Prevent or Ask UserCheck action to quarantine a malicious file.

Sample Inline Emulation Workflow (Prevent Action)

1. The ThreatCloud or Threat Emulation appliance gets a file from the Security Gateway.
2. Emulation is run on the file.

- The file is safe, and it is sent to the computer in the internal network.
- If the file contains malware, it is quarantined and logged.

Monitor Deployments

Sample Monitor Emulation Workflow

1. The ThreatCloud or Threat Emulation appliance gets a copy of a file from the Security Gateway. The original file goes to the computer in the internal network.
2. Emulation is run on the file.
   - The file is safe, no other action is done
   - If the file is identified as malware, it is logged according to the **Track** action of the Threat Prevention rule

Threat Emulation Deployments with a Mail Transfer Agent

SMTP traffic goes to the Security Gateway, and is sent for emulation. The MTA acts as a mail proxy, and manages the SMTP connection with the source. The MTA sends email files to emulation after it closes the SMTP connection. When the file emulation is completed, the emails are sent to the mail server in the internal network.

For more information on how to work with the Mail Transfer Agent, see Mail Transfer Agent.

Check Point ThreatCloud Network

By default, all gateways send threat information to the ThreatCloud.

You can change this default behavior in SmartConsole.

To configure all gateways not to send information to the ThreatCloud:

1. Open **Global Properties > Security Management Access**.
2. In the **Internet Access** area, clear this setting: **Improve product experience by sending data to Check Point**.
3. Click **OK**.
4. Restart SmartConsole.
5. In SmartConsole, install the policy.

System Specifications

These are the specifications for the Threat Emulation deployments:

- Threat Cloud - R77 (or higher) Security Gateways running Gaia (64 or 32-bit)
- R77.20 (or higher) VSX Gateways
- For Local or Remote emulation:

  Maximum size of file to send to emulation is: 100,000 KB

  Check Point Threat Emulation appliance with R77 or higher on the Gaia operating system (64-bit only), and R77.20 or higher VSX Gateways (Remote emulation only)

  Make sure that:

  - Each Virtual System has access to the Remote gateway or to the cloud.
  - Each Virtual System Gateway has access to the Internet for updates from the Check Point Download Center.

Note -This release does not support:

- Active/Standby Bridge Mode
- Virtual System Load Sharing Security Clusters with more than two members.
- MTA

Threat Emulation - Advanced

What can I do here?

Use this window to configure these advanced Threat Emulation settings:

- Emulation Connection Handling Mode
- Engine Settings
- Logging

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Threat Emulation > Advanced

Handling Connections During Emulation

Emulation Connection Handling Mode lets you configure Threat Emulation to allow or block a connection while it finishes the analysis of a file. The handling mode you select affects the form of the file that the user receives and the timing at which the user receives it. This section explains the difference between the Threat Emulation handling modes and the interaction between the Threat Emulation and Threat Extraction components with regards to the handling mode selected.

The first part of the section explains what happens when Threat Emulation works with Threat Extraction disabled and the second part explains how the Threat Emulationand the Threat Extraction components work together. You can also specify a different mode for SMTP and HTTP services. To configure the settings for the Threat Emulation handling mode, go to **Security Policies** > **Threat Prevention** > **Policy** > right-click a profile > **Threat Emulation** > **Advanced**.

Selecting an Emulation connection handling mode when Threat Extraction is disabled

If Threat Emulation reaches a verdict regarding a file within 3 seconds or less:

- If the file is benign, the gateway sends the original file to the user.
- If the file is malicious, the gateway blocks the page.

If Threat Emulation takes longer than 3 seconds to check the file:

- In **Rapid Delivery** mode - The gateway sends the original file to the user (even if it turns out eventually that the file is malicious).
- In **Maximum Prevention** mode - The user waits for Threat Emulation to complete. If the file is benign, the gateway sends the original file to the user. If the file is malicious, the gateway presents a Block page and the user does not get access to the file. Maximum Prevention mode gives you more security, but may cause time delays in downloading files.

In **Custom** mode- You can set a different handling mode for SMTP and HTTP. For example: you can set HTTP to Rapid Delivery and SMTP to Maximum Prevention.

Selecting an Emulation connection handling mode when Threat Extraction is enabled

With Threat Extraction, the gateway removes potentially malicious parts from downloaded/attached files and delivers them instantly to the user. Threat Emulation continues to run in the background, and examine the original files. Threat Extraction supports certain file types, primarily Microsoft Office files and PDFs, but not all file types, for example, executables.

- If Threat Emulation rules that the file is benign, the user gets access to the original file, using the link in the file itself or the email body banner, , without help desk overhead.
- If Threat Emulation rules that the file is malicious, the original file is blocked and the user only gets access to the cleaned file.

This way administrators can ensure maximum security, while not harming end-user productivity.

This behavior would be the same for both the Rapid Delivery and Maximum Prevention modes. Nevertheless, if you select Maximum Prevention, In CLI, you can configure an even more restrictive mode, such that:

- The user always waits for Threat Emulation to complete, even if the file is supported by Threat Extraction.
- The user receives the file only if the file is deemed benign, and if the file is supported by Threat Extraction, it will also be cleaned. To configure this mode, see sk146593.

When Threat Extraction is enabled, but the file is not supported by Threat Extraction, the user is not able to receive a cleaned version of the file. The behavior therefore, will be the same as when Threat Extraction is disabled. In Rapid Delivery mode, the user gets the original file and in Maximum Prevention mode, the user waits for the Threat Emulation verdict.

Best Practice:
If Threat Extraction is enabled, use Maximum Prevention as your handling mode (without the extra preventive CLI configuration). Because most files that users work with on a daily basis are documents, that are supported by Threat Extraction, the time penalty for waiting for the non-supported files is manageable. Users will be able to receive most files in a timely manner. If Threat Extraction is disabled, select the handling mode based on balancing your security needs versus time constraints.

If you use the **Prevent** action, a file that Threat Emulation already identified as malware is blocked. Users cannot get the file even in **Rapid Delivery** mode.

Static Analysis

Static Analysis optimizes file analysis by doing an initial analysis on files. If the analysis finds that the file is simple and cannot contain malicious code, the file is sent to the destination without additional emulation. Static analysis significantly reduces the number of files that are sent for emulation. If you disable it, you increase the percentage of files that are sent for full emulation. The Security Gateways do static analysis by default, and you have the option to disable it.

Logging

Lets you configure the system to generate logs for each file after emulation is complete.

Custom Emulation Connection Handling Mode

What can I do here?

Use this window to configure the handling mode for SMTP and HTTP services.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Threat Emulation > Advanced > Custom - configure handling mode depending on the service > Customize

Service Mode Options

Emulation Connection Handling Mode lets you configure Threat Emulation to allow or block a connection while it finishes the analysis of a file. The handling mode you select affects the form of the file that the user receives and the timing at which the user receives it. This section explains the difference between the Threat Emulation handling modes and the interaction between the Threat Emulation and Threat Extraction components with regards to the handling mode selected.

The first part of the section explains what happens when Threat Emulation works with Threat Extraction disabled and the second part explains how the Threat Emulationand the Threat Extraction components work together. You can also specify a different mode for SMTP and HTTP services. To configure the settings for the Threat Emulation handling mode, go to **Security Policies** > **Threat Prevention** > **Policy** > right-click a profile > **Threat Emulation** > **Advanced**.

Selecting an Emulation connection handling mode when Threat Extraction is disabled

If Threat Emulation reaches a verdict regarding a file within 3 seconds or less:

- If the file is benign, the gateway sends the original file to the user.
- If the file is malicious, the gateway blocks the page.

If Threat Emulation takes longer than 3 seconds to check the file:

- In **Rapid Delivery** mode - The gateway sends the original file to the user (even if it turns out eventually that the file is malicious).
- In **Maximum Prevention** mode - The user waits for Threat Emulation to complete. If the file is benign, the gateway sends the original file to the user. If the file is malicious, the gateway presents a Block page and the user does not get access to the file. Maximum Prevention mode gives you more security, but may cause time delays in downloading files.

In **Custom** mode- You can set a different handling mode for SMTP and HTTP. For example: you can set HTTP to Rapid Delivery and SMTP to Maximum Prevention.

Selecting an Emulation connection handling mode when Threat Extraction is enabled

With Threat Extraction, the gateway removes potentially malicious parts from downloaded/attached files and delivers them instantly to the user. Threat Emulation continues to run in the background, and examine the original files. Threat Extraction supports certain file types, primarily Microsoft Office files and PDFs, but not all file types, for example, executables.

- If Threat Emulation rules that the file is benign, the user gets access to the original file, using the link in the file itself or the email body banner, , without help desk overhead.
- If Threat Emulation rules that the file is malicious, the original file is blocked and the user only gets access to the cleaned file.

This way administrators can ensure maximum security, while not harming end-user productivity.

This behavior would be the same for both the Rapid Delivery and Maximum Prevention modes. Nevertheless, if you select Maximum Prevention, In CLI, you can configure an even more restrictive mode, such that:

- The user always waits for Threat Emulation to complete, even if the file is supported by Threat Extraction.
- The user receives the file only if the file is deemed benign, and if the file is supported by Threat Extraction, it will also be cleaned. To configure this mode, see sk146593.

When Threat Extraction is enabled, but the file is not supported by Threat Extraction, the user is not able to receive a cleaned version of the file. The behavior therefore, will be the same as when Threat Extraction is disabled. In Rapid Delivery mode, the user gets the original file and in Maximum Prevention mode, the user waits for the Threat Emulation verdict.

Best Practice:
If Threat Extraction is enabled, use Maximum Prevention as your handling mode (without the extra preventive CLI configuration). Because most files that users work with on a daily basis are documents, that are supported by Threat Extraction, the time penalty for waiting for the non-supported files is manageable. Users will be able to receive most files in a timely manner. If Threat Extraction is disabled, select the handling mode based on balancing your security needs versus time constraints.

If you use the **Prevent** action, a file that Threat Emulation already identified as malware is blocked. Users cannot get the file even in **Rapid Delivery** mode.

Threat Extraction - General

What can I do here?

Use this window to configure:

- UserCheck settings
- Mail Protocol
- Extraction Settings
- File types

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Edit > Threat Extraction > General

Configuring Threat Extraction Settings

To configure Threat Extraction settings for a Threat Prevention profile:

1. In the **Security Policies** view > **Custom Policy Tools** section, click **Profiles**.
2. Right-click a profile and select **Edit**.

   The **Profiles** properties window opens.
3. On the **General Policy** page in the **Blade Activation** area, select **Threat Extraction**.
4. Configure these Threat Extraction Settings:
   - Threat Extraction General Settings
   - Threat Extraction Advanced Settings
5. Click **OK**.

Note - You can configure some of the Threat Extraction features in a configuration file, in addition to the CLI and GUI. See sk114613.

Threat Extraction General Settings

On the **Threat Extraction > General** page, you can configure these settings:

UserCheck Settings

- **Allow the user to access the original file**
- **Allow access to original files that are not malicious according to Threat Emulation**

  Note - This option is only configurable when the Threat Emulation blade is activated in the **General Properties** pane of the profile.
- **UserCheck Message**

  Select a message to show the user when the user receives the clean file. In this message, the user selects if they want to download the original file or not. To select the success or cancellation messages of the file download, go to **Manage & Settings** > **Blades** > **Threat Prevention** > **Advanced Settings** > **UserCheck**. You can create or edit UserCheck messages on the UserCheck page. You can customize a UserCheck message only for SMTP files. For HTTP files (supported on R80.30 gateways and higher), the message which the user gets is not customizable in SmartConsole. You can only customize it on the gateway.

- **Optional:** To give the user access to the original email, you can add the **Send Original Mail** field in the **Threat Extraction Success Page**. Go to **Threat Prevention** > **Custom Policy Tools** > **UserCheck** > **Threat Extraction Success Page** > right-click > **Clone** > click inside the message > **Insert Field** > select **Send Original Mail**.

  Send Original Mail is added to the message body.

Protocol

- **Web (HTTP/HTTPS)** - Supported from R80.30 gateways and higher. To allow web support, enable HTTPS Inspection. By default, Threat Extraction web support works on these standard ports: HTTP - Port 80, HTTPS - Port 443, HTTPS Proxy - 8080.

  To enable web support on other ports, create a new TCP service. In **General** > **Protocol** select **HTTP**, and in **Match By**, select **Customize** and enter the required port number.

  Notes:

  - After a file is scanned by the Threat Extraction blade, the user receives a message on the action that was done on the file. To customize the message, see sk142852.
  - Threat Extraction web support applies to web downloads, but not web uploads.

- **Mail (SMTP)** - Click **Mail** to configure the SMTP traffic inspection by the Threat Extraction blade. This links you to the Mail page of the Profile settings.

For information on storage of the original files, see Storage of Original Files.

Extraction Method

- **Extract potentially malicious parts from files** - Selected by default

  Click **Configure** to select which malicious parts the blade extracts. For example, macros, JavaScript, images and so on.

- **Convert to PDF** - Converts the file to PDF, and keeps text and formatting. **Best Practice** - If you use PDFs in right-to-left languages or Asian fonts, preferably select **Extract files from potential malicious parts** to make sure that these files are processed correctly.

Extraction Settings

- **Process all files** - Selected by default
- **Process malicious files when the confidence level is:**

  Set a low, medium or high confidence level. This option is only configurable when the Threat Emulation blade is activated in the **General Properties** pane of the profile.

File Types

- **Process all enabled file types** - This option is selected by default. Click the blue link to see the list of supported file types. Out of the supported file types, select the files to be scanned by the Threat Extraction blade.

  Note - you can find this list of supported file types also in **Manage & Settings** view > **Blades** > **Threat Prevention** > **Advanced Settings** > **Threat Extraction** > **Configure File Type Support**.

- **Process specific file type families** -

  Here you can configure a different extraction method for certain file types. Click **Configure** to see the list of enabled file types and their extraction methods. To change the extraction method for a file type, right-click the file type and select: bypass, clean or convert to pdf. You can select a different extraction method for Mail and Web.

Notes:

- Supported file types for web are: Word, Excel, PowerPoint and PDF.

For e-mail attachments:

- For jpg, bmp, png, gif, and tiff files - Threat Extraction supports only extraction of potentially malicious content.
- For hwp, jtd, eps, files - Threat Extraction supports only conversion to pdf.
- For Microsoft Office and PDF files and all other file types on the list - Threat Extraction supports both extraction of potentially malicious content and conversion to pdf.
- You can also configure supported file types in the configuration file. For explanation, see sk112240.

Threat Extraction Advanced Settings

On the **Threat Extraction** > **Advanced** page, you can configure these settings:

- **Logging**
  - **Log only those files from which threats were extracted** - Logs only files on which an operation was performed (clean or convert).
  - **Log every file** -Every file that is selected in **Threat Extraction** > **General** > **File Types** is logged, even if no operation was performed on them.
- **Threat Extraction Exceptions**

- **Corrupted files**

  Block or Allow corrupted files attached to the email or downloaded from the web. Corrupted files are files the blade fails to process, possibly because the format is incorrect. Despite the incorrect format, the related application (Word, Adobe Reader) can sometimes show the content.

  Block removes the corrupted file and sends the recipient a text which describes how the file contained potentially malicious content. You can block corrupt files if they are malicious according to Threat Emulation. If the action is block, you can deny access to the original corrupted file.

  Allow lets the recipient receive the corrupted file.

- **Encrypted files**

  Block or Allow encrypted files attached to the email or downloaded from the web.

  Block removes the encrypted file and sends the recipient a text file which describes how the file contained potentially malicious content.

  If the action is block, you can also deny access to the original encrypted file.

  Allow lets the recipient receive the encrypted file.

Extraction Method

What can I do here?

Use this window to configure which parts of a file to extract.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Edit > Threat Extraction > General > Extraction Method > Configure

Extraction Method

For more see *"Threat Extraction - General" on page 356*

Threat Extraction - Supported File Types

What can I do here?

Use this window to select specific file types to process during Threat Extraction.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Edit > Threat Extraction > General > File Types > Process specific... > Configure

Supported File Types

For more see *"Threat Extraction - General" on page 356*

Threat Extraction - Advanced

What can I do here?

Use this window to configure Threat Extraction logging options and exceptions to Threat Extraction.

Getting Here - Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Edit > Threat Extraction > Advanced

Threat Extraction Advanced Settings

On the **Threat Extraction** > **Advanced** page, you can configure these settings:

- **Logging**
  - **Log only those files from which threats were extracted** - Logs only files on which an operation was performed (clean or convert).
  - **Log every file** -Every file that is selected in **Threat Extraction** > **General** > **File Types** is logged, even if no operation was performed on them.
- **Threat Extraction Exceptions**
  - **Corrupted files**

    Block or Allow corrupted files attached to the email or downloaded from the web. Corrupted files are files the blade fails to process, possibly because the format is incorrect. Despite the incorrect format, the related application (Word, Adobe Reader) can sometimes show the content.

    Block removes the corrupted file and sends the recipient a text which describes how the file contained potentially malicious content. You can block corrupt files if they are malicious according to Threat Emulation. If the action is block, you can deny access to the original corrupted file.

    Allow lets the recipient receive the corrupted file.

- **Encrypted files**

  Block or Allow encrypted files attached to the email or downloaded from the web.

  Block removes the encrypted file and sends the recipient a text file which describes how the file contained potentially malicious content.

  If the action is block, you can also deny access to the original encrypted file.

  Allow lets the recipient receive the encrypted file.

Malware DNS Trap

What can I do here?

Use this window to set the IP address for the Malware DNS trap.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Profiles > Profile > Advanced > Malware DNS Trap

Configuring a Malware DNS Trap

The Malware DNS trap works by configuring the Security Gateway to return a false (bogus) IP address for known malicious hosts and domains. You can use the Security Gateways external IP address as the DNS trap address but:

- Do not use a gateway address that leads to the internal network
- Do not use the gateway internal management address
- If the gateway external IP address is also the management address, select a different address for the DNS trap.

You can also add internal DNS servers to better identify the origin of malicious DNS requests.

Using the Malware DNS Trap you can detect compromised clients by checking logs with connection attempts to the false IP address.

At the Security Gateway level, you can configure the DNS Trap according to the profile settings or as a specific IP address for all profiles on the specific gateway.

To set the Malware DNS Trap parameters for the profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Custom Policy Tools** section, click **Profiles**.

   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Malware DNS Trap**.

5. Click **Activate DNS Trap**.
6. Enter the **IP** address for the DNS trap.
7. **Optional:** Add **Internal DNS Servers** to identify the origin of malicious DNS requests.
8. Click **OK** and close the Threat Prevention profile window.
9. Install the Threat Prevention policy.

To set the Malware DNS Trap parameters for a gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, select **Anti-Bot and Anti-Virus**.
3. In the **Malicious DNS Trap** section, select one of these options:
   - **According to profile settings** - Use the Malware DNS Trap IP address configured for each profile.
   - **IPv4** - Enter an IP address to be used in all the profiles assigned to this Security Gateway.
4. Click **OK**.
5. Install the policy.

IPS Protections

What can I do here?

Use this window to see the IPS protections, edit them, and set actions.

You can also export the protections to a *.csv* file using the **Actions > Export View** option.

Note - This window shows ThreatCloud IPS protections and Core protections related to IPS. A number of low level gateway parsing and VoIP settings previously defined as IPS Protections (in R77 and lower) have moved to Manage & Settings > Blades > General > Inspection settings. These inspection engine settings are installed as part of the Access Control Policy and not the Threat Prevention policy.

For more information on each protection, click the applicable link in the Industry Reference column.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections

IPS Protections - Show Profiles

What can I do here?

Use this window to:

- Show all IPS profiles used in the Custom Threat Prevention policy
- Show Specified IPS enabled profiles -- strict, optimized, or basic.

Getting Here - Security Policies > Threat Prevention > Custom Policy > Custom Policy Tools > IPS Protections > View > Show Profiles

IPS Actions - Profile Cleanup

What can I do here?

Use this window to cleanup the selected profile.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Actions > Profile cleanup

Protection Actions - Add Exception

What can I do here?

Use this window to add an exception to a protection.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Protections / Actions > Selected Protections > Add Exception

IPS Actions - Add Exception - Go to

What can I do here?

Click the "Go to..." link to locate the protection for which you added an exception.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections / Protections > Select protection > Actions > Add Exception > Click OK

IPS Core Protections - General

What can I do here?

Use this window to see:

- The performance impact, severity, and confidence level of the selected IPS protection.
- The action to take for the selected protection, as set by the profile.

The IPS protections are divided into two main types:

- **Core protections** - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy.
- **ThreatCloud protections** - These protections are part of the Threat Prevention policy updated from the Check Point Cloud-

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Open a core protection

IPS Core Protections - Gateways

What can I do here?

Use this window to see the gateway or gateways enforcing the selected protection, and the assigned profile.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Open a core protection > Gateways Page

IPS Core Protections - Exceptions

What can I do here?

Use this window to create an IPS exception.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Open a core protection > Exceptions Page

IPS Protection - Actions

What can I do here?

Use this window to see:

- The performance impact, severity, and confidence level of the selected IPS protection.
- The action to take for the selected protection, as set by the profile.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Open a protection

IPS Protection - Protection Details

What can I do here?

Use this window to:

- See the main action according to the profile
- Override the main action
- Set tracking options

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Open a protection > Double-click a profile.

IPS Protections - General Properties

What can I do here?

Use this window to:

- See the default action
- Override the default action
- Set logging options
- Enable packet capture

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Edit a protection.

IPS Protections - Advanced

What can I do here?

Use this window to see the scope of a protection.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Edit a protection > Advanced

Inbound DNS Requests - Advanced

What can I do here?

Use this window to apply the protection to selected DNS servers.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Inbound DNS Requests > Edit > General > Open profile > Advanced page

IPS Protection - Unknown SMTP Commands - Advanced

What can I do here?

Use this window to configure SMTP command definitions.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Unknown SMTP Commands > Edit > General > Open profile > Advanced page

IPS Protection - Scrambling - Advanced

What can I do here?

Use this window to apply the protection to all DNS traffic or selected DNS servers.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Scrambling > Edit > General > Open profile > Advanced page

IPS Protection - FTP Commands - Advanced

What can I do here?

Use this window to configure blocked FTP commands.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > FTP Commands > Edit > General > Open profile > Advanced page

IPS Protection - Directory Traversal - Advanced

What can I do here?

Use this window to apply the protection to all HTTP traffic, or to selected web servers.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Directory Traversal > Edit > General > Open profile > Advanced page

IPS Protection - Spoofed Reset - Advanced

What can I do here?

Use this window to set the number of RST packets allowed per connection, and block further RST packets for a specified time interval (in seconds).

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Spoofed Reset > Edit > General > Open profile > Advanced page

IPS Protection - SQL Injection - Advanced

What can I do here?

Use this window to:

- Set the scope of the traffic (all HTTP traffic or selected web servers)
- Block distinct and non-distinct SQL commands

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > SQL Injection > Edit > General > Open profile > Advanced page

IPS Protection - Cross-Site Scripting - Advanced

What can I do here?

Use this window to set the protection scope and block script commands.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Cross-Site Scripting > Edit > General > Open profile > Advanced page

Cross-Site Scripting Attack Description

Cross-site scripting attacks place malicious code in locations where other users see it. The intention of the attack is to steal cookies that contain user identities and credentials, or to trick users into supplying their credentials to the attacker.

One kind of cross site scripting attack is intended to steal cookies that contain user identities and credentials. A hacker may want to steal cookies in order to impersonate another user. The client sends cookies to the Web site with every HTTP Request.

Many Web sites contain forms, which are used to post information such as names and addresses, or comments on bulletin boards. The hacker can inject scripting code into the attacked Web server by adding scripting code to these forms.

The Web server will send cookies only to the client that owns them. Since the hostile code runs in the client machine, the code can instruct the Web browser on the client machine to send its cookies to another location, such as another Web site (hence the name: Cross Site Scripting), where the hacker can see the cookies.

This attack is especially dangerous because neither the user nor the Web site administrator knows that the attack is taking place, unless they analyze the posted source code.

A second variety of Cross-site scripting attack does not steal cookies, but rather dupes the victim into supplying his or her credentials to the attacker. For example, an online auction site may allow users to post advertisement that will say something like:

For sale: Rolls Royce, 1995, Only $20,000, As new.

A hacker can post an advert that contains scripting code, for example:

For sale: Rolls Royce, 1995, <script>alert("Connection broken. Please re- enter username and password")</script>Only $20,000, As new.

When a user views the advert, the script causes a popup form to appear that asks the user to supply his or her details. The user viewing the second advert assumes the pop-up is from the auction site, and fills in his username and password. The script sends those details to the attacker.

Web Security Protections

To protect against Cross-Site Scripting attacks, Web Security rejects HTTP Requests sent using the POST command, that contain scripting code. Web Security also identifies encoded data sent as part of the URL, which is an alternative way of submitting information. The scripting code is not stripped from the request, but rather the whole request is rejected.

IPS Protection - CIFS (SMB) File Name Patterns - Advanced

What can I do here?

Use this window to block file and print sharing worms.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > CIF (SMB) File Name Patterns > Edit > Open Profile > Advanced page

IPS Protection - Microsoft LDAP Remote Anonymous Denial of Service (MS13-079)

What can I do here?

Use this window to configure the actions for this protection according to the profile.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Microsoft LDAP Remote Anonymous Denial of Service (MS13-079)

IPS Protection - Additional Settings

What can I do here?

Use this window to see additional settings the selected profile applies to the protection.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Open protection for viewing > Select and open a profile.

HTTP Response Status Message Concealment - Application Engine Pattern

What can I do here?

Use this window to enforce the detection pattern for HTTP Response Status Message Concealment.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > HTTP Response Status Message Concealment > Select a profile > Edit > Advanced > Application Engine Pattern > Edit

HTTP Response Status Message Concealment

What can I do here?

Use this window to set the protection scope, concealed HTTP response status codes, and application engine patterns.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > HTTP Response Status Message Concealment > Select a profile > Edit > Advanced

HTTP Response Status Message Concealment - Detection Patterns

What can I do here?

Use this window to configure detection patterns for HTTP Response Status Message Concealment.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > HTTP Response Status Message Concealment > Select a profile > Edit > Advanced > Application Engine Pattern > Edit > Click Edit icon in window

HTTP URL Patterns - Advanced

What can I do here?

Use this window to set the protection scope for HTTP URL patterns, and block HTTP Worms.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > HTTP URL Patterns > Select a profile > Edit profile > Advanced

Host Port Scan - Advanced

What can I do here?

Use this window to set detection sensitivity.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Host Port Scan > Select a profile > Edit profile > Advanced

HTTP Header Patterns - Detection Properties

What can I do here?

Use this window to set the Header Detection Properties.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > HTTP Header Patterns > Select a profile > Edit profile > Advanced > Header Rejection > New or Edit

HTTP Header Patterns

What can I do here?

Use this window to configure the protection scope, Header detection properties, and set the behavior for URI resources in earlier versions - R65 and lower.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > HTTP Header Patterns > Select a profile > Edit profile > Advanced

LDAP Injection - Advanced

What can I do here?

Use this window to set the protection scope and block relative distinguished names.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > LDAP Injection > Select a profile > Edit profile > Advanced

HTTP Header Spoofing - Advanced

What can I do here?

Use this window to set the protection Scope, and header spoofing settings.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > HTTP Header Spoofing > Select a profile > Edit profile > Advanced

Header Spoofing Settings

What can I do here?

Use this window to set the header definition, and action.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > HTTP Header Spoofing > Select a profile > Edit profile > Advanced > Header Spoofing > New or Edit.

Sweep Scan - Advanced

What can I do here?

Use this window to set the detection sensitivity.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Sweep Scan > Select a profile > Edit profile > Advanced

Understanding Sweep Scanning

In this window you can select one of three levels of port scan detection sensitivity. Each level represents the amount of inactive ports scanned during a certain amount of time. When port scanning is detected a log or alert is issued.

Port scanning is a method of intelligence gathering. Gathering information about computers is not in itself an attack, but the information can be used later to target and attack vulnerable computers.

A sweep scan tries to find out which hosts in the network have opened a specific port, in other words, the hosts that offer a specific service.

How does IPS Detect Sweep Scans?

The Sweep Scan feature does not physically *block* port scanning. IPS *detects* ports scans with one of three possible levels of detection sensitivity. When a port scan is detected a log or alert is issued. The source of the port scan is identified in the log. The administrator can choose to add the source IP to the quarantine list.

IPS can monitor and log the ports on which a sweep scan has been performed.

How To Block Port Scans

It is possible to *block* clients that IPS detects as performing port scanning, by configuring automatic SAM (Suspicious Activity Monitoring) alert rules on the Security Management server to block offending IP addresses. For information about the sam_alert **command** see the *Command Line Interface (CLI)* guide.

Note - An automatic **sam_alert** rule may expose legitimate hosts to a remote DoS attack. An attacker could spoof a port scan from a legitimate IP, which would then be blocked by the automatic SAM rule.

Detection Sensitivity

The sensitivity of the port scan detection can be changed. Predefined or a customized settings can be chosen. The predefined settings provide high, medium or low detection sensitivity. A high sensitivity catches even long, slow scans, but may give false positives for legitimate network activity. Low detection sensitivity, reduces the number of false positives, but may miss long, patient scans.

Enforcing Servers

What can I do here?

Use this window to see enabled servers.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Open a relevant protection > open profile > Advanced > Protection scope > view > Enforcing web servers window > help
Or:
Manage & Settings > Blades > General > Inspection Settings > relevant protection > Edit Protection > Advanced > View > Enforcing web servers window

SMTP Content

What can I do here?

Use this window to configure SMTP content for R67 and earlier versions.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SMTP Content

Protection Details

What can I do here?

Use this window to see the details of a selected protection, set actions, tracking options, and packet capture.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Select protection > Actions > Edit

Protection Logs

What can I do here?

Use this window to see the logs for protections in the view, or selected logs in the view.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Logs tab at bottom > Show logs for all protections in this view

Updates - Threat Prevention

What can I do here?

Use this window to configure automatic updates to the malware database, Threat Emulation engine, Threat Emulation images, and IPS database.

Getting Here - Security Policies > Threat Prevention > Custom Policy > Custom Policy Tools > Updates
Or:
Security Policies > Autonomous Threat Prevention > Autonomous Policy Tools > Updates

Threat Prevention Scheduled Updates

Introduction to Scheduled Updates

Check Point wants the customer to be protected. When a protection update is available, Check Point wants the configuration to be automatically enforced on the gateway. You can configure automatic gateway updates for the Anti-Virus, Anti-Bot, Threat Emulation and IPS blades.

For the Anti-Virus, Anti-Bot and Threat Emulation, the gateways download the updates directly from the Check Point cloud.

For the IPS blade, prior to R80.20, the updates were downloaded to the Security Management Server, and only after you installed policy, the gateways could enforce the updates. Starting from R80.20, the gateways can directly download the updates. For R80.20 gateways and higher with no internet connectivity, you must still install policy to enforce the updates.

When you configure automatic IPS updates on the gateway, the action for the newly downloaded protections is by default according to the profile settings.

IPS, Anti-Virus and Anti-Bot updates are performed every two hours by default. Threat Emulation engine updates are performed daily at 05:00 by default, and Threat Emulation image updates are performed daily at 04:00 by default.

You can see the list of Anti-Bot and Anti-Virus protections in **Custom Policy Tools** > **Protections**, and the list of IPS protections in **Custom Policy Tools** > **IPS Protections**. The update date appears next to each protection.

Configuring Threat Prevention Scheduled Updates

To configure Threat Prevention scheduled updates:

1. In SmartConsole, go to the **Security Policies** page and select **Threat Prevention**.
2. In the **Custom Policy Tools** section of the Threat Prevention Policy, click **Updates**.
3. In the section for the applicable Software Blade, click **Schedule Update**.

   The **Scheduled Updates** window opens.
4. Make sure **Enable <blade> scheduled updates** is selected.
5. For IPS, there are 2 more configuration options for scheduling Security Management Server updates:

   - **On successful IPS update on the Security Management Server, install policy on the Security Gateway** - automatically installs the policy on the devices you select after the IPS update is completed. Click **Configure** to select these devices.

     Note - In pre-R80 gateways, IPS was part of the Access Control policy. Therefore, when you select this option, a message shows which indicates that for pre-R80 gateways, the Access Control policy is installed and for R80 and above gateways, the Threat Prevention policy is installed.
   - **Perform retries on the Security Management Server when the update fails** - lets you configure the number of tries the scheduled update makes if it does not complete successfully the first time.
6. Click **Configure**.
7. In the window that opens, set the **Time of event**:

   - **Update every**: set the update frequency by hours

OR:

- **Update at**: set the update frequency by days:
  - **Daily** - Every day
  - **Days in week** - Select days of the week
  - **Days in month** - Select dates of the month

8. Click **OK**.
9. Click **Close**.
10. In SmartConsole, install the policy.

Checking Update Status

In **Custom Policy Tools** > **Update**, a message shows which indicates the number of gateways which are up-to-date.

To check if the protections are update on a specific gateway:

1. In the **Gateways & Servers** view, select a gateway.
2. Click the **Monitor** button.

   The **Device & License Information** window opens.
3. The **Device Status** page shows the gateway status.

Updates - Threat Policy - IPS

What can I do here?

Use this window to view the progress of the IPS update.

Getting Here - SmartConsole > Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > IPS > Update now > Download using SmartConsole

Updating IPS Protections

Check Point constantly develops and improves its protections against the latest threats. You can immediately update IPS with real-time information on attacks and all the latest protections. You can manually update the IPS protections and also set a schedule when updates are automatically downloaded and installed. IPS protections include many protections that can help manage the threats against your network. Make sure that you understand the complexity of the IPS protections before you manually modify the settings.

Note - To enforce the IPS updates, you must install the Threat Prevention Policy.

To update IPS Protections:

1. In SmartConsole, click **Security Policies** > **Threat Prevention**.
2. In the **Custom Policy Tools** section, click **Updates**.
3. In the **IPS** section > **Update Now**, from the drop-down menu, select:
   - **Download with SmartConsole** - If your Security Management Server has no internet access.
   - **Download with Security Management Server**
   - **Offline Update** - If you want to manually upload the file. Select the required file for the update and click **Open**.
4. **Install Policy**.

Note - IPS purge runs automatically after every IPS update. The Security Management Server saves only the versions from the last 30 days, and deletes the others.

IPS Update Summary

What can I do here?

Use this window to see a summary of the IPS update.

Getting Here - Security Policies Threat Prevention > Policy > Custom Policy Tools > Updates > IPS > Update Now
Or:
Open Tasks window (F10) > Click Details under IPS Update

IPS Scheduled Update

What can I do here?

Use this window to:

- Enable scheduled updates for IPS
- Set a number of retries if update fails
- Configure a policy install after a successful update

Getting Here - Security Policies Threat Prevention > Policy > Custom Policy Tools > Updates > IPS > Schedule Update

Switch to Version

What can I do here?

Use this window to change the IPS Package to a previous version. This is useful when you experience problems with the updated version of the IPS package.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > IPS > Update Now > Switch to version

IPS Update - Follow Protections

What can I do here?

Use this window to mark updated protections with *Follow Up* flag.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > IPS > Follow Protections

IPS Protections Follow Up

The follow up mark lets you monitor specific IPS protections according to your selection. After you select the protections you wish to monitor, you can filter for them in the IPS Protections page and not have to search for them again.

To view protections marked for follow up:

In SmartConsole, go to **Security Policies** > **Threat Prevention** > **IPS Protections** > **Filters**, andselect **Follow Up**.

You can mark individual protections for follow up or mark all updated protections for follow up in the IPS Updates page.

Manually Marking Protections for Follow Up

You can mark individual protections for Follow Up, which lets you quickly review the identified protections in the **IPS Protections** page. To make the Follow Up feature efficient, make sure to keep the list of marked protections as short as possible. Mark newly downloaded protections and any protection that you want to monitor, but remember to remove protections from this list when you are more confident that you configured them in the best way for your environment, for now. The longer the Follow Up list is, the more difficult it is to use it as a workable task list

To manually mark protections for follow up:

In the **IPS Protections** page, select one or more protections, right-click and select **Follow Protection** from the menu.

To unmark the protection, right-click the protection and clear **Follow Protection**.

Each time the IPS protections are updated, they will be automatically marked for follow up. To unmark the protections for follow up, click **Unfollow Protections**. To unmark all marked protections, go to **Actions** > **Cleanup Options** > **Remove All Follow Up Flags**.

Note -You can add significant information about a protection in the protection's comment field. To add a comment to a protection, double-click a protection and enter you comment in the **Enter Protection Comment** field, below the protection's name. You can only add comments to ThreatCloud protections (and not Core protections). You can enter information such as the package version or date of update. Such information is useful because you can search for it at a later date.

Automatically Marking New Protections for Follow Up

Check Point provides new and updated protections as they become available (see *"Updating IPS Protections" on page 376*). To give you complete control over the process of integrating new IPS protections, you can have them automatically marked for Follow Up, which gives you time to evaluate the impact the protections have on your environment.

To have new protections marked automatically:

In SmartConsole > **Security Policies** > **Threat Prevention** > **Custom Policy Tools** > **Updates** > **IPS** >select **Follow Protections**.

Malware Database Scheduled Update

What can I do here?

Use this window to enable scheduled updates of the malware database. The scheduled update applies to Anti-Bot and Anti-Virus.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > Anti-Bot and Anti-Virus sections > Schedule Update

Threat Emulation Scheduled Update

What can I do here?

Use this window to schedule updates for the Threat Emulation engine and images.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > Threat Emulation > Schedule Update

Engine and Image updates

- **Update engine** - A group of small updates that is usually smaller than 1MB. These updates include: Threat Emulation engine, Static Analysis logic, malware rules, and a list of recommended images.
- **Update images** - Check Point updates the Threat Emulation images several times a year and each update is usually larger than 2GB. We recommend that you configure the update schedule for a time when the network is idle.

Updating Anti-Bot and Anti-Virus or Threat Emulation

What can I do here?

Use this window to schedule updates for:

- Anti-Bot and Anti-Virus
- Threat Emulation engine and images

Getting Here -
For Anti-Bot and Anti-Virus:
Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > Scheduled Update > Configure
For Threat Emulation engine and images
Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > Threat Emulation > Schedule Update > Enable Threat Emulation engine/Images scheduled update > Configure

Updating Threat Emulation

Threat Emulation connects to the ThreatCloud to update the engine and the operating system images. The default setting for the Threat Emulation appliance is to automatically update the engine and images.

. The default setting is to download the package once a day.

Best Practice - Configure Threat Emulation to download the package when there is low network activity.

Update packages for the Threat Emulation operating system images are usually more than 2GB. The actual size of the update package is related to your configuration.

To enable or disable Automatic Updates for Threat Emulation:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Custom Policy Tools** section, click **Updates**.

The **Updates** page opens.

3. Under Threat Emulation, click **Schedule Update**.
4. Select or clear these settings:
   - **Enable Threat Emulation engine scheduled update**
   - **Enable Threat Emulation images scheduled update**
5. Click **Configure** to configure the schedule for Threat Emulation engine or image updates.
6. Configure the automatic update settings to update the database:
   - To update once a day, select **At** and enter the time of day
   - To update multiple times a day, select **Every** and set the time interval
   - To update once or more for each week or month:
   a. Select **At** and enter the time of day.
   b. Click **Days**.
   c. Click **Days of week** or **Days of month**.
   d. Select the applicable days.
7. Click **OK** and then install the Threat Prevention Policy.

Image Update

What can I do here?

Use this window to select a gateway on which to update the images.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Updates > Threat Emulation > Update Images

Updating Threat Emulation Images

Update packages for the Threat Emulation operating system images are usually more than several Gigabytes. The actual size of the update package is related to your configuration.

The default setting is to download the package once a week on Sunday. If Sunday is a work day, we recommend that you change the update setting to a non-work day.

To update the operating system image for Threat Emulation on a gateway:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Custom Policy Tools** section, click **Updates**.

The **Updates** page opens.

3. Under Threat Emulation, click **Update Images**.
4. Select a gateway and click **OK**.
5. Install the Threat Prevention policy.

Protections

What can I do here?

Use this window to see a list of protections.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Protections

Whitelist Files

What can I do here?

Use this window to specify files that the Threat Prevention blade does not scan or analyze.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Whitelist Files

Using the Whitelist

Whitelist is a list of files that are trusted. Check Point Threat Prevention engine does not inspect trusted files for malware, viruses, and bots, which helps decrease resource utilization on the gateway.

Whitelist File - New

What can I do here?

Use this window to create a new whitelist file.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Whitelist Files > New Whitelist file

Adding a File to the Whitelist

To configure files on the Threat Prevention Whitelist:

1. In SmartConsole, click **Security Policies** > **Threat Prevention** > **Policy** > **Custom Policy Tools** > **Whitelist Files**.
2. Click **New**.

   The **Whitelist File** window opens.
3. Enter the **Object Name** and **MD5 signature** for the new file exception.

   Note - To edit or remove Whitelist files, right-click the file and select the applicable option.
4. Click **OK**.
5. Install the Threat Prevention policy.

Threat Indicators

What can I do here?

Use this window to create or edit Threat Indicators.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Indicators

Configuring Threat Indicators

Threat Indicators lets you add feeds to the Anti-Bot and Anti-Virus engines, in addition to the feeds included in the Check Point packages and ThreatCloud feeds. You can create your own threat indicator files or import them from external sources. You can upload the files both through SmartConsole and through the CLI.

An Indicator is a set of observables which represent a malicious activity in an operational cyber domain, with relevant information on how to interpret it and how to handle it.

An Observable is an event or a stateful property that can be observed in an operational cyber domain. Such as: IP address, MD5 file signature, SHA1 file signature, SHA256 file signature, URL, Mail sender address.

Threat Indicators demonstrate an attack by:

- Specific observable patterns
- Additional information intended to represent objects and behaviors of interest in a cyber-security context

Indicators are derived from intelligence, self-analysis, governments, partners, and so on.

Supported Indicator Files

Each record in CSV Check Point format and the STIX XML (STIX 1.0) format must have these fields:

Fields

Field	Description	Valid Values	Value Criteria	Field Type
`UNIQ-NAME`	Name of the observable	Free text	Must be unique	Mandatory
`VALUE`	A valid value for the type of the observable	As provided in this table	Value of parameter	Mandatory

Field	Description	Valid Values	Value Criteria	Field Type
TYPE	Type of the observable	URL	Any valid URL Not case-sensitive	Mandatory
		Domain	Any URL Domain	
		IP	Standard IPv4 address	
		IP Range	A range of valid IPv4 addresses, separated by a hyphen: <IP1>-<IP2>	
		MD5	Any valid MD5 hash	
		SHA1	Any valid SHA1 hash	
		SHA256	Any valid SHA256 hash	
		Mail-subject	Any non-empty text string	
		Mail-from	Can be one of these: ■ A single email address Example: abc@domain.com ■ An email domain Examples: @domain.com, or domain.com	
		Mail-to	Can be one of these: ■ A single email address Example: abc@domain.com ■ An email domain Examples: @domain.com, or domain.com	

Field	Description	Valid Values	Value Criteria	Field Type
		`Mail-cc`	Can be one of these: ■ A single email address Example: `abc@domain.com` ■ An email domain Examples: `@domain.com`, or `domain.com`	
		`Mail-reply-to`	Can be one of these: ■ A single email address Example: `abc@domain.com` ■ An email domain Examples: `@domain.com`, or `domain.com`	
`CONFIDENCE`	Degree of confidence the observable presents	■ `low` ■ `medium` ■ `high` ■ `critical`	Default - `high`	Optional
`SEVERITY`	Degree of threat the observable presents	■ `low` ■ `medium` ■ `high` ■ `critical`	Default - `high`	Optional

Field	Description	Valid Values	Value Criteria	Field Type
PRODUCT	Check Point Software Blade that processes the observable	■ AV ■ AB	■ AV - Check PointAnti-VirusSoftware Blade (default) **Note** - Only the Anti-VirusSoftware Blade can process MD5, SHA1, and SHA256 observables. ■ AB - Check PointAnti-BotSoftware Blade	Optional
COMMENT		Free text		Optional

Notes

- If an optional field is empty, the default value is used.
- If a mandatory field is empty, the Indicator file does not load.
- STIX 2.0 (JSON file) is not supported.
- Custom Indicators CLI (`load_indicators`) are not supported.
- The supported STIX elements are:

```
stix:STIX_Package
stix:STIX_Header
stix:Title
stix:Description
stix:Indicators
stix:Indicator
indicator:Title
indicator:Type
indicator:Description
indicator:Observable
cybox:Object
cybox:Properties
FileObj:Hashes
cyboxCommon:Hash
cyboxCommon:Type
cyboxCommon:Simple_Hash_Value
stix:Observables
cybox:Observable
URIObj:Value
URIObject:Value
AddressObject:Address_Value
AddressObj:Address_Value
AddressObj:AddressObjectType
AddressObjet:AddressObjectType
cybox:Title
```

Condition Type Enum and **Condition Application Enum** support the values **Equals** and **Any**.

Example:

```
<cyboxCommon:Simple_Hash_Value condition="Equals" apply_
condition="ANY">
```

Syntax rules of CSV Indicator files in Check Point format

- Use commas to separate the fields in a record
- Enter one record per line, or use '\n' to separate the records
- If free text contains quotation marks, commas, or line breaks, it must be enclosed in quotation marks
- To enclose part of free text in quotations, use double quotation marks: "<text>"

Example of a CSV Indicator File in Check Point format

```
#! DESCRIPTION = indi file,,,,,,
"#! REFERENCE = Indicator Bulletin; Feb 20, 2014",,,,,,
# FILE FORMAT:,,,,,,
"# All lines beginning ""#"" are comments",,,,,,
"# All lines beginning ""#!"" are metadata read by the SW",,,,,,
"# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT",,,,,,
observ1,8d9b6b8912a2ed175b77acd40cbe9a73,MD5,medium,medium,AV,FILENAME:WUC
 Invitation Letter Guests.doc
observ2,76700f862a0c241b8f4b754f76957bda,MD5,high,high,AV,FILENAME:essais~.swf|
NOTE:FWS type Flash file
observ4,5dda6d1446b3cdb0bd4a3f0adb85d030ff59e975,SHA1,low,high,AV,file_name.pdf
observ5,db435a875be456f088f11c579aa52f30bc83cfff272cfad5a3f6f4de74de0654,SHA256,high,high,AV,file_name.doc
observ7,http://somemaliciousdomain.com/uploadfiles/upload/exp.swf?info=
789c333432d333b4d4b330d133b7b230b03000001b39033b&infosize=00840000
,URL,high,high,AV,IPV4ADDR:196.168.25.25
observ8,svr01.passport.ServeUser.com,Dpmain,low,high,AB,TCP:80|
IPV4ADDR:172.18.18.25|NOTE:Embedded EXE Remote C&C and Encoded Data
observ9,somemaliciousdomain2.com,Domain,,low,AV,TCP:8080|IPV4ADDR:172.22.14.10
observ10,http://www.bogusdomain.com/search?q=%24%2B%25&form=MOZSBR&pc=
MOZI,URL,low,low,AB,IPV4ADDR:172.25.1.5
observ11,http://somebogussolution.com/register/card/log.asp?isnew=-1&LocalInfo=
Microsoft%20Windows%20XP%20Service%20Pack%202&szHostName=
ADAM-E512679EFD&tmp3=tmp3,URL,medium,,AB,
observ14,172.16.47.44,IP,high,medium,AB,TCP:8080
observ15,172.16.73.69,IP,medium,medium,AV,TCP:443|NOTE:Related to Flash
exploitation
observ16,abc@def.com,mail-to,,high,AV,"NOTE:truncated; samples have appended to
the subject the string ""PH000000NNNNNNN"" where NNNNNNN is a varying number"
observ34,stamdomain.com,domain,,,AB,
observ35,stamdomain.com,mail-from,high,medium,AV,
observ37,xyz.com,mail-from,medium,medium,AB,
observ38,@xyz.com,mail-from,medium,medium,AB,
observ39,a@xyz.com,mail-from,medium,medium,AB,
```

Example of a STIX 1.0 XML Indicator File

```
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#FileObject-2 ../cybox/objects/File_Object.xsd
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd"
    id="example:STIXPackage-ac823873-4c51-4dd1-936e-a39d40151cc3"
    version="1.0.1">
    <stix:STIX_Header>
        <stix:Title>Example file watchlist</stix:Title>
        <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators -
Watchlist</stix:Package_Intent>
    </stix:STIX_Header>
    <stix:Indicators>
        <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-611935aa-
4db5-4b63-88ac-ac651634f09b">
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">File Hash
Watchlist</indicator:Type>
            <indicator:Description>Indicator that contains malicious file
hashes.</indicator:Description>
            <indicator:Observable id="example:Observable-c9ca84dc-4542-4292-af54-
3c5c914ccbbc">
                <cybox:Object id="example:Object-c670b175-bfa3-48e9-a218-aa7c55f1f884">
                    <cybox:Properties xsi:type="FileObj:FileObjectType">
                        <FileObj:Hashes>
                            <cyboxCommon:Hash>
                                <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0"
condition="Equals">MD5</cyboxCommon:Type>
                                <cyboxCommon:Simple_Hash_Value condition="Equals" apply_
condition="ANY">0522e955aaee70b102e843f14c13a92c##comma##0522e955aaee70b102e843f14c13a92d##co
mma##0522e955aaee70b102e843f14c13a92e</cyboxCommon:Simple_Hash_Value>
                            </cyboxCommon:Hash>
                        </FileObj:Hashes>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Threat Indicators - Importing a File

What can I do here?

Use this window to import a file of Threat Indicators

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Indicators > New/edit > Import File

Importing Threat Indicator Files through SmartConsole

When you manually upload threat indicator files through SmartConsole, the files must be in a CSV Check Point format or STIX XML (STIX 1.0) format. The files must contain records of equal size. If an Indicator file has records which do not have the same number of fields, it does not load.

Syntax rules of CSV Indicator files in Check Point format

- Use commas to separate the fields in a record
- Enter one record per line, or use '\n' to separate the records
- If free text contains quotation marks, commas, or line breaks, it must be enclosed in quotation marks
- To enclose part of free text in quotations, use double quotation marks: "<text>"

To load Indicator files through SmartConsole

Note - To load indicators in Custom Threat Prevention policy, before you start, you must go to the applicable profile > Indicators, and make sure that **Enable indicator scanning** is selected.

Step	Instructions
1	In the SmartConsole main view, go to **Security Policies** > **Threat Prevention** > **Custom Policy /Autonomous Policy** > **Custom Policy Tools/Autonomous Policy Tools** > **Indicators**. The **Indicators** page opens.
2	Click **New**, and select **Import file**. The **Indicator** configuration window opens.
3	Enter a **Name**. Each Indicator must have a unique name.
4	**Enter Object Comment** (optional).
5	Click **Import** to browse to the Indicator file. The content of each file must be unique. You cannot load duplicate files.

Step	Instructions
6	**Select an action for this Indicator** ■ **Ask** - Threat Prevention Software Blade asks what to do with the detected observable ■ **Prevent** - Threat Prevention Software Blade blocks the detected observable ■ **Detect** - Threat Prevention Software Blade creates a log entry, and lets the detected observable go through ■ **Inactive** - Threat Prevention Software Blade does nothing
7	**Add Tag**.
8	Click **OK**. If you leave an *optional* field empty, a warning notifies you that the default values are used in the empty fields. Click **OK**. The Indicator file loads.
8	Install the Threat Prevention Policy.

To delete Indicators

Step	Instructions
1	Select an *Indicator*.
2	Click **Delete**.
3	In the window that opens, click **Yes** to confirm.

You can edit properties of an Indicator object, except for the file it uses. If you want an Indicator to use a different file, you must delete it and create a new one.

Threat Indicators - External IoC feed

What can I do here?

Use this window to create an External IoC feed.

Getting Here - Security Policies > Threat Prevention > Policy > Custom Policy Tools > Indicators > New/edit > External IOC feed.

Importing External Custom Intelligence Feeds through SmartConsole

Custom Intelligence Feeds lets you fetch feeds from a third-party server directly to the Security Gateway to be enforced by the Anti-Virus and Anti-Bot blades. The Custom Intelligence Feeds feature helps you manage and monitor indicators with minimal operational overhead.

To import an external IoC feed

Note - To load indicators in Custom Threat Prevention policy, before you start, you must go to the applicable profile > **Indicators**, and make sure that **Enable indicator scanning** is selected.

Step	Instructions
1	In the SmartConsole main view, go to **Security Policies** > **Threat Prevention** > **Custom Policy/Autonomous Policy**.
2	In the bottom left section, go to **Custom Policy Tools/Autonomous Policy Tools** > **Indicators**.
3	Click **New** and select **External IoC feed**. The **Indicator feed** configuration window opens.
4	Enter these details: ■ A feed name - Each indicator must have a unique name. ■ Enter the **Feed URL** ■ Select an **Action** for this Indicator • **Prevent** - Threat Prevention Software Blade blocks the detected observable • **Detect** - Threat Prevention Software Blade creates a log entry, and lets the detected observable go through You can disable the feed, if you clear the **Active** checkbox. ■ You can use a Security Gateway proxy for connection.
5	In the **Authentication**, enter the applicable username and password, if the external feed requires authentication.
6	If the feed is not in Check Point CSV format, click **Custom feed settings** to adjust it to your needs. See sk132193 for instructions. Custom feed settings are disabled by default.
7	Configure the settings in **Fields to Column number mappings**.
8	Click **Test Connectivity** to check if the feed runs properly.

Step	Instructions
9	Click **OK**. The new indicator shows in the **Indicators** page.
10	Install the Threat Prevention Policy.

The feeds defined will be fetched every 30 minutes and enforced immediately on the gateway with no need to install a Policy.

To change the fetching interval, go to **Manage & Settings** > **Blades** > **Threat Prevention** > **Advanced Settings**, go to **External Feed**, and select the applicable interval.

Limitations

- External Indicators of Compromise (IoC) added in SmartConsole are supported only on Security Gateways R81 and higher.
- IoC feeds are fetched on all connections and are not affected by Threat Prevention Policy.
- Policy installation does not fail if a feed is inaccessible. In this case, the Security Gateway only generates a control log can be seen in the **Logs** view.

Data Center

What can I do here?

Use this window to create or edit these types of Data Center:

- Cisco ACI
- Cisco ISE
- Google Cloud Platform
- Kubernetes
- AWS
- Microsoft Azure
- VMware NSX
- OpenStack
- VMware vCenter
- Nuage
- VMware NSX-T

- Generic Data Center
- IoT Cloud Adapter

Getting Here - SmartConsole > Objects > More object types > Cloud > Data Center

Data Center Object

What can I do here?

Use this window to view the details about a certain Data Center object, and edit the object name, comment, or color.

Getting Here - SmartConsole > Objects Bar > Object Categories > Data Center Objects > Right-click on object > Edit

Select Data Center Objects

What can I do here?

Use this window to view and search objects in the selected Data Center, and select objects to use in the rule base.

Getting Here - SmartConsole > Access Control > Policy > Source/Destination column > Add new items -Plus sign (+) in the rule base where you want to add Data Center object > Import > Select the Data Center server

Available Data Centers

What can I do here?

Use this window to select an available Data Center.

Note - This window shows only after you have created five or more Data Center objects.

Getting Here - Security Policies > Access Control > Policy > Source or Destination Column > Add new items > Import > more

Data Center Queries

What can I do here?

Use this window to query a Data center.

Getting Here - SmartConsole > Objects > More object types > Cloud > New Data Center Query

Data Center Query Objects

With the Data Center Query Objects, administrators can now create a single **Query Object** based on attributes across multiple data centers. This simplifies the work when administrators create policies for multiple rules, because they only need to **use one query object for data center objects from multiple data centers**. Furthermore, admins can create the policy even before they configure a data center in SmartConsole. This makes it easier to separate responsibilities between security admins and others teams that may need to create data centers in SmartConsole.

The new Query object is used in the same way as Data Center objects. As with Data Center Objects, once the Data Center Query is added to the Rule base the CloudGuard Controller pulls the assets from all the Data Centers in the query object and updates the Security Gateway so.

Without Data Center Query	With Data Center Query
■ Must first create the Data Center account (s) ■ Must then import objects from each Data Center to the Rule base ■ No choice for complex logic inside the rules	■ Create Data Center Query and add them to the rule base **before** you create Data Center account(s). This creates an advantage when more than one department may add Data Centers in SmartConsole. For example, if DevOps needs to add a Data Center in SmartConsole then they can do so without having to work with the Rule base. This makes for a better separation of responsibilities. ■ A single Data Center Query Object can use assets (objects) from more than one, or all, Data Centers. This results in simpler security rules. ■ The Query is more complex and larger than what can be done in the security rule's logic. ◦ `OR` logic inside each query rule ◦ `AND` logic between query rules

Example 1: Data Center Query Object

Applies to all current and future data centers

This is the query logic:

- All assets from type instances `OR` Load Balancers

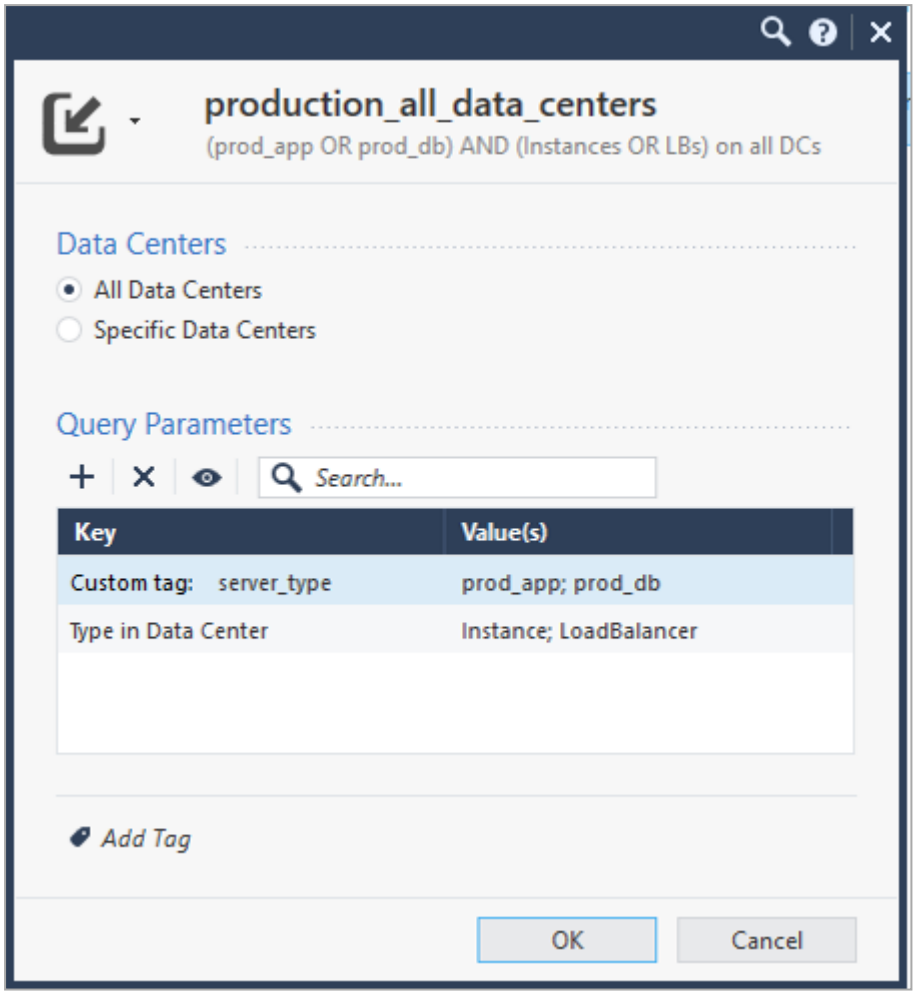
  AND

- Tagged with:

  `"server_type=prod_app"`

OR

```
"server_type=prod_dp"
```



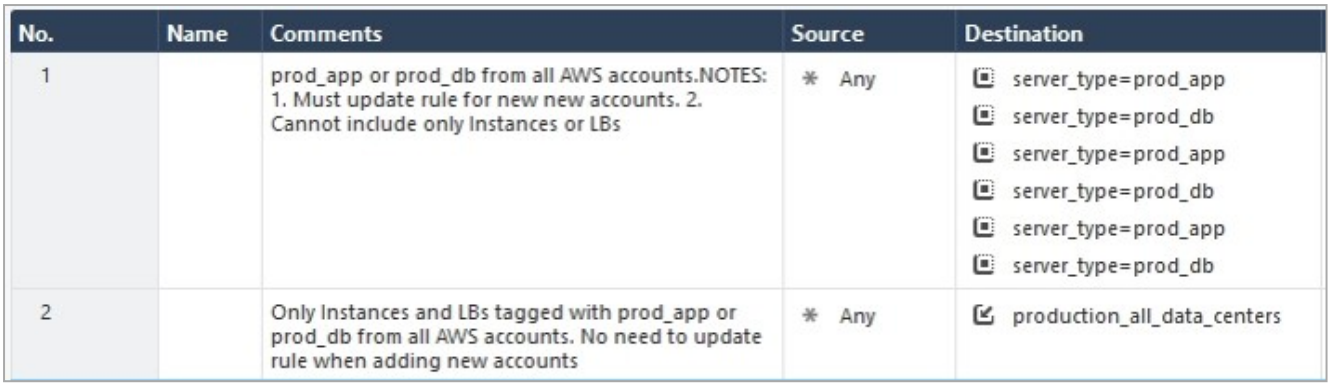
Example 2: Rule Base

Earlier versions required using tag objects for multiple accounts.

- Rules must be must be updated for every data center added.
- Rules cannot have the logic for only Instances or Load Balancers.

R81.10 uses Data Center Query objects:

- No need to update the rule when adding new data centers.
- Rule can include complex `OR` and `AND` operations to better the policy.



No.	Name	Comments	Source	Destination
1		prod_app or prod_db from all AWS accounts.NOTES: 1. Must update rule for new new accounts. 2. Cannot include only Instances or LBs	* Any	server_type=prod_app server_type=prod_db server_type=prod_app server_type=prod_db server_type=prod_app server_type=prod_db
2		Only Instances and LBs tagged with prod_app or prod_db from all AWS accounts. No need to update rule when adding new accounts	* Any	production_all_data_centers

Prerequisites:

1. Configure the Security Gateway with the Identity Awareness Blade and enable the **Web API**.

   See "Activating Identity Awareness for Security Gateways R80.10 and above" in the *R81.10 CloudGuard Controller Administration Guide*.

2. Create Data Centers Server objects in SmartConsole.

   To create data centers, see "Connecting to a Data Center Server" in the *R81.10 CloudGuard Controller Administration Guide*.

Supported Security Gateways:

- R80.10 and above

How to Configure Data Center Query Objects in SmartConsole

Step 1: Create a Data Center Query Object.

a. Go to SmartConsole > **New** > **Cloud** > **Data Center Queries**.

b. Add the relevant Data Center(s).

c. Configure the **Value** to match the value used for **Type**, **Name**, and **IP** in the **Import Data Center** window.

Type in Data Center	*Type* in Data Center, such as Instance, Virtual Machine, Load Balancer, Subnet, Availability Zone, and more.
Name in Data Center	The asset's name
IP address	The asset's IP address
Customer tag	Free text key and value

Note - All object IP addresses that match the query are updated on the Security Gateway.

d. Click **OK**.

Step 2: Add the Data Center Query object from Step 1 to the Access Control policy.

Step 3: Install the Security Policy on the Security Gateway.

Updatable Objects

What can I do here?

Use this window to import objects that will be automatically updated from external cloud services.

Getting Here - Security Policies > Access Control > Policy > Source or Destination column > Add button > Import > Updatable Objects
Or:
HTTPS Inspection > Policy > Source or Destination column > Add button > Import > Updatable Objects
Or:
Threat Prevention > Custom Policy > Protected Scope > Add button > Import > Updatable Objects

Updatable Objects

An updatable object is a network object which represents an external service, such as Office 365, AWS, GEO locations and more. External services providers publish lists of IP addresses or Domains or both to allow access to their services. These lists are dynamically updated. Updatable objects derive their contents from these published lists of the providers, which Check Point uploads to the Check Point cloud. The updatable objects are updated automatically on the Security Gateway each time the provider changes a list. There is no need to install policy for the updates to take effect. You can use an updatable object in the Access Controlor HTTPS Inspection policy as a source or a destination, or in the Threat Prevention policy as the Protected Scope.

For more on updatable objects and list of objects currently supported, see: sk173416.

Note - This feature is only supported for R80.20 and above gateways.

Use Case - Adding an Updatable Object to the Access Control Security Policy

A customer uses Office365 and wants to allow access to Microsoft Exchange services.

To add the Microsoft Exchange Updatable Object to the Security Gateway:

1. Make sure the Security Management Server and the Security Gateway have access to the Check Point cloud.
2. Go to SmartConsole > **Security Policies** > **Access Control** > **Policy**.
3. Create a new rule.
4. In the Destination column, click the + sign and select **Import** > **Updatable Objects**.

   The **Updatable Objects** window opens.
5. Select the objects to add. For this use case, select the **Exchange Services** object.

   Note - You can also add objects to the **Source** column.
6. Click **OK**.
7. Install policy.

The Exchange Services object is added to the Rule Base.

No	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Accept Exchange	WirelessZone	Exchange Services	Any	Any	Accept	Log
2	Accept Exchange	Exchange Services	WirelessZone	Any	Any	Accept	Log

You can monitor the updates in the **Logs & Monitor** > **Logs** view.

To monitor the updates:

1. Go to SmartConsole > **Logs & Monitor**.
2. From the search bar, enter **Updatable Objects**.
3. Double-click the relevant log.

   The **Log Details** window shows.
4. `Succeeded` shows in the **Status** field when the update is successful.

Updatable Object

What can I do here?

Use this window to see a definition of the Updatable Object used in the source or destination column of the Security Policy.

For more, see: *"Updatable Objects" on page 398*

Getting Here - Security Policies > Access Control > Policy > Source or Destination column > Click the + sign > Import > Updatable Objects
or Security Policies > Threat Prevention > Policy > Protected Scope column > Click the + sign > Import > Updatable Objects
or Security Policies > HTTPS Inspection > Policy > Source or Destination column > Click the + sign > Import > Updatable Objects

Logs & Monitor

What can I do here?

In this window you can open views that show you security events, logs, audit logs, and regulation compliance

Getting Here - Logs & Monitor

SmartEvent

What can I do here?

In these windows you can see the most important recent security events and logs.

You can customize the view or report , and click to drill down and see details.

Using the **Actions** menu, selected reports can be shared with other administrators, cloned, copied, renamed or deleted.

Getting Here -
Logs & Monitor > New Tab (click +)
Important - The views can also be accessed through a web browser at:
`https://<IP address of Management Server>/SmartView/`

SmartEvent Views

There are three SmartEvent views:

View	Description
General Overview	By default you can see for the past 7 days: ■ Security incidents, number of infected hosts, and the number of high risk attacks ■ Attack destinations ■ Top high risk applications
Access Control	Shows the Access Control events.
Threat Prevention	Shows the Threat Prevention events.

Event Analysis with SmartEvent

The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents, and do the necessary actions to prevent more attacks. You can customize the views to monitor the events that are most important to you. You can move from a high level view to detailed forensic analysis in a few clicks. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events.

Log Exporter

What can I do here?

Use this window to select or create a Log Exporter.

The Log Exporter exports Gateway logs to syslog/SIEM servers

What background information do I need to know?

> **Getting Here:**
> Gateways & Servers > Management Server > Logs > Export
> or:
> Gateways & Servers > Dedicated Log Server > Logs > Export

Understanding Log Exporter

Log Exporter is a multi-threaded daemon service which runs on a log server. The Log Exporter daemon reads each log, transforms it into the desired format and mapping, and sends it to the configured target.

On Multi-Domain Server / Multi-Domain Log Server, if Log Exporter is deployed on several Domains, each Domain Server has its own Log Exporter daemon service. If you export the logs to several targets, each target has its own Log Exporter daemon.

Log Exporter is implemented as the "**E-T-L**" procedure:

- **Extract** - Reads incoming logs from itself, the Log Server / SmartEvent Server of the Security Gateways.
- **Transform** - Changes the logs according to the configuration.
- **Export** - Sends the logs to the configured target server.

Log Exporter stops exporting when disconnected from the 3rd party server and remembers the last position exported. After the connection is established again, Log Exporter automatically starts exporting logs from the last known position. Log Exporter is exporting both online and offline (if any) logs in parallel. In case the 3rd party server is slow, Log Exporter reduces the offline exporting rate to prioritize the online logs over the offline logs.

For more, see: *R81.10 Logging and Monitoring Administration Guide*.

Log Exporter - General

What can I do here?

Use this window to configure a target server.

Getting Here - Gateways & Servers > Gateway > Gateway Properties > Logs > Export > New Log exporter/SIEM > General

or:

Gateways & Servers > Management Server > Logs > Export > New Log exporter/SIEM > General

Log Exporter - Data Manipulation

What can I do here?

Use this window to configure a format for the exported logs.

Getting Here - Gateways & Servers > Gateway > Gateway Properties > Logs > Export > New Log exporter/SIEM > Data Manipulation

or:

Gateways & Servers > Management Server > Logs > Export > New Log exporter/SIEM > Data Manipulation

Log Exporter - Attachments

What can I do here?

Use this window to attach links to the logs.

Getting Here - Gateways & Servers > Gateway > Gateway Properties > Logs > Export > New Log exporter/SIEM > Attachments

or:

Gateways & Servers > Management Server > Logs > Export > New Log exporter/SIEM > Attachments

Logs

What can I do here?

Use this window to see logs from all Security Gateways. The logs are stored on the Security Management Server and Log Servers.

Getting Here -
Logs & Monitor > Open Log View

Log Analysis

SmartConsole lets you transform log data into security intelligence. Search results are fast and immediately show the log records you need. The Security Gateways send logs to the Log Servers on the Security Management Server or on a dedicated server. Logs show on the SmartConsole **Logs & Monitor > Logs** tab.

You can:

- Quickly search through logs with simple Google-like searches.
- Select from many predefined search queries to find the applicable logs.
- Create your own queries using a powerful query language.
- Monitor logs from administrator activity and connections in real-time.

Enabling Log Indexing

Log indexing on the Security Management Server or Log Server reduces the time it takes to run a query on the logs. Log indexing is enabled by default.

In a standalone deployment, log indexing is disabled by default. Enable log indexing only if the standalone computer CPU has 4 or more cores.

To manually enable Log Indexing:

1. Open SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Management Server or Log Server object.

   The **General Properties** window opens.
3. In the **Management** tab, select **Logging & Status**.
4. From the navigation tree, click **Logs**.
5. Select **Enable Log Indexing**.
6. Click **OK**.
7. Publish the SmartConsole session.
8. From **Menu**, select **Install Database**.

Customizing the Results Pane

By default, SmartConsole shows a predefined set of columns and information based on the selected blade in your query. This is known as the **Column Profile**. For example:

- The DLP column profile includes columns for: Blade, Type, DLP Incident UID, and severity.
- The Threat Prevention column profile includes columns for: Origin, Action, Severity, and Source User.

A column profile is assigned based on the blade that occurs most frequently in the query results. This is called **Automatic Profile Selection**, and is enabled by default.

The Column Profile defines which columns show in the **Results Pane** and in which sequence. You can change the Column Profile as necessary for your environment.

To use the default Column Profile assignments:

- Right-click a column heading and select **Columns Profile** > **Automatic Profile Selection**.

To manually assign Column Profile assignments by default:

- Right-click a column heading and select **Columns Profile** > **Manual Profile Selection**.

To manually assign a different Column Profile:

1. Right-click a column heading and select **Columns Profile**.
2. Select a Column Profile from the options menu.

To change a Column Profile:

1. Right-click a column heading and select **Columns Profile** > **Edit Profile**.
2. In the **Show Fields** window, select a Column Profile to change.
3. Select fields to add from the **Available Fields** column.
4. Click **Add**.
5. Select fields to remove from the **Selected Fields** column.
6. Click **Remove**.
7. Select a field in the **Selected Fields**.
8. Click **Move Up** or **Move Down** to change its position in the **Results** Pane.
9. Double-click the Width column to change the default column width for the selected field.
10. To change the column width, drag the right column border in the **Results** Pane.
11. To save the column width, right-click and select **Save Profile**.

    The column is applicable to future sessions.

Viewing Rule Logs

You can search for the logs that are generated by a specific rule, from the Security Policy or from the Logs & Monitor > **Logs** tab.

To see logs generated by a rule (from the Security Policy):

1. In SmartConsole, go to the **Security Policies** view.
2. In the **Access Control Policy** or **Threat Prevention Policy**, select a rule.
3. In the bottom pane, click one of these tabs to see:
   - **Summary** - Rule name, rule action, rule creation information, and the Hit Count. Add custom information about the rule.
   - **Details** (Access Control Policy only) - Details for each column. Select columns as necessary.
   - **Logs** - By default, shows the logs for the *Current Rule*. You can filter them by **Source**, **Destination**, **Blade**, **Action**, **Service**, **Port**, **Source Port**, **Rule** (**Current rule** is the default), **Origin**, **User**, or **Other Fields**.

- **History** (Access Control Policy only) - List of rule operations in chronological order, with the information about the rule type and the administrator that made the change.

To see logs generated by a rule (by Searching the Logs):

1. In SmartConsole, go to the **Security Policies** view.
2. In the **Access Control Policy** or **Threat Prevention Policy**, select a rule.
3. Right-click the rule number and select **Copy Rule UID**.
4. In the Logs & Monitor > **Logs** tab, search for the logs in one of these ways:
   - Paste the Rule UID into the query search bar and press Enter.
   - For faster results, use this syntax in the query search bar:

     ```
     layer_uuid_rule_uuid:*_<UID>
     ```

     For example, paste this into the query search bar and press Enter:

     ```
     layer_uuid_rule_uuid:*_46f0ee3b-026d-45b0-b7f0-5d71f6d8eb10
     ```

Dynamic Log Distribution

With Dynamic Log Distribution, you can configure the gateway to distribute logs between the active Log Servers. Previously, each Log Server received a copy of every log. If one Log Server was disconnected, the gateway connected to the backup server and sent it a copy of every log. Now you can configure that each log is sent to only one Log Server and distribute the logs between the primary Log Servers. If all the primary servers are disconnected, logs are distributed between backup Log Servers. If no Log Servers are connected, the gateway writes the logs locally.

Use Case - Log distribution reduces the need for high resources on the Log Servers and the load on a specific gateway connection, and reduces the need for high CPU and disk resources:

- The gateway writes logs locally due to a high log rate.
- The load on a specific Log Server is very high.

To configure log distribution between multiple Log Servers

1. In SmartConsole, open the gateway object and select Logs > Log Distribution.
2. For Logs Distribution, select **Distribute logs between log servers for improved performance (applies to primary and backup log servers)**.
3. Select the primary and backup Log Servers.

4. Click **OK**.
5. Install the policy.

Getting Here - Open the gateway object > Logs > Log Distribution
Logs & Monitor > Open Log View

Audit Logs

What can I do here?

Use this window to see the audit logs from all Security Gateways. The logs are stored on the Security Management Server and Log Servers.

Audit logs capture workflow operations for tracking and troubleshooting. Use them to track and analyze changes to the security and network environment.

Getting Here -
Logs & Monitor > Open Audit Log View

Understanding Logging

Security Gateways generate logs, and the Security Management Server generates audit logs . The Security Policy that is installed on each Security Gateway determines which rules generate logs.

Logs can be stored on a:

- Security Management Server that collects logs from the Security Gateways. This is the default.
- Log Server on a dedicated machine. This is recommended for organizations that generate a lot of logs.
- Security Gateway. This is called local logging.

To find out how much storage is necessary for logging, see the new appliance datasheet.

In a Multi-Domain Security Management environment, the Security Gateways send logs to the Domain Management Server or to dedicated Domain Log Servers. The Multi-Domain Server generates logs, and they can be stored on the Multi-Domain Server or on a dedicated Multi-Domain Log Server. To learn how to deploy logging in a Multi-Domain Security Management environment, see the *R81.10 Multi-Domain Security Management Administration Guide*

To learn how to monitor the Log Receive Rate on the Security Management Server / Log Server in R80 and higher, see sk120341.

To decrease the load on the Security Management Server, you can install a dedicated Log Server and configure the gateways to send their logs to this Log Server. To see the logs from all the Log Servers, connect to the Security Management Server with SmartConsole, and go to the **Logs & Monitor** view **Logs** tab.

A Log Server handles log management activities:

- Automatically starts a new log file when the existing log file gets to the defined maximum size.
- Handles backup and restore for log files.
- Stores log files for export and import.
- Makes an index of the logs. Therefore, log queries work quickly.

Compliance

What can I do here?

In this view you can optimize your security settings and ensure compliance with regulatory requirements.

Getting Here - Logs & Monitor > Open Compliance View

Compliance - Action Items

What can I do here?

Use this window to see a list of Action items and messages.

Getting Here - Logs & Monitor > Open Compliance View > Action Items and Messages > click on a Pending action item or Unscheduled items.

Compliance - Action Items and Messages

What can I do here?

Use this window to view compliance action items and messages.

Getting Here - Logs & Monitor > Open Compliance View > Action Items and Messages > click on the "See All" link.

Compliance Regulatory Report

What can I do here?

Use this window to view the generated report.

> **Getting Here** - Logs & Monitor > Open Compliance View > Regulatory compliance > Open a regulation > Click Generate Report

Compliance Alerts

If you want to get a compliance alert, you must manually rescan for changes after updating one of the Threat Prevention profiles.

To rescan:

1. Open Manage & Settings > Blades > Compliance > Settings.
2. Click **Rescan**.

If the change is not recommended, a compliance security alert will show in Tasks.

For example, best practice IPS105 states: *The IPS Policy should have Server Protections automatically activated for each profile*.

If you:

1. Create a new profile in Threat Prevention.
2. Open the **IPS** page > **Pre R80 Settings**.
3. Clear **Server protections**.
4. Publish.
5. Rescan.

An alert will show in Tasks.

Security Best Practices

What can I do here?

Use this window to activate or deactivate Security Best Practices relevant to your organization.

> **Getting Here** - Logs & Monitor > Open Compliance View > Security Best Practices Compliance > See all

Best Practice Types

The Check Point Compliance Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration. A Security Best Practice is related to specified regulations in different regulatory standards. It tells you about your compliance status and recommends corrective steps.

Types of Security Best Practices

- **Global** - Examines the configuration settings for all of the organization.
- **Object-based** - Examines the configuration settings for specified objects (gateways, profiles and other objects).

Search and Export Fields

- **Type to Search** - Enter search criteria to show only those results that match specified criteria. You can do a free text search for criteria in all fields or search for values in a specified field.
- **Grouping** - Select a value to show the results in groups of a specified.

Pane Sections

- **Best Practice Details** - Name of the Security Best Practice, status, score, and other data.
- **Description and Action Items** - Detailed description of the selection, with its action item (if there is one).
- **Relevant Objects** - Objects related to the selected and their status. You can activate or deactivate enforcement of the selected Security Check for specific objects. This section shows only when the selected Security Best Practice is applicable to specific objects.
- **Relevant Regulatory Requirements** - List of regulatory standards that include the selected Security Best Practice.

Widget Settings

What can I do here?

In this window you can define widgets. Widgets are a representation of the collected data. There can be different combinations of types, fields, operations, groups, filters, and settings for each widget. You can quickly create the graphical view of security in your organization that best meets your requirements.

Getting Here -
Logs & Monitor > General Overview > Options > Edit > Add Widget
Logs & Monitor > Access Control > Options > Edit > Add Widget
Logs & Monitor > Threat Prevention > Options > Edit > Add Widget

Types of Widget

You can define these kinds of widget:

Widget	Description
Table	A fitted table of columns and rows.
Chart	A graphical representation of data statistics.
Timeline	A chart with the time already deployed in best-effort layout as the X axis.
Map	A chart that shows events that occur in different parts of the world.
Infographics	A widget used to display a numeric value in iconic way. Usually used in overviews.
Container	A widget used to group several widgets in a single box wrapper. Currently supports vertical, horizontal and grid layouts.
RichText	A static text box used to display a styled text message.

View Description, View Filter, View Settings

What can I do here?

You can edit the:

- **View Description** - A description of the view.
- **View Filter** - The filter that is applied to the view. The default filters are **Blade**, **Action**, **Application Risk**, and **Type**. You can add other filters, and delete filters.
- **View Settings** - The description of the view and the filter that is applied to the view.
- **Add widget** - add a new widget.
- **Undo** - undoes the last change.
- **Redo** - restores the last change.

Getting Here -
Logs & Monitor > General Overview > Options > View Settings
Logs & Monitor > Access Control > Options > View Settings
Logs & Monitor > Threat Prevention > Options > View Settings

Tasks Window

What can I do here?

Use this window to get details of in-progress or recent tasks.

Getting Here - Press F10 to open the tasks window, or click on the arrow in bottom left corner of the SmartConsole.

Install Policy Details

What can I do here?

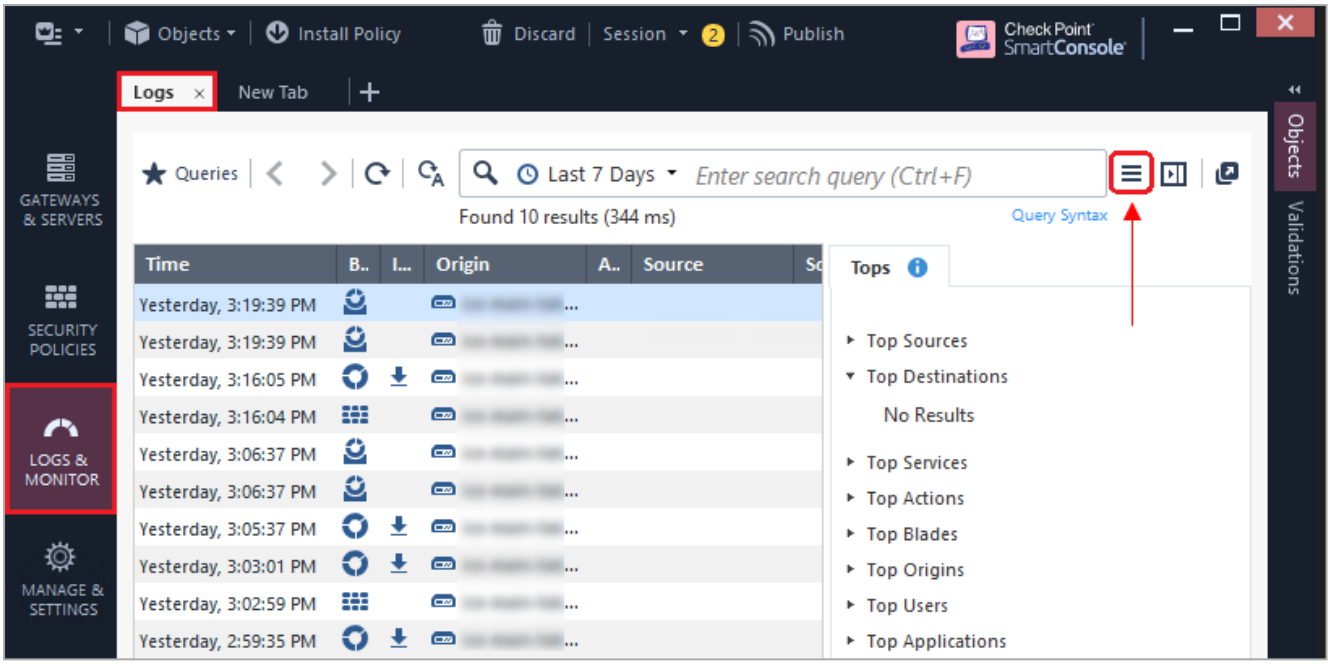
Use this window to get a detailed account of the policy installation.

Getting Here - Press F10 to open the tasks window, or click on the arrow in bottom left corner of SmartConsole. Go to a policy installation task and click Details.

Working with Queries

Running Queries

Click ☰ to the right of the search query field to see the query **Options**.



To run a query:

1. Click **Favorites** in query options, and select a predefined or custom query.
2. Click **Refresh** (or press F5).
3. Enter or select the query.
4. Click in the **Query Definition** field and select a recent query.

To create a query:

1. Click in the **Query Definition** field.
2. Enter or select criteria.

   The query runs automatically. As you add more criteria, results are updated dynamically.

To run a query again:

1. Click **Refresh** (or press F5).
2. Enter or select the query.

To activate auto-refresh:

1. Click **Auto Refresh** (or press F6).
2. Auto refresh shows new logs every 2 seconds.

Configuring Query Defaults

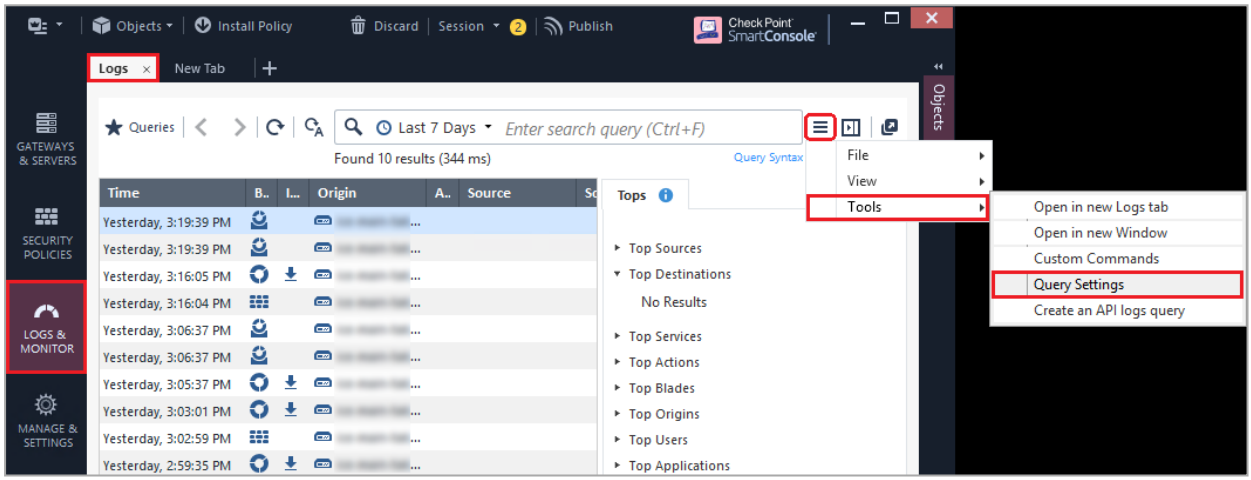
You can use the Query Settings to:

- Define the default query that runs when you open Log View.
- Set the number of items that show in the **Top Results** pane.
- Sets the time, in seconds, that the **Top Results** show after running a query.

To define the default query:

1. Go to **Menu** ☰ > **Tools** > **Query Settings**.

   The **Query Settings** window opens.



2. Enter a query (using the query syntax) in the **Default Query** field.

   Tip: Select a query or Define a query in the Query Definition field. Then copy and paste it into the **Default Query** field.

   If no default query is specified, Log View runs the **All Records** query.

3. Click **OK**.

To configure the Top Results:

1. Go to **Menu** ☰ > **Tools** > **Query Settings**.

   The **Query Settings** window opens.

2. In the **Maximum top results** field, enter the number of results to show (default =10).
3. In the **Show top results after** field, enter the time interval allocated for calculation of top results (default=10 seconds).
4. To get top results from Multi-Domain Log Server and multiple Log Servers:

a. Select **Show top results from Multi-Domain Log Server and multiple Log Servers**.

b. Enter the maximum number of **Simultaneous connections** to Log Servers (default=3).

Note - Top results are collected from all Log Servers in groups of size configured in **Simultaneous connections**.

5. Click **OK**.

Working with the Favorites List

The **Favorites** list contains predefined and saved custom queries.

The predefined queries are organized into folders by Software Blades.

You can add new queries to existing folder or create new folders hold them.

You can do these actions with the Favorites list:

- Add new custom queries.
- Add new query folders.
- Delete queries.

In this version, you cannot move a query from one folder to a different folder.

To add a folder to the Favorites list:

1. From the **Favorites** menu, select **Add to Favorites**.
2. In the **Add to Favorites** window, enter a name for the new query.

   The query criteria show in the query field.
3. Select a folder from the list, or click **Create a New Folder**.
4. Click **Add**.

You can use folders to help you organize custom queries into logical groups. You can create folders inside of other folders.

You can also do this procedure while adding a new query to the favorites list.

To create a new folder:

1. From the **Favorites** menu, select **Add to Favorites**.
2. In the **Add to Favorites** window, click the **Folder** list.
3. Select **Create a New Folder** from the list.

4. In the **Create a Folder** window, enter a name for the new folder.
5. Select a folder to contain the new folder.
6. Click **Add**.

To delete a folder:

You can delete folders that are no longer necessary.

Important - When you delete a folder, you also delete any queries included in that folder. We recommend that you carefully look at folder contents before deleting it. In this release, you cannot move a query from one folder to a different one.

1. From the **Favorites** menu, select **Organize Favorites**.
2. In the **Organize Favorites** folder, select the folder to be deleted.
3. Click **Delete**.
4. Click **Close**.

Creating Custom Queries

Queries can include one or more criteria. You can create custom queries using one or a combination of these basic procedures:

- Right-click columns in the grid view and select **Add Filter**.
- Click in the **Query Definition** field and then select the fields and filter criteria for those fields.
- Manually enter filter criteria in the **Query Definition** field.

A good way to create a new custom query is to run an existing query and then use one of these procedures to change it. You can save the new query in the **Favorites** list.

When you create complex queries, Log View suggests, or automatically enters, an appropriate Boolean operator. This can be an implied AND operator, which does not explicitly show.

Selecting Query Fields

You can enter query criteria directly from the Query search bar.

To select field criteria from the Query search bar:

1. If you are starting a new query, remove query definitions: click **Clear** 
2. Put the cursor in the Query search bar.
3. Select a criterion from the drop-down list or enter the criteria in the Query search bar.

The query runs automatically.

Selecting Criteria from Grid Columns

You can use the column headings in the **Grid** view to select query criteria. This option is not available in the **Table** view.

To select query criteria from grid columns:

1. In the **Results** pane, right-click on a column heading.
2. Select **Add Filter**.
3. Select or enter the filter criteria.
   The criteria show in the **Query search bar** and the query runs automatically.

You can continue to enter more criteria using this or other procedures.

Manually Entering Query Criteria

You can always type query criteria directly in the **Query Definition** field.

You can manually create a new query or make changes to an existing query that shows in the **Query Definition** field.

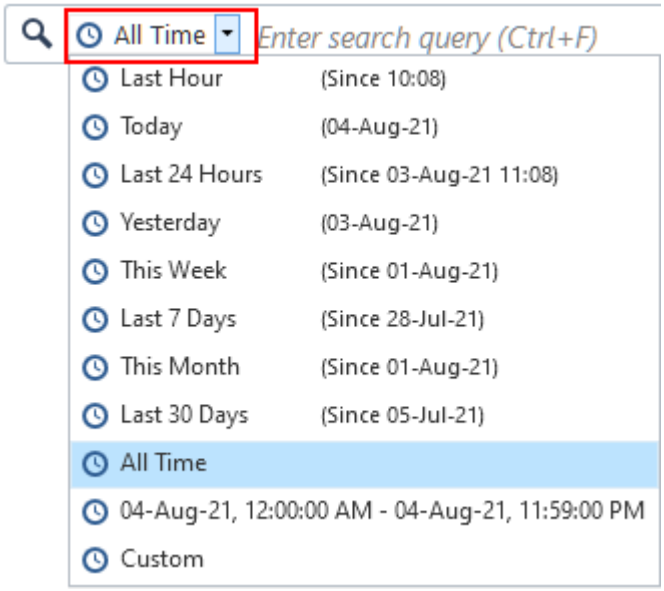
As you type, Log View helps you by showing recently used query criteria or even complete queries.

To use these suggestions, simply select them from the drop down list.

If you make a syntax error in a query, Log View shows a helpful error message that identifies the error and suggests a solution.

Filtering for Time

To filter for a specific period, click the clock icon in the search box.



Select a preset or click **Custom** to define a specific period.

SmartConsole and SmartView Query Language

A powerful query language lets you show only selected records from the log files, according to your criteria. To create complex queries, use Boolean operators, wildcards, fields, and ranges. This section refers in detail to the query language.

When you use SmartConsole to create a query, the applicable criteria show in the **Query search bar**.

The basic query syntax is `[<Field>:] <Filter Criterion>`.

To put together many criteria in one query, use Boolean operators:

`[<Field>:] <Filter Criterion> {AND|OR|NOT} [<Field>:] <Filter Criterion> ...`

Most query keywords and filter criteria are not case sensitive, but there are some exceptions. For example, "`source:<X>`" is case sensitive ("`Source:<X>`" does not match). If your query results do not show the expected results, change the case of your query criteria, or try upper and lower case.

When you use queries with more than one criteria value, an AND is implied automatically, so there is no need to add it. Enter OR or other boolean operators if needed.

Criteria Values

Criteria values are written as one or more text strings. You can enter one text string, such as a word, IP address, or URL, without delimiters. Phrases or text strings that contain more than one word must be surrounded by quotation marks.

One word string examples:

- John
- inbound
- 192.168.2.1
- mahler.ts.example.com
- dns_udp

Phrase examples

- `"John Doe"`
- `"Log Out"`
- `"VPN-1 Embedded Connector"`

IP Addresses

IPv4 and IPv6 addresses used in log queries are counted as one word. Enter IPv4 address with dotted decimal notation and IPv6 addresses with colons.

Example:

- 192.0.2.1
- 2001:db8::f00:d

You can also use the *wildcard* '*' character and the *standard network suffix* to search for logs that match IP addresses within a range.

Examples:

- src:192.168.0.0/16 (shows all records for the source IP 192.168.0.0 to 192.168.255.255 inclusive)
- src:192.168.1.0/24 (shows all records for the source IP 192.168.1.0 to 192.168.1.255 inclusive)
- src:192.168.2.* shows all records for the source IP 192.168.2.0 to 192.168.2.255 inclusive
- 192.168.* shows all records for 192.168.0.0 to 192.168.255.255 inclusive

NOT Values

You can use NOT *<field>* values with *Field Keywords* in log queries to find logs for which the value of the field is not the value in the query.

Syntax

```
NOT <field>: <value>
```

Example

```
NOT src:10.0.4.10
```

Wildcards

You can use the standard wildcard characters (* and ?) in queries to match variable characters or strings in log records. You can use more than the wildcard character.

Wildcard syntax:

- The **?** (question mark) matches one character.
- The ***** (asterisk) matches a character string.

Examples:

- Jo? shows Joe and Jon, but not Joseph.
- Jo* shows Jon, Joseph, and John Paul.

If your criteria value contains more than one word, you can use the wildcard in each word. For example, 'Jo* N*' shows Joe North, John Natt, Joshua Named, and so on.

Note – Using a single '`*`' creates a search for a non-empty value string. For example assetname:*

Field Keywords

You can use predefined field names as keywords in filter criteria. The query result only shows log records that match the criteria in the specified field. If you do not use field names, the query result shows records that match the criteria in all fields.

This table shows the predefined field keywords. Some fields also support keyword aliases that you can type as alternatives to the primary keyword.

Keyword	Keyword Alias	Description
`severity`		Severity of the event
`app_risk`		Potential risk from the application, of the event
`protection`		Name of the protection
`protection_type`		Type of protection
`confidence_level`		Level of confidence that an event is malicious
`action`		Action taken by a security rule
`blade`	`product`	Software Blade
`destination`	`dst`	Traffic destination IP address, DNS name or Check Point network object name
`origin`	`orig`	Name of originating Security Gateway
`service`		Service that generated the log entry
`source`	`src`	Traffic source IP address, DNS name or Check Point network object name
`user`		User name

Syntax for a field name query:

`<field name>:<values>`

- **<*field name*>** - One of the predefined field names
- **<*values*>** - One or more filters

To search for rule number, use the **Rule**field name. For example:

```
rule:7.1
```

If you use the rule number as a filter, rules in all the Layers with that number are matched.

To search for a rule name, you must not use the **Rule** field. Use free text. For example:

```
"Block Credit Cards"
```

Best Practice - Do a free text search for the rule name. Make sure rule names are unique and not reused in different Layers.

Examples:

- `source:192.168.2.1`
- `action:(Reject OR Block)`

  You can use the OR Boolean operator in parentheses to include multiple criteria values.

Important - When you use fields with multiple values, you must:

- Write the Boolean operator, for example **AND**.
- Use parentheses.

Boolean Operators

You can use the Boolean operators **AND** , **OR** , and **NOT** to create filters with many different criteria. You can put multiple Boolean expressions in parentheses.

If you enter more than one criteria without a Boolean operator, the **AND** operator is implied. When you use multiple criteria without parentheses, the **OR** operator is applied before the **AND** operator.

Examples:

- `blade:"application control" AND action:block`

  Shows log records from the Application and URL Filtering Software Blade where traffic was blocked.
- `192.168.2.133 10.19.136.101`

Shows log entries that match the two IP addresses. The **AND** operator is presumed.

- `192.168.2.133 OR 10.19.136.101`

  Shows log entries that match one of the IP addresses.

- `(blade: Firewall OR blade: IPS OR blade:VPN) AND NOT action:drop`

  Shows all log entries from the Firewall, IPS or VPN blades that are not dropped. The criteria in the parentheses are applied before the `AND NOT` criterion.

- `source:(192.168.2.1 OR 192.168.2.2) AND destination:17.168.8.2`

  Shows log entries from the two source IP addresses if the destination IP address is `17.168.8.2`. This example also shows how you can use Boolean operators with field criteria.

Infinity Services

Use this view to connect from your on-premises Security Management Server to the Infinity Portal.

Getting Here - SmartConsole > Infinity Services

Sharing SmartConsole Configuration and Logs with Infinity Portal

Starting from R81.10 Jumbo Hotfix Accumulator Take 93 (and SmartConsole Build 410 / Web SmartConsole Take 76), , you can connect from your on-premises Management Server to the Infinity Portal. This lets you:

- Run services that are managed in the Infinity Portal on your Management Server objects.

  To see the full list of services, go to SmartConsole > **Infinity Services** view.

  For some services, you must enable Configuration Sharing and Log Sharing. See the documentation for the specific service in the *Infinity Portal Administration Guide*.

- See a unified log view of all your Check Point products, both in cloud and on-premises.

  This way, you can search for logs and events from all Check Point products in the same place.

- Use new administrator capabilities on the on-premises Management Server.

  For example, you can run management APIs on the on-premises Management Server through the Infinity Portal securely from anywhere in the world.

Prerequisites

- You must have a valid license for each Infinity Portal application or service that you use.
- In the SmartConsole Access Control Rule Base, add this rule for Check Point Security Gateways. Use "Check Point Services" as an updatable object (see *Updatable Objects*):

Source	Destination	Services	Action
Any	Check Point Services	http	Allow

- For non-Check Point gateways, allow access to the domains listed in Scenario 3 of sk179105.

- You must have the **Manage integration with Cloud Services** option selected on your permission profile. To have this option selected:
  1. Go to **Manage & Settings** > **Permissions & Administrators** > **Permission Profiles**
  2. Open the relevant **Permission Profile**.
  3. Go to **Management**, and select **Manage integration with Cloud Services**.

For configuration, see the *R81.10 Security Management Administration Guide*

Configuration Sharing

Use this window to share data and the configuration of your Security Management Server with Infinity Portal.

Getting Here - SmartConsole > Infinity Services > Data Sharing area > Configuration Sharing > Edit

Configure Log Sharing

Use this window to share logs from your Security Management Server environment and store them in Infinity Portal.

Getting Here - SmartConsole > Infinity Services > Data Sharing area > Log Sharing > Edit

Manage & Settings

What can I do here?

Use these windows to configure:

- Administrators
- Permission profiles
- Trusted Clients
- Sessions
- Software Blades
- Database Revisions
- Idle Timeout
- Login messages

Getting Here - SmartConsole > Manage & Settings

Administrators

What can I do here?

Use this window to create new administrator accounts, edit and delete them.

Administrators are user account objects that have permission to:

- Manage the Security Management Server environment.
- Use SmartConsole clients.

If you do not select an authentication method, the administrator cannot log in to SmartConsole or SmartConsole clients such as SmartEvent.

Getting Here - SmartConsole > Manage & Settings > Permissions & Administrators > Administrators
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Administrators

Multi-Domain Administrators

For more on multi-domain administrators, see:

"Administrators Accounts" on page 673

"Multi-Domain Permission Profile" on page 675

"Domain Permission Profile - Custom" on page 679

Administrator Properties - General

What can I do here?

Configure and manage administrators, authentication methods and permissions.

Getting Here - SmartConsole > Manage & Settings > Permissions & Administrators > Administrators > New or double-click an account > General tab
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Administrators > New or double-click an account > General tab

Configuring Administrator Properties

- Enter a unique name for the administrator - The user name property is required and case sensitive.
- Select an authentication method:
  - **Undefined** users are not authenticated and access is always denied or authentication is based on a certificate (as defined in the **Admin Certificates** tab).
  - **SecurID**users are challenged to enter the number displayed on the Security Dynamics SecurID card. There are no scheme-specific parameters for the SecurID authentication scheme. The Security Gateway acts as an Authentication Manager agent..
  - **Check Point Password** means that users are challenged to enter the internal Check Point password on the gateway, defined here.

    Enter and confirm the password in the specified fields.
  - **OS Password** users are challenged to enter their Operating System password for the Security Management Server.
  - **RADIUS** users are challenged for the response, as defined by the RADIUS server.

    Select a RADIUS server from the list.

- **TACACS** passwords are forwarded to the TACACS server to determine whether access is allowed.

  Select a TACACS server from the list.

  Note - For RADIUS AND TACACS authentication. If you generate a user certificate with a non-Check Point Certificate Authority, enter the Common Name (CN) component of the Distinguished Name (DN). For example, if the DN is: [**CN = James**, O = My Organization, C = My Country], enter **James**as the user name. If you use Common Names as user names, they must contain exactly one string with no spaces.

- **API** - Generate an API key to authenticate to the management API. The administrator can only use the API for executing API commands. The API key cannot be used to log into SmartConsole.

- Assign a permissions profile - When you configure an administrator, you must assign a permissions profile. A permissions profile is a predefined set of permissions that you assign to individual administrators. Complex, granular permissions for many administrators can be configured in one profile.

  To create a new permissions profile, click **New**.

- Set an expiration date - Assign an expiration date for each administrator or configure the account never to expire. After account expiration, the administrator cannot log in to SmartConsole (or SmartConsole clients such as SmartEvent).

  Note : Account expiration has no effect on the OS administrator account. System administrators on the OS are different from administrators defined in SmartConsole for the Security Management Server.

Configuring Check Point Password Authentication for Administrators

These instructions show how to configure Check Point Password authentication for administrators.

Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

To configure a Check Point password for a SmartConsole administrator:

1. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
2. Click **New**.
3. The **New Administrator** window opens.
4. Give the administrator a name.

5. In **Authentication method**, select *Check Point Password*.
6. Click **Set New Password**, type the **Password**, and **Confirm** it.
7. Assign a **Permission Profile**.
8. Click **OK**.
9. Publish the SmartConsole session.

Configuring OS Password Authentication for Administrators

These instructions show how to configure OS Password Authentication for administrators.

OS Password is stored on the operating system of the computer on which the Security Gateway (for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required

To configure an OS password for a SmartConsole administrator:

1. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
2. Click **New**.
3. The **New Administrator** window opens.
4. Give the administrator a name.
5. In **Authentication method**, select *OS Password*.
6. Assign a **Permission Profile**.
7. Click **OK**.
8. Publish the SmartConsole session.

Configuring a RADIUS Server for Administrators

These instructions show how to configure a RADIUS server for SmartConsole administrators. To learn how to configure a RADIUS server, refer to the vendor documentation.

Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.

The RADIUS protocol uses UDP to communicate with the gateway or the Security Management Server.

RADIUS servers and RADIUS server group objects are defined in SmartConsole.

To configure a RADIUS Server for a SmartConsole administrator:

1. In SmartConsole, click **Objects** > **More Object Types** > **Server** > **More** > **New RADIUS**.
2. Configure the **RADIUS Server Properties**:
    a. Give the server a **Name**. It can be any name.
    b. Click **New** and create a **New Host** with the **IP address** of the RADIUS server.
    c. Click **OK**.
    d. Make sure that this host shows in the **Host** field of the **RADIUS Server Properties** window.
    e. In the **Shared Secret** field, type the secret key that you defined previously on the RADIUS server.
    f. Click **OK**.
    g. Publish the SmartConsole session.
3. Add a new administrator:
    a. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
    b. Click **New**.

    The **New Administrator** window opens.
    c. Give the administrator the name that is defined on the RADIUS server.
    d. Assign a **Permission Profile**.
    e. In **Authentication method**, select *RADIUS*.
    f. Select the **RADIUS Server** defined earlier.
    g. Click **OK**.
4. Publish the SmartConsole session.

Configuring a SecurID Server for Administrators

These instructions show how to configure a SecurID server for SmartConsole administrators. To learn how to configure a SecurID server, refer to the vendor documentation.

SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the AM.

Using SecurID, the Security Gateway forwards authentication requests by remote users to the AM. For administrators, it is the Security Management Server that forwards the requests. The AM manages the database of RSA users and their assigned hard or soft tokens. The gateway or the Security Management Server act as an AM agent and direct all access requests to the RSA AM for authentication. For additional information on agent configuration, refer to RSA Authentication Manager documentation.

There are no specific parameters required for the SecurID authentication method.

To configure the Security Management Server for SecurID:

1. Connect to the Security Management Server.
2. Copy the `sdconf.rec` file to the `/var/ace/` folde

   If the folder does not exist, create the folder.
3. Give the `sdconf.rec` file full permissions. Run:

   ```
   chmod 777 sdconf.rec
   ```

To configure a SecurID Server for a SmartConsole administrator:

1. In SmartConsole, click **Objects** > **More Object Types** > **Server** > **More** > **New SecurID**.
2. Configure the **SecurID Properties**:
   a. Give the server a **Name**. It can be any name.
   b. Click **Browse** and select the `sdconf.rec` file. This must be a copy of the file that is on the Security Management Server.
   c. Click **OK**.
3. Add a new administrator:
   a. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
   b. Click **New**.

      The **New Administrator** window opens.
   c. Give the administrator a name.
   d. Assign a **Permission Profile**.
   e. In **Authentication method**, select *SecurID*.
4. In the SmartConsole Menu, click **Install Database**.

Configuring a TACACS Server for Administrators

These instructions show how to configure a TACACS server for SmartConsole administrators. To learn how to configure a TACACS server, refer to the vendor documentation.

To configure a TACACS Server for a SmartConsole administrator:

1. In SmartConsole, click **Objects** > **More Object Types** > **Server** > **More** > **New TACACS**.
2. Configure the **TACACS Server Properties**:
    a. Give the server a **Name**. It can be any name.
    b. Click **New** and create a **New Host** with the **IP address** of the TACACS server.
    c. Click **OK**.
    d. Make sure that this host shows in the **Host** field of the **TACACS Server Properties** window.
    e. In the **Shared Secret** field, type the secret key that you defined previously on the TACACS server.
    f. Click **OK**.
    g. Publish the SmartConsole session.
3. Add a new administrator:
    a. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
    b. Click **New**.

    The **New Administrator** window opens.
    c. Give the administrator the name that is defined on the TACACS server.
    d. Assign a **Permission Profile**.
    e. In **Authentication method**, select *TACACS*.
    f. Select the **TACACS Server** defined earlier.
    g. Click **OK**.
4. Publish the SmartConsole session.

Creating and Changing an Administrator Account

To successfully manage security for a large network, we recommend that you first set up your administrative team, and delegate tasks.

We recommend that you create administrator accounts in SmartConsole, with the procedure below or with the First Time Configuration Wizard.

If you create it through the SmartConsole, you can choose one of these authentication methods:

- **Check Point Password**

  Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

- **OS Passord.**

  OS Password is stored on the operating system of the computer on which the Security Gateway (for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required

- **RADIUS**

  Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

  Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.

  The RADIUS protocol uses UDP to communicate with the gateway or the Security Management Server.

  RADIUS servers and RADIUS server group objects are defined in SmartConsole.

- **SecurID**

  SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the AM.

  Using SecurID, the Security Gateway forwards authentication requests by remote users to the AM. For administrators, it is the Security Management Server that forwards the requests. The AM manages the database of RSA users and their assigned hard or soft tokens. The gateway or the Security Management Server act as an AM agent and direct all access requests to the RSA AM for authentication. For additional information on agent configuration, refer to RSA Authentication Manager documentation.

There are no specific parameters required for the SecurID authentication method.

- **TACACS**

  Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

  TACACS is an external authentication method that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. For administrators, it is the Security Management Server that forwards the requests. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

To create an administrator account using SmartConsole:

1. Click **Manage & Settings** > **Permissions & Administrators**.

   The **Administrators** pane shows by default.

2. Click **New Administrator**.

   The **New Administrators** window opens.

3. Enter a unique name for the administrator account.

   Note - This parameter is case-sensitive.

4. Set the Authentication Method, or create a certificate, or the two of them.

   Note - If you do not do this, the administrator will not be able to log in to SmartConsole.

   To define an Authentication Method:

   In the **Authentication Method** section, select a method and follow the instructions in *Configuring Authentication Methods for Administrators*.

   To create a Certificate - If you want to use a certificate to log in:

   In the **Certificate Information** section, click **Create**, and follow the instructions in *Configuring Certificates for Administrators*.

5. Select a **Permissions** profile for this administrator, or create a new one.

6. Set the account **Expiration** date:

   - For a permanent administrator - select **Never**
   - For a temporary administrator - select an **Expire At** date from the calendar

The default expiration date shows, as defined in the Default Expiration Settings. After the expiration date, the account is no longer authorized to access network resources and applications.

7. **Optional**: Configure **Additional Info - Contact Details**, **Email** and **Phone Number** of the administrator.
8. Click **OK**.

To change an existing administrator account:

1. Click **Manage & Settings** > **Permissions & Administrators**.
2. Double-click an administrator account.

   The **Administrators** properties window opens.

Creating an administrator with 'cpconfig'

We do not recommend creating an administrator with `cpconfig`, the Check Point Configuration Tool. Use it only if there is no access to SmartConsole or the Gaia Portal. If you use `cpconfig` to create an administrator:

- You must restart Check Point Services to activate the administrator.
- It does not show the other administrators
- Check Point Password is automatically configured as the authentication method.

Configuring Default Expiration for Administrators

If you want to use the same expiration settings for multiple accounts, you can set the default expiration for administrator accounts. You can also choose to show notifications about the approaching expiration date at the time when an administrator logs into SmartConsole or one of the SmartConsole clients. The remaining number of days, during which the account will be alive, shows in the status bar.

To configure the default expiration settings:

1. Click **Manage & Settings > Permissions & Administrators > Advanced**.
2. Click **Advanced**.
3. In the **Default Expiration Date** section, select a setting:
   - **Never expires**
   - **Expire at** - Select the expiration date from the calendar control

- **Expire after** - Enter the number of days, months, or years (from the day the account is made) before administrator accounts expire

4. In the **Expiration notifications** section, select **Show 'about to expire' indication in administrators view** and select the number of **days in advance** to show the message about the approaching expiration date.
5. Publish the SmartConsole session.

Administrator Properties - Additional Info

Use this window to enter optional contact information.

Getting Here - SmartConsole > Manage & Settings > Permissions & Administrators > Administrators > New or double-click an account > Additional Info page
Or:
Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Administrators > New or double click an account > Additional Info page

Contact Options

You can optionally add contact information for this user:

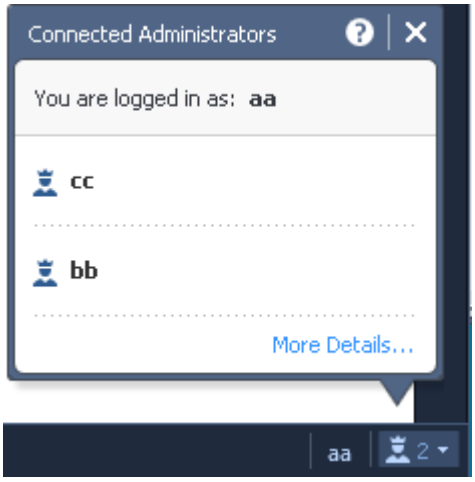
- **Email** - Enter the administrator email address.
- **Contact Details** - Enter additional contact information.
- **Phone** - Enter the administrator telephone number.

Note - If you upgraded from an earlier release, the system copies these values into the new release.

Connected Administrators

What can I do here?

Use this window to see a list of administrators currently connected to the Security Management Server.



Getting Here - Click the upward facing arrow in the bottom right hand corner of SmartConsole.

Permission Profiles

What can I do here?

Use this window to create new permission profiles, edit and delete them.

Getting Here - Manage & Settings > Permission and Administrators > Permission Profiles
Or:
Multi domain > Permissions & Administrators > Permission Profiles

Assigning Permission Profiles to Administrators

A permission profile is a predefined set of Security Management Server and SmartConsole administrative permissions that you can assign to administrators. You can assign a permission profile to more than one administrator. Only Security Management Server administrators with the *Manage Administrators* permission in the profile can create and manage permission profiles.

For Multi-Domain Permission Profiles

For the type of permission profile available in Multi-Domain, see *"Multi-Domain Permission Profile" on page 675*

Custom Permission Profile - Overview

What can I do here?

Use this window to configure new permission profiles for Security Management and Multi Domain.

Getting Here - SmartConsole > Manage & Settings > Permission and Administrators > Profiles > Permission Profiles > New or edit Profile > Overview
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or edit profile > Domain Permission Profile > Overview

New Profile - Permissions Overview

Settings and Parameters:

- **Read/Write All** - Full read and write permissions for all objects
- **Auditor (Read Only All)**
- **Customized**

Custom Permission Profile - Gateways

What can I do here?

Use this window to set permissions for provisioning Security Gateways and running scripts.

Getting Here - SmartConsole > Manage & Settings > Permission and Administrators > Profiles > Permission Profiles > New or Edit Profile > Gateway's page
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or edit Domain Permission Profile > Gateway's page

Gateways

Configure permissions for these Security Gateway management tasks.

Provisioning

- **SmartUpdate** - Install, update and delete Check Point licenses. This includes permissions to use SmartUpdate to manage licenses.

- **SmartLSM Gateway Database** - Access to objects defined in SmartLSM gateway tables. These objects are managed in the SmartProvisioning GUI or LSMcli command-line.

  Manage Provisioning Profiles - Administrator can add, edit, delete, and assign provisioning profiles to gateways (both SmartLSM and non-SmartLSM).
- **VSX Provisioning** - Create and configure Virtual Systems and other VSX virtual objects.
- **System Backup** - Backup Security Gateways.
- **System Restore** - Restore Security Gateways from saved backups.
- **Open Shell** - Use the SmartConsole CLI to run commands.

Scripts

- **Run One Time Script** - Run user scripts from the command line.
- **Run Repository Script** - Run scripts from the repository.
- **Manage Repository Scripts** - Add, change and remove scripts in the repository.

Custom Permission Profile - Access Control

What can I do here?

Use this window to define granular permissions for Access Control Policy rules.

> **Getting Here** - SmartConsole > Manage & Settings > Permissions & Administrators > Permissions profile > profile > New or Edit > Access Control page
> Or:
> SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or Edit > Domain Permission Profile > Access Control page

Access Permission Profile

Configure permissions for these Access Control Policy activities

Policy

Show Policy - Select to let administrators work with Access Control rules and NAT rules. If not selected, administrators cannot see these rules.

- **Edit Layers by Software Blades** - Select this option to configure permissions to with these features in Access Control Layers:
  - **Firewall** - Work with Access Control and other Software Blades that do not have their own Policies.

- **Application and URL Filtering** - Use Application and URL Filtering in Access Control rules.
- **Content Awareness** - Use specified data types in Access Control rules.
- **Mobile Access** - Work with Mobile Access rules.

  To let administrators work with these Policy options, you must also enable these blades in in the **Policy Layer Editor**. This permission profile must also include **all** of the Software Blades enabled in the **Layer Editor**. If you do not do this, administrators with this permission profile cannot work with rules for Access Control Software Blades.

  For example, if you enable Read/Write access for the Firewall, Application and URL Filtering , and Content Awareness Software Blades in the Layer Editor, you must also select them in the permission profile.

- **Edit Layers by selected profiles in the Layer editor** - Select this option to use only those Layer permissions defined in the Layer Editor. There is no Software Blade-level granularity.

Additional Policies

- **NAT Policy** - Work with NAT in Access Control rules.
- **QoS Policy** - Work QoS Policies and rules.
- **Data Loss Prevention** - Configure DLP rules and Policies.
- **Geo Policy** - Work with Access Control rules that control traffic to and from specified countries.

General

- **Access Control Objects and Settings** - allow editing of these object types: .
  - VPN Community .
  - Access Role .
  - Custom application group .
  - Custom application .
  - Custom category .
  - Limit .
  - Application - Match Settings .
  - Application category - Match Settings .
  - Override Categorization .

- Application and URL Filtering blade - Advanced Settings .
- Content Awareness blade - Advanced Settings .

Actions

- **Install Policy** - Install Access Control Policies.
- **Application and URL Filtering Update** - Install Application and URL Filtering updates.

Custom Permission Profile - Threat Prevention

What can I do here?

Use this window to configure permissions and actions for Threat Prevention policies.

> **Getting Here** - SmartConsole > Manage & Settings > Permissions & Administrators > Permission Profiles> > Profile > New or Edit > Threat Prevention page
> Or:
> SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or Edit > Domain Permission Profile > Threat Prevention page

Threat Permission Profile

Configure these permissions for Threat Prevention:

Policy

- Policy **Layers**
  - **Edit all Layers** - Gives permission to edit all layers.
  - **Edit layers by the selected profiles in the layer editor** - Administrators can only edit the layer if the Threat Prevention layer editor gives editing permission to their profiles.
- **Policy Exceptions** - Configure exceptions to Threat Prevention rules.

Permissions

- **Policy Rules** - Configure Threat Prevention Policy rules.
- **Policy Exceptions** - Configure exceptions to Threat Prevention rules.
- **Profiles** - Configure Threat Prevention profiles.
- **Protections** - Work with malware protections.
- **Settings** -Work with general Threat Prevention settings.

Actions

- **Install Policy**- Install Policies.
- **IPS Update** - Update IPS protections.

  Note - You do not have to log into the User Center to receive IPS updates.

Custom Permission Profile - Others

What can I do here?

Use this window to configure read/write permissions for other features.

Getting Here - SmartConsole > Manage & Settings > Permissions & Administrators > Permission Profiles > Custom > New or Edit > Others page
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or Edit > Domain Permission Profile > Others page

Other Permission Profiles

Permissions:

- **Common Objects** - Define and manage objects in the Check Point database: Network Objects, Services, Custom Application Site, VPN Community, Users, Servers, Resources, Time, UserCheck, and Limit.
- **Check Point Users Database** - Work with user accounts and groups.
- **LDAP Users Database** - Work with the LDAP database and user accounts, groups and OUs.
- **User Authority and Access** - Work with Check Point User Authority authentication.
- **HTTPS Inspection** - Enable and configure HTTPS Inspection rules.
- **Client Certificates** - Create and manage client certificates for Mobile Access.
- **User and Device Management** - Gives access to the UDM (User & Device Management) web-based application that handles security challenges in a "bring your own device" (BYOD) workspace.

Custom Permission Profile - Monitoring and Logging

What can I do here?

Use this window to configure Permissions Profiles for different monitoring and logging features.

Getting Here - SmartConsole > Manage & Settings > Permissions & Administrators > Profile > Custom > New or Edit > Monitoring and Logging page
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or Edit > Domain Permission Profile > Monitoring and Logging page

Monitoring and Logging

Monitoring and Logging:

- **Monitoring** - See monitoring views and reports.
- **Management Logs** - See Multi-Domain Server audit logs.
- **Track Logs** - Use the log tracking features in SmartConsole.
- **Application and URL Filtering Logs** - Work with Application and URL Filtering logs.
- **HTTPS Inspection logs** - See logs generated by HTTPS Inspection.
- **Packet Capture and Forensics** - See logs generated by the IPS and Forensics features.
- **Show Packet Capture by default** - Enable packet capture by default.
- **Identities** - Show user and computer identity information in logs.
- **Show identities by default** - Show user and computer identity information in logs by default.
- **DLP logs** - Show DLP logs including confidential fields.
- **View/Release/Discard DLP messages** - See, disable, and delete DLP messages.

Custom Permission Profile - Events and Reports

What Can I do here?

Use this window to configure SmartEvent permissions:

Getting Here - SmartConsole > Manage & Settings > Permissions & Administrators > Profile > Custom > New or Edit > Events and Reports page
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or Edit > Domain Permission Profile > Events and Reports page

Event and Reports

Events and Reports Settings and Parameters:

- **SmartEvent Events** - Work with event queries on the **Events** tab. Create custom event queries.
- **SmartEvent Policy** - Configure SmartEvent Policy rules and install SmartEvent Policies.
- **SmartEvent Reports** - Create and run SmartEvent reports.

Custom Permissions Profile - Management

What can I do here?

Use this window to set management and High Availability permissions

> **Getting Here** - SmartConsole > Manage & Settings > Permissions & Administrators > Profile > Custom > New or Edit > Management
> Or:
> SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or Edit > Domain Permission Profile > Management page

Management

Configure these Domain management permissions

- **Manage Administrators** - Manage other administrator accounts.
- **Manage Sessions** - Lets you disconnect, discard, publish, or take over other administrator sessions.
- **High Availability Operations** - Configure and work with Domain High Availability.
- **Management API Login** - Permission to log in to the Security Management Server and run api commands using these tools:
  - mgmt_cli (Linux and Windows binaries)
  - Gaia CLI (clish)
  - Web Services (REST)

  Useful if you want to *prevent* administrators from running automatic scripts on the Management.

  Note: This permission is not required to run commands from within the API terminal in SmartConsole.

- **Cloud Management Extension (CME) Operations** - permission to read or read / edit the Cloud Management Extension (CME) configuration.

Custom Permission Profile - Endpoint

What can I do here?

Use this window to set permissions for Endpoint administrators.

Getting Here - SmartConsole > Manage & Settings > Permissions & Administrators > Profile > Custom > New or Edit > Endpoint page
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New or Edit > Domain Permission Profile > Endpoint page

Endpoint Security Permissions

Endpoint Security uses the Permissions Profiles configured in SmartConsole to define administrator roles.

Configure these Endpoint Permissions:

- **Manage Policies and Software Deployment** - The administrator can work with policies, rules and actions.

  Select Read/Write permissions.
- **Policies Installation** - The administrator can install policies on endpoint computers.
- **Software Deployment** - The administrator can define deployment rules, create packages for export, and configure advanced package settings.

  Select Read/Write permissions.
- **Software Deployment Installation** - The administrator can deploy packages and install endpoint clients.
- **Recovery Media** - The administrator can create recovery media on endpoint computers and devices.
- **Remote Help** - The administrator can use the Remote Help feature to reset user passwords and give access to locked out users.
- **Reset Computer Data** - The administrator can reset a computer, which deletes all information about the computer from the Security Management Server.
- **Authorize Preboot Users** - The administrator can add and remove the users who are permitted to log on to Endpoint Security client computers with Full Disk Encryption.

- **Allow Executing Push Operations** -The administrator can start operations that the Security Management Server pushes directly to client computers with no policy installation required.

Permissions & Administrators - Advanced

What can I do here?

Use this window to configure:

- Administrator Account Settings
- Idle Timeout for SmartConsole
- Check Point Password
- Login Restrictions for locking and unlocking administrator accounts.

Getting Here - Manage & Settings Permissions & Administrators > Advanced
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Advanced

Trusted Clients

What can I do here?

Use this window to create a trusted client, or edit the properties of a trusted client.

Getting Here - Getting Here - Manage & Settings Permissions & Administrators > Trusted Clients
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Trusted Clients

Assigning Trusted Clients to Domains

You must assign all Domains to one or more trusted SmartConsole clients before you can connect to them. If you do not do this, an error message will show when you try to connect.

Each Domain assignment identifies trusted SmartConsole clients based on one of these criteria:

- An IP address
- A host name

- A range of IP addresses
- Net mask
- IP addresses with wildcard characters
- **Any** - All SmartConsole clients can connect

To assign a trusted client to a Domain:

1. Connect to the Multi-Domain Server with SmartConsole
2. Select **Multi-Domain** > **Permissions & Administrators** > **Trusted Clients**.
3. Click **New**.
4. In the **New Trusted Client** window, enter a unique name for this Domain assignment.
5. Select an identification criterion from the **Type** list and enter the applicable information.
6. Add one or more Domains to the **Domain Assignment** list.
7. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.

To add another Domain to an existing trusted client:

1. Select **Multi-Domain > Permissions & Administrators > Trusted Clients**.
2. Double-click the trusted client name.
3. In the **Trusted Client** window, add one or more Domains to the **Domains Assignment** list.

To change a Domain assignment:

1. Select **Multi-Domain** > **Permissions & Administrators** > **Trusted Clients**.
2. Double-click an existing trusted client name.
3. Select an identification criterion from the **Type** list and enter or change the applicable information.
4. Add or delete one or more Domains in the **Domain Assignment** list.
5. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.

Trusted Client - General

What can I do here?

Use this window to create a trusted client.

Getting Here - Manage & Settings > Permissions & Administrators > Advanced > Trusted Clients > New
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Advanced > Trusted Clients > New

Trusted Client Object Editor

Configure these Trusted Client assignment parameters:

- **Object Name** - Enter a unique administrator name.
- **Object Comment** - Optionally, enter a free text description or comment.
- **General**
  - **Type** - Select a trusted client object type:
    - **Any** - Allow access from all clients.
    - **IP Address** - Allow client access for a specified an IPv4 or IPv6 address. Click **Resolve from name** to get the IP address from the DNS.
    - **IP address range** - Allow client access from a specified range of IPv4 or IPv6 addresses.
    - **Net Mask** - Allow client access from the specified IPv4 or IPv6 IP address and subnet.
    - **Name** - Allow access from the specified host name.
    - **Wildcards** - Allow access from all clients that match the specified IP address wildcard characters.

For Trusted Domain Clients

Configure assignment parameters:

- **Domain Assignment**:
  - **+** - Click and select a Domain to add to the profile.
  - **X** - Delete the selected Domain from the profile.

- **Multi-Domain Server Trusted Client** - Let this SmartConsole client connect to all Multi-Domain Servers in the deployment.

Sessions - View Sessions

What can I do here?

You can see a list of connected user sessions and, optionally, disconnect user sessions. You can filter the sessions shown by:

- Domain
- Client application
- Connection mode (Read or Read/Write)
- Connectivity status (Connected or Disconnected)

Use this window to see which administrator accounts are connected to the Security Management Server. You can also disconnect an account.

Getting Here - Manage & Settings > Sessions
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Sessions

Working in SmartConsole Session View

The Session view shows all unpublished sessions in the system. The view shows the sessions of the current administrator, sessions of other administrators and sessions from other applications. The columns in the view can be customized and show the session owner, name, description, connection mode, number of private changes, number of locks, application and other values.

To see session information, click **Manage & Settings > Sessions > View Sessions**.

Actions available to administrators on private sessions are determined by the **Manage Sessions** permission on their profile.

Administrators without the Manage Session permission can:	Administrators with the Manage Session Permission can:
■ Publish and discard their own sessions ■ See sessions opened by other administrators, the number the locks they have and number of changes they have made ■ Take over sessions created by applications, for example sessions created by the API command line tool	■ Publish and discard their own sessions ■ See sessions opened by other administrators, the number the locks they have and number changes they have made ■ **Publish & Disconnect** the private sessions of other administrators ■ **Disconnect & Discard** the private sessions of other administrators ■ **Disconnect** another administrator's private session ■ **Take over** sessions created by applications, for example sessions created by the API command line tool ■ **Take over** the private sessions of other administrators. **Note** : If you want to keep changes made in your own private session, publish these changes *before* you take over the session of another administrator. If you do not publish your changes, you will lose them. When you take over, you disconnect the other administrator's SmartConsole session. ■ **Publish & Disconnect** the private sessions of other administrators. The action applies to both SmartConsole sessions and command line API sessions. ■ **Disconnect** the private session of other administrators ■ **Discard & Disconnect** the private session of other administrators

Working with Database Revisions

To see saved database versions:

In SmartConsole, go to **Manage & Settings > Revisions**.

To see the changes made during a specific revision:

1. In the **Manage & Settings > Revisions** window, select revision.

   The bottom pane shows the audit logs of the changes made in the revision.

2. **Optional:** Click **View**.

   A separate read-only SmartConsole session opens.

To delete all versions of the database that are older than the selected version:

1. In the **Manage & Settings > Revisions** window, select a revision.
2. Click **Purge**.
3. In the confirmation window that opens, click **Yes**.

   Important - Deletion is irreversible. When you purge, that revision and older revisions are deleted permanently.

Session Settings - Advanced

What can I do here?

Use this window to enforce session requirements. Select requirements from the list.

Getting Here - Manage & Settings > Sessions > Advanced

Administrators Working with Multiple Sessions

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

Use Case

Suppose you are making changes in a private session and are asked to solve some immediate problem. The task involves making a change and publishing it. You do not wish to publish or discard your current private session.

You open a new private session, make the change required resolve the issue, publish the change, then return to your previous private session.

To do this, you need to work with multiple sessions. To switch on multiple sessions, you need the **Manage Sessions** permission selected on your administrator profile.

To enable working in multiple sessions:

1. Open the relevant permission profile.
2. Make sure the **Manage Sessions** permission is selected on the **Management** page.
3. Open SmartConsole > **Manage & Settings** View > **Sessions** > **Advanced**.
4. Select **Each administrator can manage multiple SmartConsole sessions at the same time**.
5. Publish the SmartConsole session.

When working with multiple sessions, you can:

- Open and manage multiple sessions to the Security Management Server using the same administrator account
- Switch between the active session and previously saved sessions
- Publish, discard and disconnect other sessions
- Take over other sessions

The SmartConsole Session menu

After multiple sessions are enabled, the SmartConsole Session menu has these new options:

Option	Description
Edit sessions details	Lets you change the session name and description.
Create new session	**In the current window** Opens a new session in the current SmartConsole **In a new window** Opens a new session in a new SmartConsole
Recent	Shows a list of recent sessions. Selecting a session opens the session in the current SmartConsole
More	Opens the **Open Session** window that shows sessions that you previously created and saved. ■ Sessions shown in this window are owned by the current user in the current domain. ■ The **Open Session > Actions** menu has options to open a saved session in the current SmartConsole or open the session in a new SmartConsole.

The SmartConsole Session View

When multiple sessions are enabled, you can perform these additional actions:

Action	You can:
For sessions that you own	■ Discard and Disconnect ■ Publish and Disconnect ■ Disconnect ■ Open an older session
For sessions owned by other administrators that have made private changes	■ Publish and Disconnect their changes ■ Discard and Disconnect ■ Disconnect ■ Take over their changes
For sessions owned by other administrators that have not made private sessions	■ Disconnect ■ Take over

Notes :

- When working in single session, you need to publish or discard your changes before taking over another session. In multiple sessions, you do not have to publish or discard your session before taking over the session of another administrator.
- In multiple sessions, an administrator connecting from another desktop to an already connected session can still take over the connected session by default.

Switching between Multiple and Single Session

If the session management settings switch from multiple SmartConsole sessions to allow only a single SmartConsole session at a time:

- Administrators can still publish, discard and open sessions that they own.
- Cannot create new sessions until they have published or discarded all their unpublished sessions with private sessions
- Cannot take over the sessions of other administrators or applications (for example sessions created with API commands in the *mgmt_cli* utility) until they have published or discarded all their previously saved private sessions.

Session Details

What can I do here?

Use this window to add a custom name and description for the session.

Getting Here - Menu > Session Details, or click Session in the SmartConsole title bar.

Session Details - View

What can I do here?

Double click on a session to view the session details.

Getting Here - Manage & Settings > Sessions > View Sessions

Open Session

What can I do here?

Use this window to manage active sessions.

Getting Here - Menu > Open Session

Blades

What can I do here?

Use this window to configure general settings for all Software Blades or particular settings of one blade.

Getting Here - Manage & Settings > Blades

Inspection Settings - General

What can I do here?

Use this window to view Threat Prevention protections and their settings.

For configuring individual inspections, see: Inspection Settings

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General

Inspection Settings

You can configure inspection settings for the Firewall:

- Deep packet inspection settings
- Protocol parsing inspection settings
- VoIP packet inspection settings

The Security Management Server comes with two preconfigured inspection profiles for the Firewall:

- **Default Inspection**
- **Recommended Inspection**

When you configure a Security Gateway, the **Default Inspection** profile is enabled for it. You can also assign the **Recommended Inspection** profile to the Security Gateway, or to create a custom profile and assign it to the Security Gateway.

To activate the Inspection Settings, install the Access Control Policy.

Note - In a pre-R80 SmartConsole, Inspection Settings are configured as IPS Protections.

Inspection Settings Table

Column	Description
Protection	Name of the protection
Performance Impact	How much this protection and its resources affect gateway or server performance
Profile	Displays profiles created on the Profiles page

Aggressive Aging - Advanced

What can I do here?

Use this window to configure aggressive aging timeouts and enforcements.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Aggressive Aging > Profile > Advanced

Understanding Aggressive Aging

To increase gateway stability, aggressive Aging helps manage the capacity of the connection table and gateway memory consumption.

Aggressive Aging introduces a new set of short timeouts called aggressive timeouts. When a connection is idle for more than its aggressive timeout, it is marked as "eligible for deletion". When the connections table or memory consumption reaches a user defined threshold, Aggressive Aging begins to delete "eligible for deletion" connections until memory consumption or connection capacity falls to the applicable level.

Aggressive Aging lets the Security Gateway handle large amounts of unexpected traffic, for example during a Denial of Service attack.

If the defined threshold is exceeded, each incoming connection triggers the deletion of ten connections from the "Eligible for Deletion" list. An additional ten connections are deleted with every new connection until the memory consumption or the connections capacity falls below the enforcement limit. If there are no "Eligible for Deletion" connections, no connections are deleted but the list is checked for each subsequent connection that exceeds the threshold.

Timeout settings are a key factor in memory consumption configuration. When timeout values are low, connections are deleted faster from the table, enabling the firewall to handle more connections concurrently.

Best Practice : When memory consumption exceeds its threshold, work with shorter timeouts that can maintain the connectivity for the majority of the traffic.

In the **Aggressive Aging Timeouts are enforced when** section, select whether they will be enforced if the Connections table exceeds a limit, if Memory exceeds a limit, or if both exceed their limits.

If you select both, the values in the percentage fields of the other options are applied. Default is 80%, with connections from the "Eligible for Deletion" list being deleted if either the Connections table or Memory consumption passes this limit.

Note - The limits for the Connections table and Memory consumption are set for each profile. The Aggressive Aging timeouts are global. Therefore: different gateways may enforce the same timeouts at different thresholds.

Activate this protection in either **Prevent** or **Detect** mode.

Aggressive Aging Timeouts - Advanced

What can I do here?

Use this window to configure aggressive aging timeouts.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Aggressive Aging > Profile > Advanced > Aggressive Aging timeouts > Configure

IPS Protections - Advanced Options

What can I do here?

Use these windows to configure advanced protection options.

Note : Only the protections listed here have advanced options.

Getting Here - Security Policies > Threat Prevention > Custom Policy Tools > IPS Protections

ASCII Only Request - Advanced

What can I do here?

Use this window to configure the protection scope and the blocking of non ASCII characters.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > ASCII Only Request > Profile > Advanced

Block MGCP or SIP Messages with Binary Characters - Advanced

What can I do here?

Use this window to allow extended ASCII characters.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Block MGCP/SIP Messages with Binary Characters > Profile > Advanced

Directory Listing - Advanced

What can I do here?

Use this window to configure the protection scope.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Directory Listing > Profile > Advanced

DNS - General Settings - Advanced

What can I do here?

Use this window to configure how DNS connections are monitored.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > DNS - General Settings > Profile > Advanced

DNS Maximum Request Length - Advanced

What can I do here?

Use this window to set the maximum UDP request byte length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > DNS Maximum Request Length > Profile > Advanced

Dynamic Ports - Advanced

What can I do here?

Use this window to configure monitoring, and the dynamic port protection mode.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Dynamic Ports > Profile > Advanced

FTP Security Server - General Settings - Advanced

What can I do here?

Use this window to set the protection scope of the server.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > FTP Security Server - General Settings > Profile > Advanced

Gzip Enforcement - Advanced

What can I do here?

Use this window to configure compression and decompression options.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Gzip Enforcement > Profile > Advanced

H.323 - Advanced

What can I do here?

Use this window to configure H.323 advanced options.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > H.323 > Profile > Advanced

H.323 Max Allowed Phone's Extension Length - Advanced

What can I do here?

Use this window to set the maximum length of the phone's extension.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > H.323 Max Allowed Phone's Extension Length > Profile > Advanced

HTTP Format Sizes - Advanced

What can I do here?

Use this window to set the protection scope, configure format sizes and specific header lengths.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > HTTP Format Sizes > Profile > Advanced

Header Length Editor

What can I do here?

Use this window to edit the name and set a maximum header length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > HTTP Format Sizes > Advanced > Specific Header Lengths

HTTP Methods - Advanced

What can I do here?

Use this window to set Protection scope and configure blocked HTTP Methods.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > HTTP Methods > Profile > Advanced

Blocked HTTP Methods

What can I do here?

User this window to configure HTTP methods blocked by the web server.

Note : The configuration defined here applies only to web servers that are not configured to block default HTTP methods.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > HTTP Methods > Profile > Advanced > Blocked HTTP Method Configuration.

HTTP Protocol - General Settings - Advanced

What can I do here?

Use this window to split the URL between the query and fragment sections.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > HTTP Protocol - General Settings > Profile > Advanced

IP Fragments

What can I do here?

Use this window to allow IP Fragments and set the number of incomplete packs allowed.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > IP Fragments > Profile > Advanced

Mail and Recipient Content

What can I do here?

Use this window to set aggressive MIME strips

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Mail and Recipient Content > Profile > Advanced

Mail Global Protection Scope - Advanced

What can I do here?

Use this window to set the protection scope to all connections or only those connections related to resources in the rule base.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Mail Global Protection Scope> Profile > Advanced

Max Allowed H.245 Message Length - Advanced

What can I do here?

Use this window to configure the maximum allowed H.245 message length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Max Allowed H.245 Message Length > Profile > Advanced

Max Allowed Q.931 Message Length - Advanced

What can I do here?

Use this window to set the maximum Q.931 message length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Max Allowed Q.931 Message Length > Profile > Advanced

Max Allowed RAS Message Length - Advanced

What can I do here?

Use this window to set the maximum allowed RAS message length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Max Allowed RAS Message Length > Profile > Advanced

Max Allowed SCCP Message Length - Advanced

What can I do here?

Use this window to set maximum allowed length of the SCCP message.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Max Allowed SCCP Message Length > Profile > Advanced

Maximum Bad POP3 Commands Enforcement - Advanced

What can I do here?

Use this window to maximum number of bad commands allowed.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Maximum Bad POP3 Commands Enforcement > Advanced

Maximum Bad SMTP Commands Enforcement - Advanced

What can I do here?

Use this window to configure the maximum number of bad commands allowed.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Maximum Bad SMTP Commands Enforcement > Profile > Advanced

Maximum No-Effect Commands Enforcement - Advanced

What can I do here?

Use this window to set the maximum number of no-effect commands allowed.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Maximum No-Effect Commands Enforcement > Profile > Advanced

Maximum Number of Recipient Enforcement - Advanced

What can I do here?

Use this window to set the maximum number of email recipients.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Maximum Number of Recipient Enforcement > Profile > Advanced

Maximum POP3 Command Line Length Enforcement - Advanced

What can I do here?

Use this window to set the maximum POP3 command line length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Maximum POP3 Command Line Length Enforcement > Profile > Advanced

Maximum POP3 Commands Per Connection Enforcement - Advanced

What can I do here?

Use this window to set the maximum number of POP3 commands per connection.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Maximum POP3 Commands Per Connection Enforcement > Profile > Advanced

Maximum SMTP Command line length Enforcement - Advanced

What can I do here?

Use this window to set the maximum line length for SMTP commands.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Maximum SMTP Command line length Enforcement > Profile > Advanced

Maximum SMTP Commands Per Connection Enforcement - Advanced

What can I do here?

Use this window to set maximum number of SMTP commands allowed per connection.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Maximum SMTP Commands Per Connection Enforcement > Profile > Advanced

MGCP Command

What can I do here?

Use this window to add or edit a blocked MGCP command.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP > Profile > Advanced > Add or edit command

MGCP - Advanced

What can I do here?

Use this window to:

- Select MGCP commands that are blocked
- Verify MGCP header content
- Drop multi-cast RTP connections

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP > Profile > Advanced

MGCP - General Settings - Advanced

What can I do here?

Use this window to:

- Block dynamic opening of ports for the MGCP media channel
- Hide the NAT changed source port for MGCP

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP - General Settings > Profile > Advanced

MGCP Command Filtering - Advanced

What can I do here?

Use this window to configure supported MGCP commands and block unknown commands.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP Command Filtering > Profile > Advanced

MGCP Max Allowed Call-ID Length - Advanced

What can I do here?

Use this window to set the maximum allowed length of the Call-ID.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP Max Allowed Call-ID Length > Profile > Advanced

MGCP Max Allowed Connection Mode Length - Advanced

What can I do here?

Use this window to set the maximum allowed connection mode length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP Max Allowed Connection Mode Length > Profile > Advanced

MGCP Max Allowed Domain Name Length - Advanced

What can I do here?

Use this window to set the maximum allowed length of the Domain name.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP Max Allowed Domain Name Length > Profile > Advanced

MGCP Max Allowed EndpointID Length - Advanced

What can I do here?

Use this window to set the maximum allowed length of the EndpointID.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP Max Allowed EndpointID Length > Profile > Advanced

MGCP Max Allowed TransactionsID Length - Advanced

What can I do here?

Use this window to set the maximum allowed length of the TransactionsID.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP Max Allowed TransactionsID Length > Profile > Advanced

MGCP Max Length of Header Value - Advanced

What can I do here?

Use this window to set the maximum length of the MGCP header value.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > MGCP Max Length of Header Value > Profile > Advanced

Minimum Command Line Length Enforcement - Advanced

What can I do here?

Use this window to set he minimum command line length

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Minimum Command Line Length Enforcement > Profile > Advanced

Network Quota - Advanced

What can I do here?

Use this window to configure connections settings and objects excluded from the Network Quota.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Network Quota > Profile > Advanced

Non Compliant HTTP - Advanced

What can I do here?

Use this window to:

- Enforce strict HTTP parsing
- Configure setting for R70 and above

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Network Quota > Profile > Advanced > Objects excluded from the Network Quota > click +

Non-TCP Flooding - Advanced

What can I do here?

Use this window to stop non-TCP connections from flooding the connection table.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Non-TCP Flooding > Profile > Advanced

Packet Sanity - Advanced

What can I do here?

Use this window to disable relaxed UDP length verification.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Packet Sanity > Profile > Advanced

POP3/IMAP Security - Advanced

What can I do here?

Use this window to configure:

- Protection scope
- Buffer overrun protection
- Denial of service
- Known POP3 Commands

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > POP3/IMAP Security > Profile > Advanced

Pattern Name for Inspection Settings and IPS Protections

What can I do here?

Use this window to set a pattern name.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Protection > Profile > Advanced page > Add or edit command in table
Or:
Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Protection > Advanced page > Add or edit command in table

Edit Pattern String

What can I do here?

Use this window to add, edit or remove worm pattern definitions.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Protection > Profile > Advanced page > Add or edit command in table
Or:
Security Policies > Threat Prevention > Policy > Custom Policy Tools > IPS Protections > Protection > Advanced page > Add or edit command in table

Worm Pattern Definitions

Worm patterns are described using regular expressions that define the suspicious pattern in HTTP URLs. Regular expressions are a very flexible way of pattern matching. If Web Security matches the pattern in a URL, the packet is dropped.

What is a CIFS worm pattern?

CIFS worm patterns are described using regular expressions that define suspicious patterns. Patterns are matched against file names (including file paths but excluding the disk share name) that the client is trying to read or write from the server.

The file names used by many worms are predictable and thus can be blocked using worm patterns.

These patterns can also be used to block certain CIFS services (like the remote registry service) that utilize the IPC$ hidden share.

If Web Intelligence matches the pattern in a file name to one of its list of worm patterns, the packet is dropped.

Worm Patterns

This is an example of a worm pattern file:

```
(
        : (
  :pattern ("\.test\?")
  :pattern_date (1021220693)
  :worm_name (TestWorm)
  :mode (true)
 )
)
```

SCCP General Settings - Advanced

What can I do here?

Use this window to block the opening of dynamic ports for the SCCP media channel.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SCCP General Settings > Profile > Advanced

SCCP (Skinny) - Advanced

What can I do here?

Use this window to drop multicast RTP connections and verify SCCP header content.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SCCP (Skinny) > Profile > Advanced

Sequence Verifier - Advanced

What can I do here?

Use this window to track out of state packets.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Sequence Verifier > Profile > Advanced

Out of State Packets

Packets that enter a Security Gateway but whose session was initiated through a different Security Gateway, are considered "out-of-state" packets.

SIP Protections

SIP General Settings - Advanced

What can I do here?

Use this window to configure:

- Registration expiration and idle timeout
- NAT
- VoIP network extension length
- Dynamic pinholing

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP General Settings > Profile > Advanced

SIP Method Filtering - Advanced

What can I do here?

Use this window to configure supported methods and block unknown ones.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Method Filtering > Profile > Advanced

SIP Custom Properties - Advanced

What can I do here?

Use this window to:

- Block SIP early media
- Block SIP proxy failover
- Block calls using a proxy or redirect server
- Block SIP calls that use different voice connections for incoming and outgoing audio
- Set the default proxy registration timeout period
- Set the SIP user suffix length

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Custom Properties > Profile > Advanced

SIP Filtering - Advanced

What can I do here?

Use this window to configure SIP application filtering and method filtering.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Filtering > Profile > Advanced

SIP Max Allowed Content Length - Advanced

What can I do here?

Use this window to set the SIP maximum allowed content length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > > Profile > Advanced

SIP Max Allowed Call-ID Length - Advanced

What can I do here?

Use this window to set the maximum allowed length of the Call-ID.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed Call-ID Length > Profile > Advanced

SIP Max Allowed Domain Length - Advanced

What can I do here?

Use this window to set maximum length of the Domain.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed Domain Length > Profile > Advanced

SIP Max Allowed Header Name Length - Advanced

What can I do here?

Use this window to set the maximum allowed length of the header name.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed Header Name Length > Profile > Advanced

SIP Max Allowed Header Value Length - Advanced

What can I do here?

Use this window to set the maximum length of the header value.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed Header Value Length > Profile > Advanced

SIP Max Allowed Occurrences of the Same Field - Advanced

What can I do here?

Use this window to set the maximum allowed occurrences of the same field when the field occurs multiple times.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed Occurrences of the Same Field > Profile > Advanced

SIP Max Allowed SDP Length - Advanced

What can I do here?

Use this window to set the maximum allowed SDP Length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed SDP Length > Profile > Advanced

SIP Max Allowed Tag Length - Advanced

What can I do here?

Use this window to set the maximum allowed tag length.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed Tag Length > Profile > Advanced

SIP Max Allowed URI Length - Advanced

What can I do here?

Use this window to set the maximum allowed length of a URI.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed URI Length > Profile > Advanced

SIP Max Allowed Retransmissions - Advanced

What can I do here?

Use this window to set the maximum allowed retransmissions.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Max Allowed Retransmissions > Profile > Advanced

SIP Min Allowed 'Max-forwards' Value - Advanced

What can I do here?

Use this window to set the minimum allowed 'Max-forwards' value.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP Min Allowed 'Max-forwards' Value > Profile > Advanced

SIP Protections - Advanced

What can I do here?

Use this window to:

- Verify SIP header content
- Block basic authorization
- Block notify with invalid subscription state
- Block calls from unregistered users
- Set the maximum number of retransmissions allowed
- Set the maximum number of invitations per call

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SIP protections > Profile > Advanced

Small PMTU - Advanced

What can I do here?

Use this window to set minimal MTU byte size, and minimal byte size for IPv6

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Small PMTU > Profile > Advanced

SNMP - Advanced

What can I do here?

Use this window to configure SNMP actions: to monitor or allow traffic.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SNMP > Profile > Advanced

SYN Attack - Advanced

What can I do here?

Use this window to:

- Override the Security Gateway SYNDefender configuration
- Configure activation settings

- Configure SYN Attack Detection
- Logging options

For more information on SYN attacks configuration, see sk120476

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SYN Attack > Profile > Advanced

SNMP - Drop requests with Default Community Strings

What can I do here?

Use this window to configure default community strings that cause the Security Gateway to drop SNMPv1 or SNMPv2 requests.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > SYN Attack > Profile > Advanced > Allow all SNMP traffic > Drop requests with default community strings... > Configure

Syslog Relay Server List - Advanced

What can I do here?

Use this window to configure a list of syslog relay servers.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > Syslog Relay Server List > Profile > Advanced

VoIP Call Initiations Rate Limiting - Advanced

What can I do here?

Use this window to set the number of call attempts per ID per minute.

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > VoIP Call Initiations Rate Limiting > Profile > Advanced

VoIP Denial of Service - Advanced

What can I do here?

Use this window to :

- Enable VoIP DoS Protection
- Set the maximum number of call attempts per IP per minute

Getting Here - Manage & Settings > Blades > General > Inspection Settings > General > Protections table > VoIP Denial of Service > Profile > Advanced

Inspection Settings - Profiles

What can I do here?

Use this window to see, edit, or create a new profile

Getting Here - Manage & Settings > Blades > Inspection Settings > Profiles

Inspection Settings - Profile

What can I do here?

Use this window to edit a new profile.

Getting Here - Manage & Settings > Blades > Inspection Settings > Profiles > double-click a new profile

Inspection Settings - Gateways

What can I do here?

Use this window to see the profiles assigned to gateways.

Getting Here - Manage & Settings > Blades > Inspection Settings > Gateways

Gateway Profile Assignment

What can I do here?

Use this window to change the profile assigned to the selected gateway.

Getting Here - Manage & Settings > Blades > Inspection Settings > Gateway > Edit
Or:
Security Policies > Shared policies > Geo Policy > Gateways > Edit
Or:
Security Policies > Threat Prevention > Custom Policy Tools > IPS Protections > In Filter, under Type, select Core > Open a core protection > Gateways page > Double click a gateway in the table

Inspection Settings - Exceptions

What can I do here?

Use this window to view exceptions to the Inspection Settings.

Getting Here - Manage & Settings > Blades > Inspection Settings > Exceptions

New Exception Rule

What can I do here?

Use this window to create exception rules for Inspection Settings.

Getting Here - Manage & Settings > Blades > Inspection Settings > Exceptions > New Exception rule
Or:
Security Policies > Shared Policies > Geo Policy > Exceptions

Application Control and URL Filtering - Advanced Settings - General

What can I do here?

Use this window to configure general settings for the Application Control and URL Filtering Software Blade. These are global settings that apply to all Security Gateways with Application Control and URL Filtering enabled.

Getting Here - Manage & Settings > Blades > Application Control and URL Filtering > Advanced Settings > General

Advanced Settings in SmartConsole connected to a Multi-Domain Server

Note - When you open *Manage & Settings > Blades > Application Control and URL Filtering > Advanced Settings*from a SmartConsole connected to a Multi-Domain Server, only this section shows.

Services

By default, HTTPS traffic on port 443 and HTTP and HTTPS proxy on port 8080 is inspected. You can include more services and ports in the inspection by adding them to the services list.

To select other HTTPS/HTTP services, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of services and select a service. Other services, such as SSH are not supported.

Web Browsing

If you do not enable URL Filtering on the Security Gateway, you can use a generic Web browser application called **Web Browsing** in the rule.

This application includes all HTTP traffic that is not a defined application. Because Web Browsing traffic can generate many logs, the Web browsing application has its own activation setting.

Application Control and URL Filtering assigns **Web Browsing** as the default application for all HTTP traffic that does not match an application in the Application Control and URL Filtering Database. The **Web Browsing** application is activated by default.

If you deactivate the Web browsing application:

- **Web Browsing** in Access Control Policy rules is not enforced. For example, if you have a rule that blocks **Web Browsing**, traffic is allowed.
- No **Web Browsing** logs are generated.

To deactivate the Web Browsing application:

1. Go to **Manage & Settings > blades > Application and URL Filtering > Advanced Settings**.
2. Deselect **Enable web browsing logging and policy enforcement**.

Fail Mode

You can select the enforcement option to use if the Application Control and URL Filtering engine fails during inspection.

To select the enforcement option

1. Go to **Manage & Settings** > **Blades** > **Application Control and URL Filtering** > **Advanced Settings**.
2. In the **Application Settings** window, select one option:
   - **Allow all requests (fail-open)** - All traffic is allowed.
   - **Block all requests (fail-close)** - All traffic is blocked (default).

URL Filtering

In this section of the **Application Settings** window, you can enable these URL Filtering features:

- Categorize HTTPS sites (without activating HTTP inspection).
- Enforce safe search in search engines.
- Categorize cached pages and translated pages in search engines.

Categorize HTTP sites

This option lets Application Control and URL Filtering assign categories to HTTPS sites without activating HTTPS inspection. It assigns a site category based on its domain name and whether the site has a valid certificate. If the server certificate is:

- **Trusted** - Application Control and URL Filtering gets the domain name from the certificate and uses it to categorize the site.
- **Not Trusted** - Application Control and URL Filtering assigns a category based on the IP address.

Application Control and URL Filtering uses these pages (in the SmartConsole **Manage & Settings** tab > **Blades** > **HTTPS Inspection** > **Configure in SmartDashboard**) to make sure that a certificate is valid:

- **Trusted CAs** page - Makes sure the certificate is not stolen or revoked.

  Note : If your company issues certificates, you must add your company CA to the list of Trusted CAs.

- **HTTPS Validation** page - If the certificate is blacklisted, for example, it is not trusted and the site categorized according to its IP address.

  Important - Application Control and URL Filtering gets the site URL from the SSL "CONNECT" request sent to the proxy, if:
  - There is a proxy between the Firewall and the destination site or
  - The Firewall is configured to work as a proxy

When the **Categorize HTTPS sites** option is selected, these settings from the HTTPS validation page are applied:

- **Certificate Blacklisting**
- **Automatically retrieve intermediate certificate**

Enforce safe search in search engines

Select this option to require use of the safe search feature in search engines. When activated, the URL Filtering Policy uses the strictest available safe search option for the specified search engine. This option overrides user specified search engine options to block offensive material in search results.

Categorize cached pages and translated pages in search engines

Select this option to assign categories to cached search engine results and translated pages. When this option is selected, Application Control and URL Filtering assigns categories based on the original Web site instead of the **'search engine pages'** category.

Connection Unification

Application Control and Web site traffic generate a large quantity of logs. To make logs manageable, Application Control and URL Filtering consolidates logs by session. A session is a period that starts when the user first connects to an application or site. The Security Gateway generates one log entry for each application or site accessed during the session. All actions that occur during are included in the log.

To change the length of a session:

1. Go to **Manage & Settings** > **Blades** > **Application Control and URL Filtering** > **Advanced Settings**.
2. In the **Application Settings** window:
   - For applications and sites that are allowed in a Rule Base, the default session is three hours (180 minutes). To change this, click **Session Unification Timeout** and enter a different value, in minutes.
   - For applications and sites that are blocked in the Rule Base, the default session is 30 seconds. You cannot change this setting.

Application Control Web Browsing Services

Application Control Web browsing services are the services that match a Web-based custom **Application/Site**.

These are the default Application Control Web browsing services:

- `http` on port 80
- `https` on port 443
- `HTTPS_proxy` on port 8080
- `HTTP_proxy` on port 8080

Other services, such as SSH are not matched.

To add to the list of services that match Web applications:

1. Go to **Manage & Settings** > **Blades** > **Application Control and URL Filtering** > **Advanced Settings**.
2. In the **Application Control and URL Filtering Settings** window:
   a. Click the add icon + to open the list of services.
   b. Select a service.

Application Port Match

Match Web application on 'Any' port when used in Block rule - By default, this is selected, and applications are matched on all services when used in a Block rule.

Domain Level Permissions

Selecting this option allows the editing of applications, categories, and services used in the Global Domain.

Web Browsing

If you do not enable URL Filtering on the Security Gateway, you can use a generic Web browser application called **Web Browsing** in the rule.

This application includes all HTTP traffic that is not a defined application. Because Web Browsing traffic can generate many logs, the Web browsing application has its own activation setting.

Application Control and URL Filtering assigns **Web Browsing** as the default application for all HTTP traffic that does not match an application in the Application Control and URL Filtering Database. The **Web Browsing** application is activated by default.

If you deactivate the Web browsing application:

- **Web Browsing** in Access Control Policy rules is not enforced. For example, if you have a rule that blocks **Web Browsing**, traffic is allowed.
- No **Web Browsing** logs are generated.

To deactivate the Web Browsing application:

1. Go to **Manage & Settings > blades > Application Control and URL Filtering > Advanced Settings**.
2. Deselect **Enable web browsing logging and policy enforcement**.

HTTP Inspection

Enable HTTP inspection on non standard ports for Application Control and URL filtering - Applications that use HTTP normally send the HTTP traffic on TCP port 80. Some applications send HTTP traffic on other ports also.

By default, the Application Control and URL Filtering Software Blades inspect HTTP traffic on non-standard ports.

You can configure the Application Control and URL Filtering Software Blades to only inspect HTTP traffic on port 80.

Compatibility with R75 and R75.10 Gateway Settings

These settings are for compatibility with Security Gateway versions earlier than R75.20:

- **Unify connections from the same user/IP to a specific application into a single session/log**
  - Select this to unify logs for all application traffic during a session into one log. This is the default.
  - Clear this to generate one log for each connection or activity during a session
- **Issue a separate log per each domain accessed**

  Optional: When you select the **Unify connections** option, this additional option is available:
  - When cleared, connections of the **Web Browsing** application from a user or IP address during a session are consolidated into one log record. This is the default.
  - When selected, connections of the **Web Browsing** application generate one log for each domain that a user or IP address browses to, for each session.

Application Control and URL Filtering - Check Point Online Web Service

What can I do here?

Use this window to configure Check Point online web service settings.

Getting Here - Manage & Settings > Blades > Application Control and URL Filtering > Advanced Settings > Check Point online web service

Check Point Online Web Service

The Check Point Online Web Service is used by the URL Filtering engine for updated website categorization and by the Application Control engine for updated Widget definitions. The responses the Security Gateway gets are cached locally to optimize performance.

- **Block requests when the web service is unavailable**
  - When selected, requests are blocked when there is no connectivity to the Check Point Online Web Service.
  - When cleared, requests are allowed when there is no connectivity (default).
- **Website categorization mode** - You can select the mode that is used for website categorization:
  - **Background - requests are allowed until categorization is complete** - When a request cannot be categorized with a cached response, an uncategorized response is received. Access to the site is allowed. In the background, the Check Point Online Web Service continues the categorization procedure. The response is then cached locally for future requests (default). This option reduces latency in the categorization procedure.
  - **Hold - requests are blocked until categorization is complete** - When a request cannot be categorized with the cached responses, it remains blocked until the Check Point Online Web Service completes categorization.
  - **Custom - configure different settings depending on the service** -Lets you set different modes for URL Filtering and Social Networking Widgets. For example, click **Customize** to set URL Filtering to Background mode and Social Networking Widgets to Hold mode.
- **Categorize Social Network Widgets**
  - When selected, the Security Gateway connects to the Check Point Online Web Service to identify social networking widgets that it does not recognize (default).
  - When cleared or there is no connectivity between the Security Gateway and the Check Point Online Web, the unknown widget is treated as Web Browsing traffic.

Content Awareness

What can I do here?

Use this window to configure advanced settings for Content Awareness. These are global settings that apply to all Security Gateways with Content Awareness enabled.

Getting Here - Manage & Settings > Blades > Content Awareness > Advanced Settings

Fail Mode

You can select the enforcement option to use if the Content Awareness engine fails during inspection. However, if the engine fails on a connection that is inspected for logging only, the connection is allowed.

This setting is for R80.10 Gateways and higher.

To select the enforcement option

1. Go to **Manage & Settings** > **Blades** > **Content Awareness** > **Advanced Settings**.
2. In the **Content Awareness Settings** window, select one option:
   - **Allow all requests (fail-open)** - All traffic with data is allowed.
   - **Block all requests (fail-close)** - All traffic with data is blocked. *This is the default.*

Content Awareness Services

Specify the services that Content Awareness inspects. Content Awareness inspects these services by default:

- `HTTPS_proxy` on port 8080
- `HTTP_proxy` on port 8080
- `ftp` on port 21
- `http` on port 80
- `https` on port 443
- `smtp` on port 25

To add to the list of services that match rules with Content Awareness:

1. Go to **Manage & Settings** > **Blades** > **Content Awareness** > **Advanced Settings**.
2. In the **Content Awareness Settings** window:
   a. Click the add icon + to open the list of services.
   b. Select a service.

Data Inspection

Inspect archives -examine the content of archive files. For example, files with the extension .zip, .gz, .tgz, .tar.Z, .tar, .lzma, .tlz, 7z, .rar

HTTP Inspection

Enable HTTP inspection on non standard ports for Content Awareness -

Servers usually send HTTP traffic on TCP port 80. Some servers send HTTP traffic on other ports also. By default, this setting is enabled and Content Awareness inspects HTTP traffic on non-standard ports. You can disable this setting and configure Content Awareness to inspect HTTP traffic only on port 80.

Threat Prevention Engine Settings - General

What can I do here?

Use this window advanced settings for Threat Prevention such as:

- Fail mode in case of internal system error
- Check Point Online Web Service
- Connection Unification timeout
- HTTP Inspection

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > Threat Prevention Engine Settings window > General page

Engine Settings

Fail Mode

Select the behavior of the ThreatSpect engine if it is overloaded or fails during inspection. For example, if the Anti-Bot inspection is terminated in the middle because of an internal failure. By default, in such a situation all traffic is allowed.

- **Allow all connections (Fail-open)** - All connections are allowed in a situation of engine overload or failure (default).
- **Block all connections (Fail-close)** - All connections are blocked in a situation of engine overload or failure.

Check Point Online Web Service

The Check Point Online Web Service is used by the ThreatSpect engine for updated resource categorization. The responses the Security Gateway gets are cached locally to optimize performance.

- **Block connections when the web service is unavailable**
  - When selected, connections are blocked when there is no connectivity to the Check Point Online Web Service.
  - When cleared, connections are allowed when there is no connectivity (default).
- **Resource categorization mode** - You can select the mode that is used for resource categorization:
  - Background - connections are allowed until categorization is complete - When a connection cannot be categorized with a cached response, an uncategorized response is received. The connection is allowed. In the background, the Check Point Online Web Service continues the categorization procedure. The response is cached locally for future requests (default).
    This option reduces latency in the categorization process.
  - Hold - connections are blocked until categorization is complete - When a connection cannot be categorized with the cached responses, it remains blocked until the Check Point Online Web Service completes categorization.
  - **Custom - configure different settings depending on the service** - Lets you set different modes for Anti-Bot and Anti-Virus. For example, click **Customize** to set Anti-Bot to Hold mode and Anti-Virus to Background mode.

Connection Unification

Gateway traffic generates a large amount of activity. To make sure that the amount of logs is manageable, by default, logs are consolidated by session. A session is a period that starts when a user first accesses an application or site. During a session, the gateway records one log for each application or site that a user accesses. All activity that the user does within the session is included in the log.

For connections that are allowed or blocked in the Anti-Bot and Anti-Virus Rule Base, the default session is 10 hours (600 minutes). To change this, click Session Timeout and enter a different value.

HTTP Inspection

Enable HTTP inspection on non-standard ports for Threat Prevention blades.

Check Point Online Web Service - Custom

What can I do here?

Use this window to set different modes for resource categorization.

> **Getting Here** - Manage & Settings > Blades > Threat Prevention > Advanced Settings > General > Check Point Online Web Service > Custom option > Customize.

Resource Categorization Mode Options

- **Background - requests are allowed until categorization is complete** - When a request cannot be categorized with a cached response, an uncategorized response is received. Access to the site is allowed. In the background, the Check Point Online Web Service continues the categorization procedure. The response is then cached locally for future requests (default). This option reduces latency in the categorization procedure.
- **Hold - requests are blocked until categorization is complete** - When a request cannot be categorized with the cached responses, it remains blocked until the Check Point Online Web Service completes categorization.

Anti-Bot

What can I do here?

Use this window to exclude internal emails or email domains from Anti-Bot scanning.

Emails that are sent to external networks are scanned by the Suspicious Mail engine. Depending on your topology, internal emails are also scanned. You can create a list of email addresses or domains that are not be inspected by Anti-Botand exclude internal emails.

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > Anti-Bot

Threat Prevention - Threat Emulation Settings

What can I do here?

Use this window to configure Threat Emulation settings such as File Type support and Emulation Limits.

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > Threat Emulation

Emulation Limits

To prevent too many files that are waiting for emulation, configure these emulation limits settings:

- Maximum file size
- Maximum time that the Software Blade does emulation

- Maximum time that a file waits for emulation in the queue (for Threat Emulation appliance only)

If emulation is not done on a file for one of these reasons, the Fail Mode settings for Threat Prevention define if a file is allowed or blocked.

You can configure the maximum amount of time that a file waits for the Threat Emulation Software Blade to do emulation of a file. There is a different setting that configures the maximum amount of time that emails are held in the MTA.

If the file is waiting for emulation more than the maximum time:

- Threat Emulation Software Blade - The Threat Prevention profile settings define if a file is allowed or blocked
- MTA - The MTA settings define if a file is allowed or blocked

Configuring Emulation Limits

1. In SmartConsole, select **Manage & Settings > Blades > Threat Prevention > Advanced Settings**.

   The **Threat Emulation Engine Settings** window opens.

2. Click **Configure settings**.

   The **Threat Emulation Settings** window opens.

3. Configure the settings for the emulation limits.

   - From When limit is exceeded traffic is accepted with track, select the action if a file is not sent for emulation:
   - None - No action is done
   - Log - The action is logged
   - Alert - An alert is sent to SmartView Monitor

4. Click **OK** and then install the policy.

Changing the Local Cache

When a Threat Emulation analysis finds that a file is clean, the file hash is saved in a cache. Before Threat Emulation sends a new file to emulation, it compares the new file to the cache. If there is a match, it is not necessary to send it for additional emulation. Threat Emulation uses the cache to help optimize network performance.

Best Practice - Do not change this setting.

Changing the Size of the Local Cache

1. In SmartConsole, select **Manage & Settings > Blades > Threat Prevention > Advanced Settings**.

   The **Threat Prevention Engine Settings** window opens.

2. Click **Configure Settings**.

   The **Threat Emulation Settings** window opens.

3. From **Number of file hashes to save in local cache**, configure the number of file hashes that are stored in the cache.

4. Click **OK** and then install the policy.

Threat Emulation - File Type support

What can I do here?

Select supported file types for Threat Emulation. The selected file types show in the Threat Prevention profile settings.

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > Threat Emulation > File Type support > Configure

Proxy Configuration

What can I do here?

Use this window to configure a proxy server.

Getting Here - Security Policies > Access Control/Threat Prevention > Policy > Access Tools > Updates > "Configure Proxy" link in notification message
Or:
Manage & Settings > Blades > Threat Prevention > Advanced Settings > Threat Emulation >
File Type support > Configure > "Configure Proxy" link in notification message
Note - the proxy link shows only if no proxy configured.

Threat Prevention Engine Settings - Threat Extraction

What can I do here?

Use this window to configure file type support and mail signatures for threat extraction.

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > Threat Extraction

Threat Extraction - Supported File Types

What can I do here?

Use this window to select file types supported by Threat Extraction.

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > Threat Extraction > Configure File Type Support

Configuring File Type Support

To configure file type support:

1. In the **Threat Prevention Engine Settings** window > **Threat Extraction**, click **Configure File Type Support**.

   The **Threat Extraction Supported File Types** window opens.
2. From the list select the file types which the Threat Extraction blade supports.
3. Click **OK**.

Threat Extraction - Configure Mail Signatures

What can I do here?

Use this window to configure mail signatures for Threat Extraction.

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > Threat Prevention Engine Settings window > Threat Extraction > Configure Mail Signatures

Configuring Mail Signatures

To configure mail signatures:

1. In the **Threat Prevention Engine Settings** window > **Threat Extraction**, click **Configure Mail Signatures**.

   The **Threat Extraction Mail Signatures** window opens.

   Use this window to configure text for:

   - **Mail signatures for attachments with potential threats extracted**

     The first signature is always attached to an email that had threats extracted.

     The second signature is added to the first if the email recipient has access to the original file.

   - **Mail signatures for unmodified attachments**

     You can insert predefined field codes into the signature text, such as:

     - A link to the file before it was modified by the blade.

     The link opens the UserCheck Portal. The portal shows a list of attachments the recipient can download.

     - Reference ID.

     Use this ID to send the file to the recipient. You can also find the ID in the logs.

     On the gateway, run the command: `scrub send_orig_email`.

2. Click **OK**.

Threat Prevention Engine Settings - UserCheck

What can I do here?

Use this window to configure UserCheck approved page and canceled page.

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > UserCheck

Threat Prevention Engine Settings - External Feed Retrieval

What can I do here?

Use this window to configure when external custom intelligence feeds are fetched.

The default feed interval is set to 5 minutes and enforced immediately on the gateway with no need to install policy

What background information do I need to know?

Custom Intelligence Feeds lets you fetch feeds from a third-party server directly to the Security Gateway to be enforced by the Anti-Virus and Anti-Bot blades. The Custom Intelligence Feeds feature helps you manage and monitor indicators with minimal operational overhead.

Getting Here - Manage & Settings > Blades > Threat Prevention > Advanced Settings > External Feed

Revisions

What can I do here?

In this view you can see the history of published all changes to configuration settings in your deployment. You can see:

- The status of each session after the change was published
- The session name and tags
- The administrator who published the changes
- The time and date of the changes
- Generate a report of session changes

You can:

- Launch SmartConsole in read-only mode to see the selected session
- Verify of a revert to a previous version of the database is possible, and probable consequences. (Actions > Revert to this revision > step 2)
- Revert to an earlier version of the database (Actions > Revert to this revision > step 4)
- Purge (delete) all data older than the selected session

Getting Here - Manage & Settings > Sessions > Revisions > Actions > Revert to this Revision
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Sessions > Revisions > Revert to this Revision
Or:
Install Policy > Select a Policy > View Changes link

Working with Database Revisions

The Security Management architecture has built-in revisions. Each publish operation creates a new revision which contains only the changes from the previous revisions.

Benefits of the revision architecture:

- Safe recovery from a crisis, restore a Domain to a good known revision (see Notes below).
- Fast policy verification, based on the difference between installed versions
- More efficient Management High Availability.

Important - Before using the revision feature consider these limitations:

- 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 all of their private sessions.

Best Practices:

1. It is recommended to update the IPS and Application Control signatures and install the policy after the revert. Install policy if changes to log destinations are applied.
2. If it is necessary to restore a full environment to a certain point in time, use **Restore Backup**. All work done after the backup is lost. To learn more, see the: *R81.10 Gaia Administration Guide*
3. We recommend to purge irrelevant revisions. Accumulating too many revisions can create a heavy load on the server, which may cause disk and performance issues.

Notes - Revision is not supported in these scenarios:

- The Endpoint Security Management Server is enabled.
- VSX configuration or related networks differ between the source and target revisions.
- A new Domain Management Server or a Check Point object was created or deleted after the target revision date.
- The corresponding revision of the Global Domain, or the IPS or Application Control components was purged.

To see saved database versions:

In SmartConsole, go to **Manage & Settings** > **Sessions** > **Revisions**.

To see the changes made during a specific revision:

1. Go to **Manage & Settings > Sessions > Revisions**, and select a revision.

   The bottom pane shows the audit logs of the changes made in the revision.

2. **Optional:** Click **View**.

   A separate read-only SmartConsole session opens.

To revert to an earlier revision

1. Go to **Manage & Settings > Sessions > Revisions**, and select a revision.
2. In **Actions**, click **Revert to this Revision**.

   The **Revert to Revision** wizard opens.

To delete all versions of the database that are older than the selected version:

1. Go to **Manage & Settings > Sessions > Revisions**, and select a revision.
2. In **Actions**, click **Purge**.
3. In the confirmation window that opens, click **Yes**.

Important - Purge is irreversible. When you purge, that revision and older revisions are deleted.

Use Case - Managing a Crisis Using Database Revisions

A network problem occurs after downloading a Threat Prevention update and installing it on gateways.

Solution

1. From **Security Policies** > **Threat Prevention** > **Custom Policy Tools** > **Updates**, in the **IPS** section, select an update that is known to be good.
2. Click **Switch to Version**.
3. Install the Threat Prevention Policy.

The Gateway gets that version of the IPS protections. Other network objects and policies do not change.

Managing a Crisis Using Database Revisions

Use Case	Solution
Network problem after downloading a Threat Prevention update and installing it on gateways.	1. From **Security Policies** > **Threat Prevention** > **Custom Policy Tools** > **Updates**, in the **IPS** section, choose an update that is known to be good. 2. Click **Switch to Version**. 3. Install the Threat Prevention Policy. The Gateway gets that version of the IPS protections. Other network objects and policies do not change.

More Database Revision Scenarios:

- Need a full environment restore to a certain point in time.

  Best Practice - Use **Restore Backup**. All work done after the backup is lost. To learn more, see the: *R81.10 Gaia Administration Guide*

Revision Options

The **Revisions** view shows this information about each revision:

- **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** - Of the changes

The list shows the versions by number.

- The **Summary tab** pane shows a brief summary of the changes made in each version.
- Right-clicking a version in the list lets you purge the selected revision and revisions older than the one selected. All data from the selected revision and those prior to it are deleted. The revert operation returns the Rule Base to an earlier version but does not:
  - Revert network objects to their earlier versions.
  - Revert CA data.
  - Create a report of the expected outcome of the operation, as in R77 and lower.

- Right-clicking a version and selecting **View** from the menu opens a new instance of SmartConsole in read-only mode.

  The new instance of SmartConsole lets you see the state of the database at the time the version was created.

Important - Version control is not supported when the Security Management Server database contains VSX objects.

In a Multi-Domain environment, the list shows the revisions made to the domain SmartConsole is connected to.

Revision Details

What can I do here?

Use this window to see or edit a description of the revision details.

Getting Here - Manage & Settings > Revisions > Edit
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Revisions > Edit

Revert to Revision

What can I do here?

Use this wizard to revert to a previous revision. The wizard verifies if a revision is possible and lists the consequences of returning to an earlier version of the database.

Getting Here - Manage & Settings > Sessions > Revisions > Actions > Revert to this Revision
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Sessions > Revisions > Revert to this Revision

Verify Revert - Task Details

What can I do here?

Use this window to see a summary of the revert task details. The details window shows warnings and explains the consequences of reverting to an earlier version of the database.

Getting Here - SmartConsole connected to Security Management Server or Multi-Domain Server > Recent Tasks window > Details link

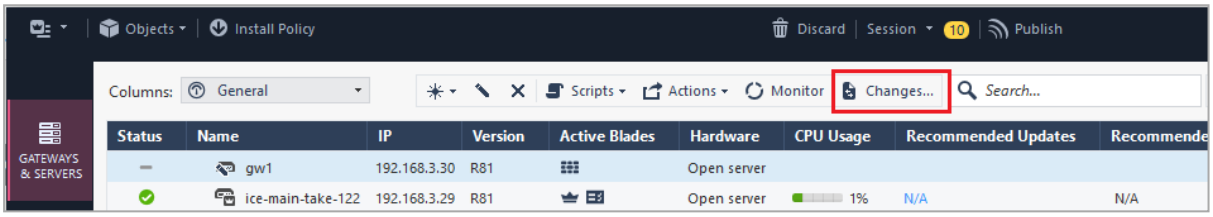
Session Changes

You can generate a report to show you the changes made in a specific session, it can be your current session or a different one. Tracking the changes made in sessions lets you track and monitor the changes made, and troubleshoot bugs.

To view the changes made in your current session:

Click the **Changes** button in the toolbar of one of these views:

- The **Security Policies** view > Threat Prevention policy and Access Control policy
- The **Gateways & Servers** view



A report is generated which shows the changes made in the current private session.

To view the changes made in any session of your choice:

1. In SmartConsole, go to the **Manage & Settings** view > **Sessions** > **View Sessions.**

   The list of sessions appears.

2. Click on the required session,

3. Click the **Changes** button in the toolbar.

   A changes report is generated. The report shows a comparison between the selected private sessions.

Note - There is inconsistency between the number of changes which appears in the session toolbar and the Revisions view.

Getting Here - SmartConsole > Gateways & Servers
or
Manage & Settings > Sessions > View Sessions or Revisions

Management API Settings

What can I do here?

Use this window to configure startup settings, server settings, and access settings for the API server.

Getting Here - Manage & Settings > Blades > Management API > Advanced Settings

API

You can configure and control the Management Server through API Requests you send to the API Server that runs on the Management Server.

The API Server runs scripts that automate daily tasks and integrate the Check Point solutions with third party systems, such as virtualization servers, ticketing systems, and change management systems.

To learn more about the management APIs, to see code samples, and to take advantage of user forums, see:

- The API Documentation:
  - Online - *Check Point Management API Reference* (at the top, select the correct version)
  - Local - `https://<Server IP Address>/api_docs`

    By default, access to the local API Documentation is disabled. Follow the instructions in sk174606.

    Note - On a Standalone server (a server which runs both a Security Management Server and a Security Gateway), the API Documentation web portal (`https://<Server IP Address>/api_docs`) stops working when you open SmartView Web Application (`https://<Server IP Address>/smartview`).
- The **Developers Network** section of *Check Point CheckMates Community*.

API Tools

You can use these tools to work with the API Server on the Management Server:

- Standalone management tool, included with Gaia operating system:

  `mgmt_cli`
- Standalone management tool, included with SmartConsole:

  `mgmt_cli.exe`

  You can copy this tool from the SmartConsole installation folder to other computers that run Windows operating system.
- Web Services APIs that allow communication and data exchange between the clients and the Management Server over the HTTP protocol.

  These APIs also let other Check Point processes communicate with the Management

Server over the HTTPS protocol.

`https://<IP Address of Management Server>/web_api/<command>`

Configuring the API Server

To configure the API Server:

1. Connect with SmartConsole to the Security Management Server or applicable Domain Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. In the upper left section, click **Blades**.
4. In the **Management API** section, click **Advanced Settings**.

   The **Management API Settings** window opens.
5. Configure the **Startup Settings** and the **Access Settings**.

   Configuring Startup Settings

   Select **Automatic start** to automatically start the API server when you start or reboot the Management Server.

   Notes:
   - If the Management Server has more than 4GB of RAM installed, the **Automatic start** option is activated by default during Management Server installation.
   - If the Management Server has less than 4GB of RAM, the **Automatic Start** option is deactivated.

Configuring Access Settings

Select one of these options to configure which clients can connect to the API Server:

- **Management server only** - Only the Management Server itself can connect to the API Server. This option only lets you use the `mgmt_cli` utility on the Management Server to send API requests. You cannot use SmartConsole or Web services to send API requests.
- **All IP addresses that can be used for GUI clients** - You can send API requests from all IP addresses that are defined as **Trusted Clients** in SmartConsole. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.
- **All IP addresses** - You can send API requests from all IP addresses. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.

6. Click **OK**.
7. In the upper left section, click **Permissions & Administrators**.
8. In the object of each applicable Administrator, make sure the assigned Permission Profile allows access to Management API.

   Instructions

   a. Edit the Administrator object.

   b. In the left panel, click **General**.

   c. In the **Permissions** section, on the right side of the selected Permission Profile, click the eye icon.

      The Permission Profile object opens in the read-only view.

   d. In the left panel, click **Management**.

   e. The permission **Management API Login** has to be selected.

      If it is not selected, then close this window and edit this Permission Profile object.

   f. Click **Close**.

9. Publish the SmartConsole session.
10. Restart the API Server on the Management Server with this command:

```
api restart
```

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

- The output of this command must show:

```
API started successfully
```

11. Examine the status of the API server on the Management Server with this command:

```
api status
```

Notes:

- The output of this command must show:

```
----------------------------------------------
Overall API Status: Started
----------------------------------------------

API readiness test SUCCESSFUL. The server is up and ready
to receive connections
```

- The output this command may show the state of the "**API**" process as "**Stopped**" when the API access is set to "**All IP addresses that can be used for GUI clients**", and more than 200 Trusted Clients are configured:

```
Processes:

Name       State     PID       More Information
-----------------------------------------------
API        Stopped   ...
```

Tags

What can I do here?

Use this window to create or edit tags.

Getting Here - Manage & Settings > Tags
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Tags

Sync with User Center

What can I do here?

Use this window to add information regarding your environment to User Center, such as gateway name, version, and active blades. Check Point uses this additional information for better inventory management, pro-active support, and more efficient ticket resolution.

To learn more, see sk94064

Getting Here - Manage & Settings > Sync with User Center

Preferences

What can I do here?

Use this window to configure:

- **Network Management** - which type of IP address and subnet mask formats show in SmartConsole
- **Subnet Display Format** - set the subnet display format
- **Network defined by routes** - The gateway dynamically calculates the topology behind the selected interface every second (default value). Set here, the update interval applies globally to all interfaces on all gateways of version R80.10 and higher.
- **Domain Management** - Select the domain server display for format.
- **Login message** - set a custom login message and format
- **User Preferences** - to restore message boxes were set to not be shown again, and debug the SmartConsole application.
- **SmartConsole Extensions** - lets you embed web-applications within SmartConsole. For more, see: SmartConsole Extensions
- **Language** - Localize your SmartConsole to your region's language
- **Accessibility** - Turns on the high-contrast color theme if you have difficulty reading text in the default theme.

Getting Here - Manage & Settings > Preferences
Or:
SmartConsole for Multi-Domain Server > Multi Domain > Preferences

Setting IP Address Versions of the Environment

Many objects and rules use IP addresses. Configure the version that your environment uses to see only relevant options.

To set IP address version:

1. Click **Manage & Settings**.
2. Click **Preferences**.
3. Select the IP address version that your environment uses: **IPv4**, **IPv6**, or **IPv4 and IPv6**.
4. Select how you want to see subnets: **Mask Length** or **Subnet Mask**.

User Preferences

Some windows in the SmartConsole offer administrators the option to not see the window again. You can undo this selection, and restore all windows to show again.

This option is available only if administrators selected **do not show** in a window.

To restore windows from "do not show":

1. Click **Manage & Settings**.
2. Click **Preferences**.
3. In the **User Preferences** area, click **Restore All Messages**.

Login Message

Administrators in your environment use SmartConsole daily. Customize the Login window, to set the environment to comply with your organization's culture.

To customize the Login window:

1. Click **Manage & Settings**.
2. Click **Preferences** > **Login Message**.

   The **Login Message** window opens.
3. Select **Show custom message during login**.
4. In **Customize Message**, enter a **Header** and **Message** for administrators to see.

   The default suggestion is:

   ```
   Warning
   ```

```
This system is for authorized use only
```

5. If you want the message to have a warning icon, in **Customize Layout**, select **Add warning sign**.
6. If you want the Login window to show your organization's logo, in **Customize Layout**, select **Add logo** and then **Browse** to an image file.

Debugging SmartConsole

1. Click **Start Debugging**.
2. Reproduce the problem.
3. Stop debugging.
4. Send the generated log file to Check Point when requested.

SmartConsole Extensions

SmartConsole Extensions is an open platform within SmartConsole which allows it to integrate with web-based interfaces of other systems. For example, you can create a web-interface for an existing ticketing system, and integrate it within SmartConsole so that associated tickets are seen for every rule in the Rule Base.

Customers, vendors, and third-parties can develop their own Extensions to integrate into SmartConsole.

Importing Extensions into SmartConsole

The client system that runs SmartConsole saves installed Extensions locally. You must install Extensions on each client system that runs SmartConsole.

To import an extension:

1. On SmartConsole, go to **Manage & Settings** > **Preferences** > **SmartConsole Extensions** > **+**.

   The **Import SmartConsole Extension** window opens.

2. Enter the web-service manifest URL for the manifest file and click **OK**. The URL must be an HTTPS URL.

   Note -When the hosting server uses an invalid SSL certificate (self-signed), it prompts an **Invalid Certificate** confirmation window. Confirm the server's fingerprint against the SSL certificate which runs the Extension by selecting **View Certificate**. On the **Certificate** window, you can enable trust for this certificate with a click on **Install Certificate** to use the **Certificate Import Wizard**.

SmartConsole retrieves the manifest file and displays these Extension details in the **SmartConsole Extension Installation** window:

Parameter Name	Description	Example
Name	Extension displayed name	Demo Extension
Provider	The URL for the Extension service entry point	ACME Labs
Server Name	The Extension provider hosting server name	acme.com
Certificate	Server Certificate	
Required Permission	The required accessibility which Extension request to acquire	Read relevant objects from the installed location

You can disable Extensions from SmartConsole. To disable an Extension, clear the box next to the Extension name. To uninstall an Extension, select the Extension and click the X above the Extension list. You do not need to restart SmartConsole to install, uninstall, enable, or disable Extensions.

Configuring Extension Settings

To configure the Extension settings:

In SmartConsole, go to **Manage & Settings** > **Preferences** > **SmartConsole Extensions**, double-click the Extension you imported. The Settings window for the Extension opens:

- The **Extension Key** allows any string you enter to identify the Extension.
- **Key Data** allows developers to customize the extensions through these keys, such as choosing a color theme.

Certified Check Point Extensions and Development

Extensions reviewed and verified by Check Point are distinguished by a green check sign.

To learn more about developing extensions, see the SmartConsole Extension Developer Guide.

SmartConsole Extension Installation

What can I do here?

Use this window to install the extension in SmartConsole

Getting Here - Manage & Settings > Preferences > Click (+) and enter the extension URL

SmartConsole Extensions

SmartConsole Extensions is an open platform within SmartConsole which allows it to integrate with web-based interfaces of other systems. For example, you can create a web-interface for an existing ticketing system, and integrate it within SmartConsole so that associated tickets are seen for every rule in the Rule Base.

Customers, vendors, and third-parties can develop their own Extensions to integrate into SmartConsole.

Importing Extensions into SmartConsole

The client system that runs SmartConsole saves installed Extensions locally. You must install Extensions on each client system that runs SmartConsole.

To import an extension:

1. On SmartConsole, go to **Manage & Settings** > **Preferences** > **SmartConsole Extensions** > **+**.

   The **Import SmartConsole Extension** window opens.

2. Enter the web-service manifest URL for the manifest file and click **OK**. The URL must be an HTTPS URL.

   Note -When the hosting server uses an invalid SSL certificate (self-signed), it prompts an **Invalid Certificate** confirmation window. Confirm the server's fingerprint against the SSL certificate which runs the Extension by selecting **View Certificate**. On the **Certificate** window, you can enable trust for this certificate with a click on **Install Certificate** to use the **Certificate Import Wizard**.

SmartConsole retrieves the manifest file and displays these Extension details in the **SmartConsole Extension Installation** window:

Parameter Name	Description	Example
Name	Extension displayed name	Demo Extension
Provider	The URL for the Extension service entry point	ACME Labs
Server Name	The Extension provider hosting server name	acme.com
Certificate	Server Certificate	
Required Permission	The required accessibility which Extension request to acquire	Read relevant objects from the installed location

You can disable Extensions from SmartConsole. To disable an Extension, clear the box next to the Extension name. To uninstall an Extension, select the Extension and click the X above the Extension list. You do not need to restart SmartConsole to install, uninstall, enable, or disable Extensions.

Configuring Extension Settings

To configure the Extension settings:

In SmartConsole, go to **Manage & Settings** > **Preferences** > **SmartConsole Extensions**, double-click the Extension you imported. The Settings window for the Extension opens:

- The **Extension Key** allows any string you enter to identify the Extension.
- **Key Data** allows developers to customize the extensions through these keys, such as choosing a color theme.

Certified Check Point Extensions and Development

Extensions reviewed and verified by Check Point are distinguished by a green check sign.

To learn more about developing extensions, see the SmartConsole Extension Developer Guide.

SmartConsole Extension Window

What can I do here?

To understand how to use this window, see the documentation provided by the extension developer.

Getting Here - To understand how to use this window, see the documentation provided by the SmartConsole extension developer.

Extension Settings

What can I do here?

Use this window to add an extension key and change key data.

- The **Extension Key** can be any string you enter to identify the extension by.
- **Key Data** - The extension developer may let you customize the extension through these keys. The developer will send details of what can be customized, for example the color theme.

Getting Here - Manage & Settings > Preferences > SmartConsole Extensions

Extension Changes

What can I do here?

Use this window to approve changes submitted by a SmartConsole extension.

Getting Here - Window shows whenever an extension submits a request

Extension Details

What can I do here?

To understand how to use this window, see the documentation provided by the extension developer.

Getting Here - List of extensions shown in some editor windows.

Tags Management

What can I do here?

Use this window to edit tags or create new ones.

Getting Here - Manage & Settings > Preferences > Tags Management > New or Edit

SmartTasks

What can I do here?

Use this window to create, edit, or delete SmartTasks.

Getting Here - Manage & Settings > Preferences > Tasks > SmartTasks > New or Edit

SmartTask Overview

Management SmartTasks let you configure automatic actions according to different triggers in the system. A SmartTask is a combination of trigger and action.

- **Triggers** are events – currently defined in terms of existing management operations, such as installing a policy or publishing a session.
- **Actions** are automatic responses that take place after the trigger event , such as running a script or posting a web request.

Available Triggers

- **Before Publish** - Fired when an administrator publishes a session. The SmartTask passes the sessions meta-data (publishing administrator, domain information and session name) to the action. If the local Management API server is available, the session changes about to be published are formatted as a response to the "show changes" API.
- **After Publish** - Fired after an administrator successfully publishes a session. The SmartTask passes the same information to the action as the **Before Publish** trigger.
- **After Install Policy** - Fired after a policy has been installed. The SmartTask passes to the action information related to the policy installation task, such as the package installed, the administrator who initiated the installation and the task's result.

Available Actions

- **Run Script** - Runs a pre-defined Repository Script. The script gets the trigger's data as the first parameter. The trigger's data is passed as Base64 encoded JSON data, which can be decoded to implement custom business logic.

  For SmartTasks configured to run with "Before" operation triggers, the repository script can signal whether to abort or continue the operation by printing a JSON object with the "result" and optional "message" fields and then exit with code 0. If the value of the "result" field is "failure" the operation aborts.

  For SmartTasks configured to run with other triggers, exit code 0 is treated as success. Any other exit code is treated as failure.

  Notes:

  - By default, Repository Scripts run on the local Security Management Server although this can be customized using the Web API.
  - The ~ character is not supported in scripts for security reasons.

- **Web Request** - Executes an HTTPS POST web request to the configured URL. The trigger's data is passed as JSON data to the request's payload.

  Notes:

  - The configured URL must start with HTTPS and the target web server capable of handling such requests.
  - For web servers with self-signed SSL certificates, establish trust by specifying the certificate's fingerprint. You can get the fingerprint by clicking **Get Fingerprint** in the SmartTask editor or by viewing the certificate in a web browser.

  For SmartTasks configured to run with "Before" operation triggers, the repository script can signal whether to abort or continue the operation by responding with JSON object "result" and optional "message" fields and a status of 200 OK. If the value of the "result" field is "failure" the operation aborts.

For SmartTasks configured to run with other triggers, a 200 OK return code is treated as success. Any other exit code is treated as failure.

SmartTask - General

What can I do here?

Use this window to add SmartTask automation to SmartConsole.

SmartTasks are preconfigured actions linked to specific triggers. For example, running a script (action) before publishing (trigger).

Getting Here - Manage & Settings > Preferences > Tasks > SmartTasks > New or Edit > General

Configuring SmartTask Properties

1. Enter a unique name for the SmartTask - The name property is required and case sensitive.
2. Switch the SmartTask **ON** or **OFF** using the toggle button.
3. Optional - enter a description for the SmartTask.
4. Select a trigger for the SmartTask.
5. Select an action that will happen once the trigger is fired.
6. Custom Data – You can add additional information to the JSON data sent with the trigger information by adding a JSON object to the **Custom Data** field. The JSON custom data is concatenated to the trigger's payload and passed to the action.
7. Optional - add tags for the SmartTask object.

SmartTask - Advanced

What can I do here?

Use this window to configure advanced options for the selected action, such as script or web-hook error handling.

Getting Here - Manage & Settings > Preferences > Tasks > SmartTasks > New or Edit > Advanced

SmartTask Advanced Properties

The available advanced options depend on the action selected on the **General** tab.

Send Web Request

- **Time-out** – Number of seconds before the request times out and the request aborted.
- **If the HTTPS request times out** - Treat the time-out as an error and abort the event or continue normally.
- **X-chkp-shared-secret** – Enter a shared secret that can be used by the target web server to identify the Security Management Server. The value is sent as part of the request in the *X-chkp-shared-secret* header in the out-going web request.

Run script

- **Time-out** – Number of seconds before the request times out and the request aborted.
- **If the script fails to run or times-out** – Treat time-out (or execution failure) as an error and abort the event or continue normally.

Package Repository

Use this window to download packages from the cloud or upload packages from a local directory to the package repository. You can then deploy the packages in the package repository to gateways and clusters.

Getting Here - Manage & Settings > Package Repository

Introduction

Use Central Deployment in SmartConsole to perform batch deployment of:

- Jumbo Hotfix Accumulators and Hotfixes on Security Gateways and Cluster Members.
- Upgrade Packages on Security Gateways and Cluster Members.

You can Deploy a Hotfix or Upgrade Package from:

- The Check Point Cloud.
- The Package Repository on the Management Server.

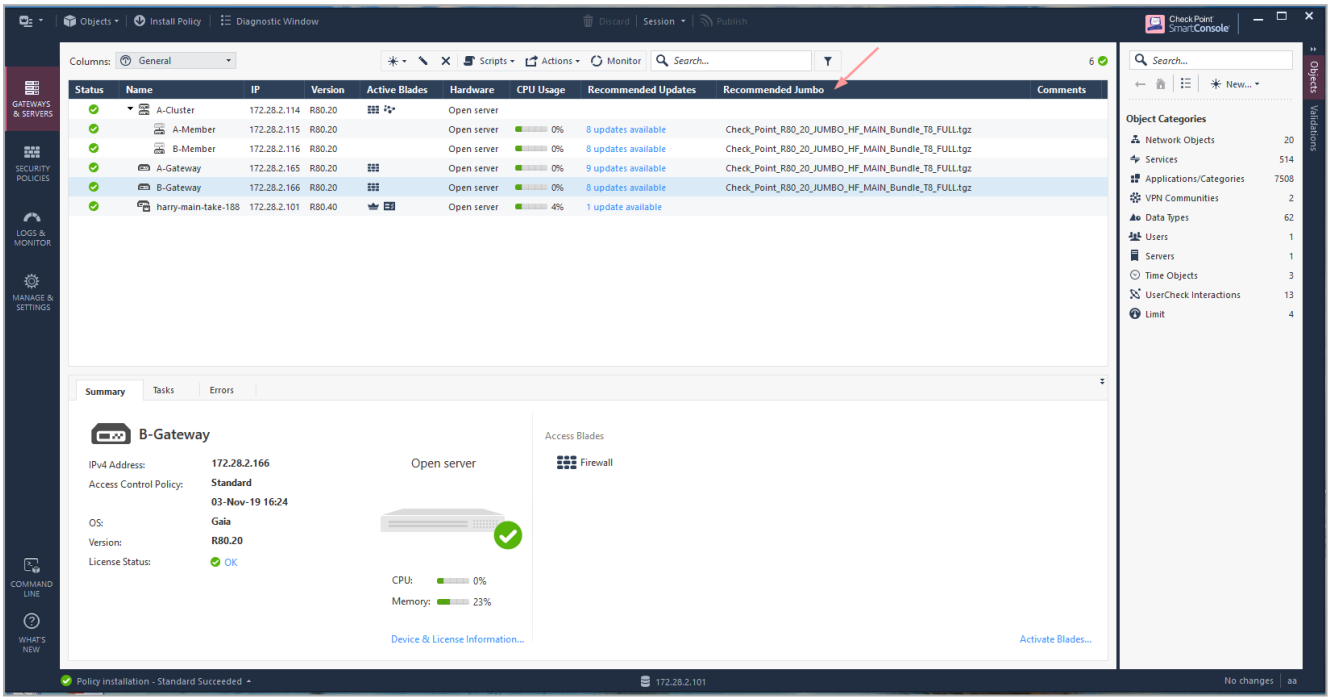
  First, you must upload the applicable package to the Package Repository.

To use Central Deployment through the API, see the *Check Point Management API Reference* (at the top, select the correct version) .

Best Practice - Use the Package Repository on the Management Server if the target's connectivity to the Management Server is better than the target's connectivity to the cloud, or if the target is overloaded with traffic.

Note - You can select up to 30 Security Gateways and Cluster Members, but installation can take place only on 10 targets at the same time. The Management Server places each target above the 10th in a queue. Each time an installation completes on one of the targets, the Management Server installs it on the next target in the queue.

Some Security Gateways have Recommended Hotfixes. See the **Recommended Jumbo** column in the **Gateways & Servers** view:



You can deploy a Recommended Jumbo Hotfix Accumulator or a specific Jumbo Hotfix Accumulator take.

Prerequisites

To use Central Deployment:

- The administrator must have SmartUpdate write permission on the Management Server.
- The latest build of the CPUSE Deployment Agent must be installed on the target Security Gateways and Cluster Members.
- SIC must already be established between the Management Server and the target Security Gateways and Cluster Members.
- A policy must be installed on the target Security Gateways and Cluster Members.
- Only full clusters can be deployed (you cannot select and deploy one cluster member).

To use Central Deployment directly from the Check Point Cloud:

1. The Management Server must be able to connect to the Check Point Cloud.
2. The target Security Gateways and Cluster Members must be able to connect to the Check Point Cloud.

To install the *Recommended* Jumbo Hotfix Accumulator on the target Security Gateways and Cluster Members, at least these Jumbo Hotfix Accumulator takes must be installed:

Target Version	Minimal Jumbo Hotfix Accumulator Take
R80.40 and higher	Any take.
R80.30	Take 76 or higher.
R80.20	Take 118 or higher.
R80.10	Take 245 or higher.

Limitations

- Upgrade from the R80.30, R80.20, and R80.10 versions (to upgrade from these versions to a higher version, use the CPUSE in-place upgrade).
- Central Deployment does not support:
  - Connecting from SmartConsole to the Management Server through a proxy server.

    In this case, use the applicable API command.
  - ClusterXL in High Availability mode configured as "`Switch to higher priority Cluster Member`" (known as "`Primary Up`").
  - ClusterXL in Load Sharing mode.
  - VRRP Cluster.
  - Standalone server.
  - Security Group in Maestro.
  - Security Group on Scalable Chassis 40000 / 60000.
  - Centrally Managed Quantum Spark Appliances running Gaia Embedded operating system.
  - Standby Security Management Server.
  - On Multi-Domain Servers, SmartConsole connected to the Global Domain, or the Multi-Domain Server context.

- Log Server.
- SmartEvent Server.

Installation

Adding a package to the Package Repository

1. From the left navigation panel, click **Manage & Settings**.
2. From the left tree, click **Package Repository**.
3. Click **New** and select one of these options:
   - **Download from cloud** - To download the package to the Package Repository from the Check Point Cloud, paste the package CPUSE Identifier and click **Download**.
   - **Upload from local** - To upload the package to the Package Repository from your device, browse to the applicable package and click **Open**.

   After the download or upload is complete, the package appears in the **Package Repository** window in SmartConsole > **Manage & Settings** view.

Note - Add packages to the repository one at a time.

Installing a Hotfix or Upgrade Package on multiple Security Gateways or Cluster Members

Best Practice - Central deployment of Hotfixes or upgrade packages on the Security Management Server relies on the status reports from the managed Gaia servers. Therefore, we recommend to wait for two minutes after the Gaia server is up and running before you install a Hotfix or upgrade package.

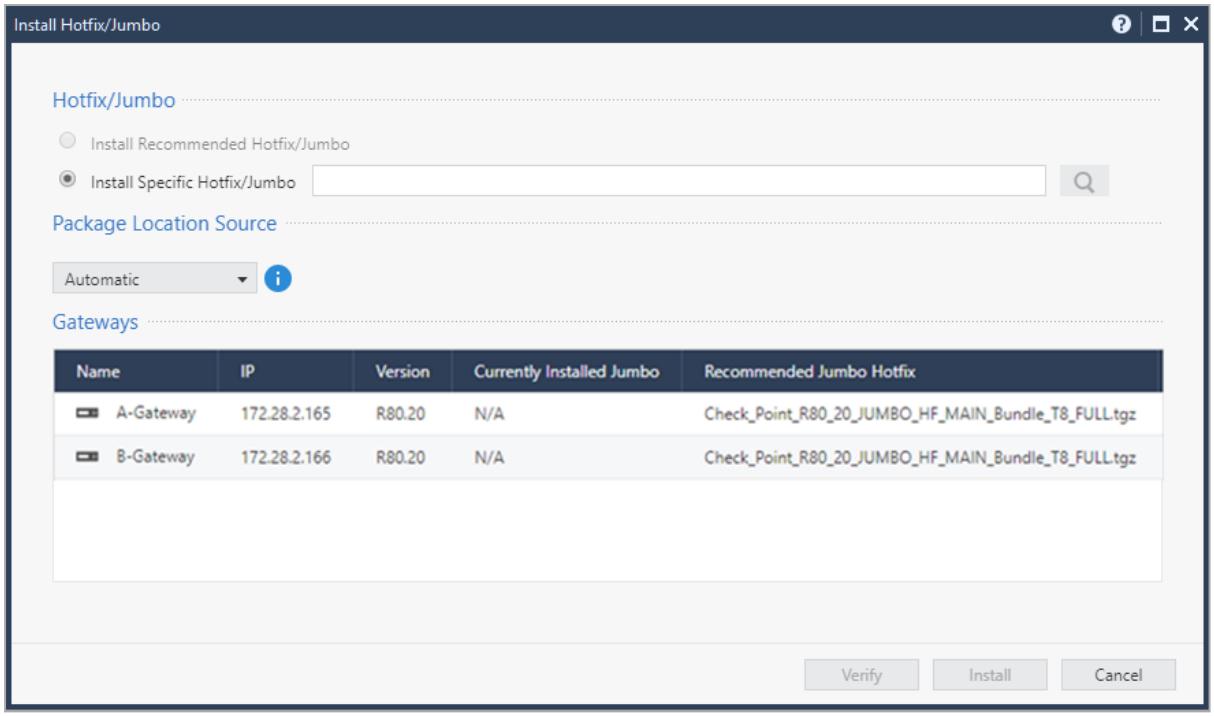
1. From the left navigation panel, click **Gateways & Servers**.
2. Select the target Security Gateways or Cluster Members for deployment.

   To select multiple targets, press and hold the **CTRL** key.

   To upgrade Cluster Members, select the cluster object.
3. From the toolbar menu, click **Actions** and select one of these options:
   - **Install Hotfix/Jumbo**
   - **Version Upgrade**

   The **Install Hotfix** or **Version Upgrade** window opens, and shows Information about the selected targets and their corresponding recommended Hotfix or Upgrade Package.

   Example:



4. **If you selected "Install Hotfix/Jumbo", in the "Hotfix/Jumbo" section, select one of these options:**

    - **Install the Recommended Hotfix/Jumbo**

      or

- **Install a Specific Hotfix/Jumbo**

  Note - If there is no recommended Jumbo Hotfix Accumulator for the selected targets, this option is grayed out. If a recommended Jumbo Hotfix Accumulator applies only to some of the selected targets, the deployment takes place only for those targets.

  a. Enter the Hotfix file name.

  You can copy the Hotfix file name from the applicable SK article to the **Install Specific Hotfix** text box.

  Note - Use the field "**Install a Specific Hotfix/Jumbo**" to install a firmware package on Quantum SparkAppliances that run Gaia Embedded OS **R80.20.xx and higher**. The Management Server considers firmware packages based on the same main version as Jumbo Hotfixes. For example, all firmware packages R81.10.XX are based on the main version R81.10.

  Example for a Security GatewayR80.20:

  - Ongoing Take

Product	Take	Date	CPUSE Online Identifier	SmartConsole package
Security Gateway / Standalone	Jumbo HF Take_127	03 Dec 2019	Check_Point_R80_20_JUMBO_HF_Bundle_T127_sk137592_Security_Gateway_and_Standalone_2_6_18_FULL.tgz	(EXE) Build 081
Security Management			Check_Point_R80_20_JUMBO_HF_Bundle_T127_sk137592_Security_Management_3_10_FULL.tgz	

  b. Click the search icon next to the text box to find the available package.

If you selected "Version Upgrade", in the "Upgrade Version" window, select one of these options:

- **Upgrade to the Recommended Major Version**

  or

- **Upgrade to a Specific Major Version**

  a. Enter the version number.

  b. Click the search icon next to the text box to find the available package.

5. Select the **Package Location Source**:

   - **Gateway** - The package is downloaded from the Check Point Cloud.
   - **Management** - The package is uploaded from the Package Repository.

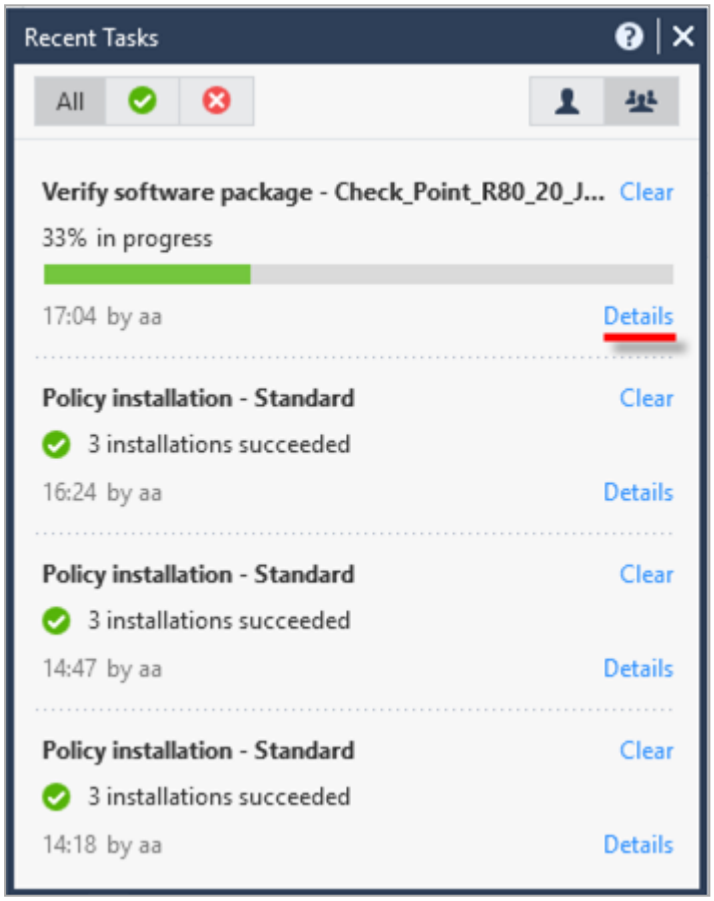
- **Automatic** - If the package is in the Package Repository, it is downloaded from the Package Repository. If the package is not in the Package Repository, the package is downloaded from the Check Point Cloud.

6. Click **Verify**.

   The **Install Hotfix** or **Upgrade Version** window is minimized, and the verification process starts. The verification process makes sure that the selected Hotfix Take or Upgrade Package can be installed on the targets. The verification process checks other installed Hotfixes are not overridden and that enough free disk space is available for the process to complete.

   To see the progress of the verification process open the **Tasks** view in the bottom left corner of SmartConsole and click **Details**.

   Example:



7. Repeat steps 1-6.
8. Click **Install**.
9. Central Deployment verifies that Access Control Policy is installed.
10. After the installation is complete, you must install the applicable Threat Prevention policy on the target Security Gateways and Clusters

Note - If different targets have different recommended Hotfixes or Upgrade Packages, each target gets its applicable recommended Hotfix or Upgrade Package.

Rule Base Cell Settings

Use this window to configure cell values for rule creation and other default behavior.

Getting Here - Manage & Settings > Policy Settings

Starting from R81.10:

- The default value for the **Source**, **Destination**, and **Services & Applications** columns in a new rule is "**None**".

  In versions R81 and lower, the default value for these columns in a new rule is "**Any**".

- The default value a cell gets after removing the last object from the cell is "**None**".

  The "last object" is the object that remained the last object in the cell after all other objects were removed.

  In versions R81 and lower, the default value for the last object deleted from a cell is "**Any**".

To configure the default values for the Source, Destination, and Services & Applications columns:

1. In the **Manage & Settings** view > **Policy Settings** > **Rule Base Cell Settings**.
2. In **Security Access Defaults**, select the values for the Source, Destination and Services & Applications columns.

To configure the value for the Source, Destination, and Services & Applications columns after removing the last object from a cell:

1. In the **Manage & Settings** view > **Policy Settings** > **Rule Base Cell Settings**.
2. In the **After removing the last object in a cell** section, select one of these options:
   - **Add 'None' to the cell** - After removing the last object from a cell, the value in the cell becomes "**None**".
   - **Add the object according to the Rule Base cell default** - After removing the last object in a cell, the value in the cell becomes as configured in the **Security Access Defaults** section.

Note - Right-click a cell to switch between "**Any**" and "**None**".

Enforcement of Rules with the Value "None"

On Security Gateways with versions from R80.10 to R81, the policy is installed without rules that contain the value "**None**" in one or more cells.

On Security Gateways with versions R77.30 and lower, the policy installation if there is a rule that contains the value "**None**" in one or more cells.

To configure the message which appears when a rule has "None":

Go to **Manage & Settings** > **Policy Settings** > **Rule Base Cell Settings** > **'None' object behavior**

Upgrading of a Management Server from R81 and Lower Versions

During an upgrade from R81 and lower versions:

- Default value for the **Source**, **Destination**, and **Services & Applications** columns remains "**Any**".
- Default value after the last object in a cell is removed becomes "**None**".

Network Object Explorer

What can I do here?

Use the Object Explorer to

- Create and edit network objects
- See unused objects by clicking **All** and selected **Unused Objects**.
- Export a list of objects to CSV format.
  - Organize the columns before selecting **Actions > Export**.
  - Export only exports the columns currently on view.

Getting Here - Menu > Open Object Explorer
Or:
SmartConsole > Objects > Object Explorer

Network

What can I do here?

Use this window to create or edit an object that represents a network.

Getting Here - Object Explorer > New > Network

Networks

A Network is a group of IP addresses defined by a network address and a net mask. The net mask indicates the size of the network.

A Broadcast IP address is an IP address which is destined for all hosts on the specified network. If this address is included, the Broadcast IP address will be considered as part of the network.

NAT

What can I do here?

Use this window to configure Network Address Translation.

Getting Here - Object Explorer > New > Network > NAT page
Or:
Object Explorer > New > Host > NAT page

Translating IP Addresses

NAT (Network Address Translation) is a feature of the Firewall Software Blade and replaces IPv4 and IPv6 addresses to add more security. You can enable NAT for all SmartConsole objects to help manage network traffic. NAT protects the identity of a network and does not show internal IP addresses to the Internet. You can also use NAT to supply more IPv4 addresses for the network.

The Firewall can change both the source and destination IP addresses in a packet. For example, when an internal computer sends a packet to an external computer, the Firewall translates the source IP address to a new one. The packet comes back from the external computer; the Firewall translates the new IP address back to the original IP address. The packet from the external computer goes to the correct internal computer.

SmartConsole gives you the flexibility to make necessary configurations for your network:

- Easily enable the Firewall to translate all traffic that goes to the internal network.
- SmartConsole can automatically create Static and Hide NAT rules that translate the applicable traffic.
- You can manually create NAT rules for different configurations and deployments.

How Security Gateways Translate Traffic

A Security Gateway can use these procedures to translate IP addresses in your network:

- **Static NAT** - Each internal IP address is translated to a different public IP address. The Firewall can allow external traffic to access internal resources.

  The configuration of static NAT on a *range* results in the translation of the IP addresses in the range into a *range of the same size, starting with the IP address specified.*

- **Hide NAT** - The Firewall uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the internal IP structure. Connections can only start from internal computers; external computers CANNOT access internal servers. The Firewall can translate up to 50,000 connections at the same time from external computers and servers.

- **Hide NAT with Port Translation** - Use one IP address and let external users access multiple application servers in a hidden network. The Firewall uses the requested service (or destination port) to send the traffic to the correct server. A typical configuration can use these ports: FTP server (port 21), SMTP server (port 25) and an HTTP server (port 80). It is necessary to create manual NAT rules to use Port Translation (see *"NAT Rule Base" on page 114*).

Using Hide NAT

For each SmartConsole object, you can configure the IP address that is used to translate addresses for Hide NAT mode:

- Use the IP address of the external Security Gateway interface
- Enter an IP address for the object

Hide NAT uses dynamically assigned port numbers to identify the original IP addresses. There are two pools of port numbers: 600 to 1023, and 10,000 to 60,000. Port numbers are usually assigned from the second pool. The first pool is used for these services:

- `rlogin` (destination port 512)
- `rshell` (destination port 513)
- `rexec` (destination port 514)

If the connection uses one of these services, and the source port number is below 1024, then a port number is assigned from the first pool.

You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

Host - General

What can I do here?

Use this window to edit or create a host object.

Getting Here - Object Explorer > New > Host

Check Point Hosts

A Check Point Host can have multiple interfaces but no routing takes place. It is an endpoint that receives traffic for itself through its interfaces. (In comparison, a Security Gateway routes traffic between its multiple interfaces.) For example, if you have two unconnected networks that share a common Security Management Server and Log Server, configure the common server as a Check Point Host object.

A Check Point Host has one or more Software Blades installed. But if the Firewall blade is installed on the Check Point Host, it cannot function as a firewall. The Host requires SIC and other features provided by the actual firewall.

A Check Point Host has no routing mechanism, is not capable of IP forwarding, and cannot be used to implement Anti-spoofing. If the host must do any of these, convert it to be a Security Gateway.

The Security Management Server object is a Check Point Host.

Note - When you upgrade to R81.10 from R77.30 or earlier versions, Node objects are converted to Host objects.

Host - Network Management

What can I do here?

Use this window to set the IP address of the host.

Getting Here - Object Explorer > New > Host > Network Management

Host - Interface

What can I do here?

Use this window to create or edit a host interface.

Note - You can define both IPv4 and IPv6 address for the host, or you can define only an IPv6 or an IPv4 address.

Getting Here - Object Explorer > New > Host > Network Management > Interface - add new, or edit existing

Host - Interface Options

- **Name** - Enter the interface name, which must match the physical interface as defined in the operating system.
- **IPv4 / IPv6** - Enter the address in the correct format.

Host - Advanced

What can I do here?

Use this window to configure SNMP settings. The settings identify the host to SNMP management applications by retrieving (Get) or sending (Set) SNMP information.

Getting Here - Object Explorer > New > Host > Advanced

SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to send and receive information between network devices. As part of the TCP/IP protocol suite, SNMP enables network administrators to manage network operations.

The SNMP mib allows Check Point devices to talk to and report on status to network management software such as HP OpenView. The Security Gateway SNMP daemon also provides Check Point specific variables.

When setting up a machine, you can assign those values. An SNMP management tool verifies the identity of a machine by querying those values. For example, when defining this network object, you can verify that the IP address is correct by pressing **Get** . This retrieves the IP address from the SNMP agent, and you can verify that it is the expected value.

In this window:

- **Name** is the object's name.
  - **Get**retrieves and displays information about this network object.
- **Location** is the object's location.
  - **Set** sets the object's properties to those shown in this window.
- **Contact** is the name of a contact person.
- **Description** describes the Check Point device.

  This value is set in the SNMP management application (HP OpenView).
- **Read Community** is the community with read permission for this object.
- **Write Community** is the community with write permission for this object.

Host - Servers

What can I do here?

Use this window to create a server of type:

- Web Server
- Mail Server
- DNS Server

Getting Here - Object Explorer > New > Host > Servers

Wildcard Object

What can I do here?

Use this window to create a wildcard object that represents a series of IP addresses that are not sequential.

Getting Here - Object Explorer > New > Network Object > Wildcard Object

Using Wildcard Objects

Wildcard objects let you define IP address objects that share a common pattern that can be permitted or denied access in a security policy.

Note - This feature is only supported for R80.20 and above gateways.

To create a new wildcard object:

1. Open **Object Explorer** > **New** > **More** > **Network Object** > **Wildcard object**.
2. Enter the Wildcard IP address and Wildcard Netmask in IPv4 or IPv6 Format.
3. Click **OK**.

Understanding Wildcard Objects

The wildcard object contains a wildcard IP address and a wildcard netmask.

The *wildcard netmask* is the mask of bits that indicate which parts of the IP address must match and which do not have to match. For example:

Wildcard IP:	194.	29.	0.	1
Wildcard Netmask:	0.	0.	3.	0

The third octet represents the mask of bits. If we convert the 3 to binary, we get 00000011. The 0 parts of the mask must match the equivalent bits of the IP address. The 1 parts of the mask do not have to match, and can be any value.

0 0 0 0 0 0	1 1
Must match the equivalent bits in the IP Address	Do not have to match

The binary netmask produces these possible decimal values:

128	64	32	16	8	4	2	1
						Binary	**Decimal**

0	0	0	0	0	0	0	0	**0**
0	0	0	0	0	0	0	1	**1**
0	0	0	0	0	0	1	0	**2**
0	0	0	0	0	0	1	1	**3**

The netmask permits only these IP addresses:

- 194.29.0.1
- 194.29.1.1
- 192.29.2.1
- 194.29.3.1

Use Cases

Scenario One

A supermarket chain has all of its cash registers on subnet 194.29.x.1, where x defines the region. In this use case, all the cash registers in this region must have access to the database server at 194.30.1.1.

Instead of defining 256 hosts (194.29.0.1, 194.29.1.1, 194.29.2.1....194.29.255.1), the administrator creates a wildcard object that represents all the cash registers in the region:

Wildcard IP:	194.	29.	0.	1
Wildcard Mask:	0.	0.	255.	0

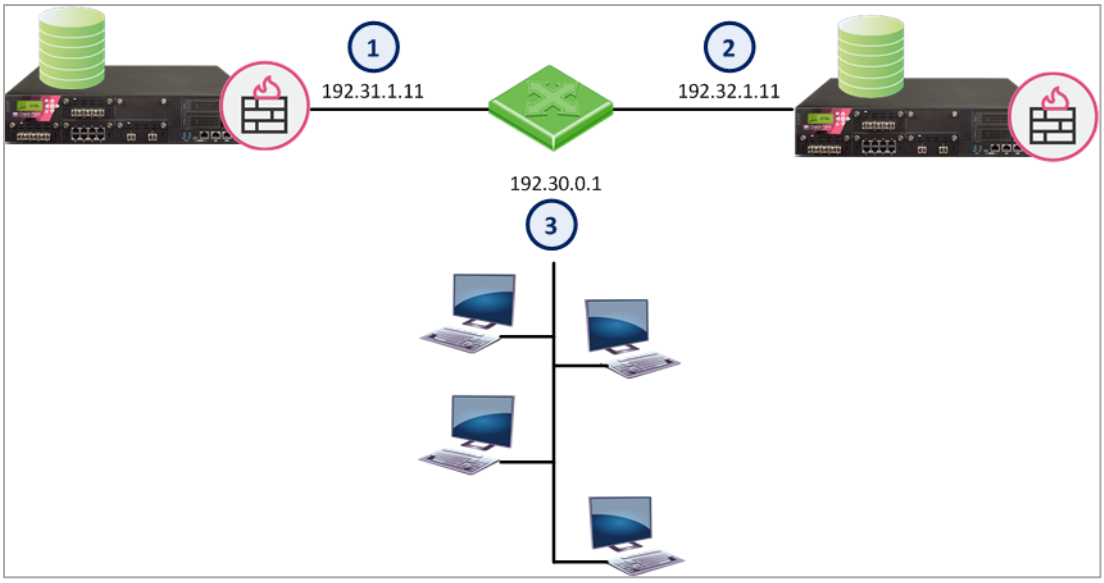
The wildcard object can now be added to the access control policy.

Source	Destination	Action	Track
Wildcard Object	Database server object	Accept	Log

Scenario Two

In this use case, a supermarket chain has stores in Europe and Asia.

The 192.30.0-255.1 network contains both the Asian and European regions, and the stores within those regions.



Item	Description
1	Database Server for Europe
2	Database Server for Asia
3	European and Asia network

The administrator wants stores in the European and Asia regions to access different database servers. In this topology, the third octet of the European and Asia network's IP address will be subject to a wildcard. The first four bits of the wildcard will represent the region and the last four bits will represent the store number.

Bits that represent the region	Bits that represent the store number
0000	0000

In the Wildcard IP:

- The Asia region is represented by **0001xxxx** (Region **1** in decimal)
- The European region is represented by **0010xxxx** (Region **2**in decimal)

In binary:

Binary		Decimal
Region	Store	
0001	0000	16 - Asia Region
0010	0000	32 - European Region

To include all the stores of a particular region, the last four bits of the wildcard mask must be set to 1 (15 in Decimal):

Binary		Decimal
Region	Store	
xxxx	1111	15 - all Asian stores
xxxx	1111	15 - all European stores

A wildcard object that represents all the Asian stores will look like this:

Wildcard IP address	192.30.16.1	(The region)
Wildcard netmask	0.0.15.0	(for stores in the region)

For this range of IP addresses: 192.30. **16-31** .1

A wildcard object that represents all the European stores will look like this:

Wildcard IP address	192.30.32.1	(the region)
Wildcard netmask	0.0.15.0	(for stores in the region)

For this range of IP addresses: 192.30. **32-47** .1

The administrator can now use these wildcard objects in the access control policy:

Source	Destination	Action	Track
Asian Stores Wildcard	Database Server for Asia	Accept	Log
European Stores Wildcard	Database Server for Europe	Accept	Log

Scenario Three

In this scenario, the netmask bits are not consecutive.

Wildcard IP	1	1	0	1
Wildcard mask	0	0	5	0

Wildcard IP	00000001.00000001.00000000.00000001
Wildcard Mask	00000000.00000000.00000101.00000000

Mask:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0

Which will match only these IP addresses:

IP Address	Binary	Comment
1.1.0.1	00000001.00000001.00000000.00000001	The IP address itself
1.1.1.1	00000001.00000001.00000001.00000001	The equivalent bit at position 23 does not matter
1.1.4.1	00000001.00000001.00000100.00000001	The equivalent bit at position 21 does not matter
1.1.5.1	00000001.00000001.00000101.00000001	The equivalent bits at positions 21 and 23 do not matter

IPv6

The same principles apply to IPv6 addresses. For example, if the wildcard object has these values:

IPv6 Address	2001::1:10:0:1:41
Wildcard netmask	0::ff:0:0

The wildcard will match: 2001::1:10:0-255:1:41

Web Server - Configuration

What can I do here?

Use this window to configure settings for the web server, such as operating system, application engines, port configuration, and the enforcement points that protect it.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server

Understanding Web Servers

Defining Web server properties per host makes it possible to define granular protection per Web server, in addition to the global protection settings configured via Web Security.

Defining protection settings per Web server is also an easier and more intuitive way of defining application security, than using a resource and placing the resource in a rule in the Security Rule Base.

Note that you should still define Access control in the Rule Base, in order to restrict the allowed source and destination of HTTP connections.

Web Server Options

- **Operating System**

  Specifies the operating system that the Web server host is running. The Web Security **Malicious Code Protector** is only effective for Web servers running on the following OSs:

  Windows

  x86 Linux

  SPARC Linux.

  SPARC Solaris

  Other

- **Application Engines** - Defines the Web application engines running on this Web server. If any of the engines defined in the **Error Concealment** protection are not running on this Web server, then Web Security will not look for patterns relevant to that engine on this Web server. Proper configuration of this field optimizes Web Security performance.
- **Ports Configurations** - Defines whether or not this Web server uses the standard port 80. If it uses other ports, specify them here. Note that you must allow all HTTP ports in the Security Rule Base.

  Note - Adding https port (tcp 443) will not affect Web Security protections since https connections are encrypted and Web Security protections cannot be enforced on encrypted protections.
- **Protection** - Specifies the enforcement points that protect this Web server. Licensing is enforced by counting the number of Web servers that are protected by each gateway. If **All* is specified, the number of counted Web servers is incremented for *all* gateways that enforce Web Security features.

Web Server Protections

What can I do here?

Use this window to configure web server protections.

Enforcement of these protections is dependent upon the IPS profile that protects the server.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections

Web Security

Select a protection to apply it to the Web server. For those protections which can be configured, click **Advanced** to configure the protection's behavior.

The more information about the protections that can be applied specifically to a web server object, see:

- General HTTP Worm Catcher
- Malicious Code Protector
- Cross Site Scripting
- LDAP Injection
- SQL Injection
- Command Injection
- Directory Traversal
- Header Spoofing
- Error Concealment
- Directory Listing
- HTTP Format Sizes
- ASCII Only Request
- Header Rejection
- HTTP Methods

Monitor-Only Per Web Server

All protections on a particular web server can be set to Detect-only. This makes it possible to put a new web server in place and investigate which protections it needs, while ensuring that connectivity is maintained.

To configure Detect-only per web server, use the Check Point Database Tool (see sk13009). Using Database Tool (GuiDBEdit Tool), search for the web server name, and then look for the field **web_server_monitor_only** and set it to **true** .

Malicious Code Protector

What can I do here?

Use this window to select the web server's protection level against malicious code.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections > Select Malicious Code Protector > Advanced

Malicious Code Protector - Options

Low (default level)

- URLs are analyzed only if they contain at least one non-ASCII character.
- HTTP headers are analyzed only if they contain at least one non-ASCII character. Headers that contain only plain ASCII are not analyzed.
- POST bodies are analyzed only if an HTTP header value contains at least one non-ASCII character. This ensures that innocent file uploads are not scanned.

Medium

- URLs are fully analyzed.
- HTTP headers are analyzed only if they contain at least one not allowed/suspicious ASCII character.
- POST bodies are analyzed if there is at least one non-ASCII character in an HTTP header, or if the POST body itself contains at least one non-ASCII character.

High

- URLs are fully analyzed.
- HTTP headers are fully analyzed.
- POST bodies are analyzed either if there is at least one non-ASCII character in an HTTP header, or if the POST body itself contains at least one non-ASCII character.

Cross Site Scripting

What can I do here?

Use this window to select the web servers protection level against cross site scripting.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections > Select Cross Site Scripting > Advanced

Cross Site Scripting Options

- **High** - Rejects requests containing HTML tags,the strictest and safest approach.
- **Medium** - A cautious approach that rejects requests that contain HTML tags in the URL and body from fields.
- **Low** - The least strict approach that rejects requests that contain HTML tags and script commands in the path and from fields.

LDAP Injection

What can I do here?

Use this window to configure the web server's level of protection against LDAP injection.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections > Select LDAP Injection > Advanced

Components of LDAP Injection Protection

The LDAP Injection protection examines LDAP queries and enforces the following:

- **Filter Injection** protection rejects one of the & (AND), | (OR) and ! (NOT) logical operators in combination with unbalanced (or balanced but reversed) parentheses.
- **DN Injection** protection rejects Relative Distinguished Name (RDN) fields. RDN fields are not normally used explicitly in the LDAP queries. The list of RDN fields that this protection looks for can be customized. This makes it possible to control the use of customized LDAP fields, as well as standard ones.

This protection can identify "Percent Encoded" or "UTF-8 Encoded" expressions as well as text-based LDAP expressions. For details about LDAP, refer to RFC 1779.

What Part of the HTTP Request Is Searched?

LDAP queries are sent in HTTP Requests to the Web server.

The LDAP queries usually appear in the form fields of the HTTP Request (i.e., in the URL or HTTP Request body), but could also appear in other parts of the HTTP Request.

This protection searches for LDAP Injection either in the form fields of the HTTP Request, or in the whole Request - depending on the Security Level.

LDAP Injection Options

- **High** protects against *Filter Injection* and *DN Injection*. The protections searches the whole HTTP Request.
- **Medium** protects against *Filter Injection* and *DN Injection*. The protections searches in the form fields of the HTTP Request only (that is, in the URL and HTTP Request body).
- **Low** protects against *Filter Injection*. The protections searches in the form fields of the HTTP Request only (that is, in the URL and HTTP Request body).

SQL Injection

What can I do here?

Use this window to configure the web server's level of protection against SQL injection.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections > Select SQL Injection > Advanced

Understanding SQL Injection

Attack Description

SQL injection attacks allow a remote attacker to execute SQL commands disguised as a URL or form input to a database. A successful attack may get the database to run undesirable commands. This could cause damage by revealing confidential information, modify the database, or even shut it down.

Web Security Protection

Web Security can inspect for the presence of SQL commands in Web forms or URLs sent in HTTP Requests to a server. The protection looks for several categories of commands: distinct SQL commands, non-distinct SQL commands, and special SQL separator characters (e.g., + ' -). Strings that are unique to SQL and not likely to appear in common language are considered distinct (e.g., "sql_longvarchar", "sysfilegroups", etc.). Strings that may appear in common language are considered non-distinct (e.g., "select", "join", etc.).

SQL Injection Options

Depending on the protection level, the search is made either between separators of the path and query sections of the URL, or across the entire path and query. In the path section of the URL, the separator is the / character. In the query section, the separator is the & character.

- **High** - Rejects forms and URLs that contain special SQL, distinct SQL commands, or non-distinct SQL commands in the entire URL or form input.
- **Medium** - Rejects forms and URLs that contain special SQL characters, distinct SQL commands, or non-distinct SQL commands between separator characters in the URL and form input.
- **Low** - Rejects forms and URLs that contain special SQL characters or distinct SQL commands between separator characters in the URL and form input.

Command Injection

What can I do here?

Use this window to configure the web server's level of protection against Command injection.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections > Select Command Injection > Advanced

Understanding Command Injection

Attack Description

Command injection attacks allow a remote attacker to execute operating system commands disguised as a URL or form input to a Web server. A successful system command execution can provide a remote attacker with administrative access to a Web server. This could result in damage such as defacement of the Web site, data theft, or data loss.

Web Security Protection

Web Security looks for the presence of system commands in Web forms and URLs sent to a protected server. The protection looks for several categories of commands: distinct system commands, non-distinct system commands, and special system characters (e.g.,;[ ]<>&\t). Strings that are unique to system commands, not likely to appear in common language, and often used in command injection are considered distinct (e.g., "chown", "regsvr32", etc.), while strings that may appear in common language are considered non-distinct (e.g., "format", "convert", etc.).

Command Injection Options

Note - The security level can be set in this window only when the **Protection Scope** is set to **Apply to all HTTP traffic** .

- **High** - Rejects forms that contain special Shell characters, distinct Shell commands, or non-distinct Shell commands in the HTTP Request body and in the path and query sections of the URL, even within variable names. For example, the following will be blocked because of the presence of the string "arp", which is a command: http://www.server.com/search?execarp2=x+y+z.
- **Medium** - Rejects forms that contain special Shell characters, distinct Shell commands, and non-distinct Shell commands in the HTTP Request body and in the path and query sections of the URL.
- **Low** - Rejects forms that contain special Shell characters and distinct Shell commands in the HTTP Request body and in the path and query sections of the URL.

Error Concealment

What can I do here?

Use this window to configure the web server's level of error concealment.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections > Error Concealment > Advanced

Detection of Status Codes and Application Engines

Detection of HTTP Response Status Codes

Web servers place a status code in the header of the HTTP Response. Some codes indicate a valid response, such as `200 OK`. The 4XX and 5XX codes on the other hand indicate an error status. Some of the 4XX and 5XX codes could reveal unnecessary information.

If these error codes are detected in the HTTP Response, this protection conceals the response. You can **configure** which of these HTTP Response codes will be concealed.

Configure Detection of Application engines

Web application engines generate error messages. If the application engine is properly configured, these error messages are masked by the Web server, which will generate an HTTP Response with an error status code. However, if the Web server is incorrectly configured, it may display detailed error information that a remote attacker could use to tailor an attack. These error messages are characteristic to each application engine.

Error Concealment Options

- **Low** - conceals responses which contain specific response status codes (those configured in the **Concealed HTTP response status codes**window of the Web Security **Error Concealment** protection).
- **High** - conceals responses which contain specific Response status codes

Directory Listing

What can I do here?

Use this window to configure the web server's level protection against directory listing.

> **Getting Here** - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections > Directory Listing > Advanced

Directory Listing Options

- **Low** - examines only suspicious responses. A suspicious response is a response to a request that contains a URL that ends with a "/" or "\", for example http://www.example.com/shop-online/ and http://www.example.com/shop-online/?john-doe. Responses found to meet all of the following conditions will be dropped:
  1. The name of the requested directory is found in the title of the HTML page. For example, <TITLE>Index of /shop-online</TITLE>.
  2. There is a link to the parent directory in the HTML page. For example, <A HREF="/">.
  3. The word "Parent Directory" appears in the HTML page within a link that points to the parent directory. For example, <A HREF="/">Parent Directory</A>.
- **Medium** - examines all HTTP responses. Responses found to meet all of the following conditions will be dropped:
  1. The name of the requested directory is found in the title of the HTML page. For example, <TITLE>Index of /shop-online</TITLE>.
  2. There is a link to the parent directory in the HTML page. For example, <A HREF="/">.
  3. The word "Parent Directory" appears in the HTML page within a link that points to the parent directory. For example, <A HREF="/">Parent Directory</A>.
- **High** - examines all HTTP responses. Responses found to meet the following condition will be dropped:

The word "Parent Directory" appears in the HTML page within a link that points to the parent directory. For example, <A HREF="/">Parent Directory</A>.

HTTP Methods

What can I do here?

Use this window to configure HTTP methods the web server will block.

Getting Here - Object Explorer > New > Host > Servers > Select Web Server > Web Server > Protections > Advanced

Understanding HTTP Methods

Web Security divides the HTTP methods into three groups: Standard safe (GET, HEAD and POST), standard unsafe (the other standard HTTP methods), and WebDAV. By default, all methods are blocked other than the standard safe methods.

HTTP Method Block Options

- **Block Default HTTP Methods** - Block standard Safe, Unsafe and WebDav methods for this Web server.
- **Block selected HTTP methods (configure globally from Web Security)** - Select this option to block specified methods.

Mail Server - Configuration

What can I do here?

Use this window to select POP3/IMAP/SMTP servers and configure their ports and logging.

Note -

- **Log POP3/IMAP username** logs POP3/IMAP usernames and passwords used to access Mail servers
- Additional Protections are configured globally from IPS

Getting Here - Object Explorer > New > Host > Servers > Select Mail Server > Mail Server > Configuration

Mail Server - Protections

What can I do here?

Use this window to enable IPS protections that set limitations on email messages delivered to the network using POP3/IMAP protocols.

Selecting **POP3/IMAP Security** enables IPS protection for the Mail server.

Getting Here - Object Explorer > New > Host > Servers > Mail Server > Protections

DNS Server - Configuration

What can I do here?

Use this window to create a list of domain, host and/or network objects for the purpose of controlling DNS functionality.

Getting Here - Object Explorer > New > Host > Servers > Select DNS Server > DNS Server > Configuration

Authorization Domain List

Select a preconfigured domain object that contains the name of the domain for which you would like to enable external queries (for example, queries arriving through the external interface).

To enable back resolving (from an IP address to a host name) for this specific DNS server, create/select a host object with the IP address for which you would like to enable back resolving and add it to the **Authorization domains list** .

To enable back resolving for a specific network, create/select a network object and add it to the **Authorization domains list** .

Protected by shows the firewall that protects the DNS Server.

DNS Server Protections

What can I do here?

Use this window to protect the DNS Server from cache poisoning.

Getting Here - Object Explorer > New > Host > Servers > Mail Server > Protections

Cache Poisoning

Cache Poisoning occurs when DNS caches receive mapping information that was deliberately altered from a remote name server. The DNS server caches the incorrect information and sends it out as the requested information. As a result, email messages and URL addresses can be redirected and the information sent by a user can be captured and corrupted.

Cache Poisoning Options

- **Scramble source port and session id** - Scrambles the source port and query ID number of each DNS request for specific name servers
- **Drop inbound requests for external domains** - Prevents unauthorized inbound queries whose content is not a part of the name servers predefined zone.

Note - Enforcement of these settings depends on the profile that protects the server.

Network Group - New

What can I do here?

Use this window to create a new network group.

Getting Here - Object Explorer > New > Network Group
Or:
Object Explorer > New > Network Object > Group > Network Group

Network Groups

A network group is a collection of hosts, gateways, networks or other groups. Groups can be used to facilitate and simplify network management. When you have the same set of objects which you want to use in different places in the Rule Base, you can create a group to include such set of objects and reuse it. Modifications are applied to the group instead of to each member of the group.

Groups are also used where SmartConsole lets you select only one object, but you need to work with more than one. For example, in the gateway editor > **Network Management** > **VPN Domain** > **Manually defined**, you can only select on object from the drop-down menu. If you want to select more than one object for your VPN Domain, you can create a group, add the required objects to the group, and select the group from the drop-down menu.

Grouping Network Objects

To create a group of network objects:

1. In the **Objects** tree, click **New** > **Network Group**.

   The **New Network Group** window opens.
2. Enter a name for the group
3. Set optional parameters:
   - Object comment
   - Color
   - Tag (as custom search criteria)
4. For each network object you want to add, click the **[+]** sign and select it from the list that shows.
5. Click **OK**.

From R80.20.M2, you can also associate groups to a network object directly from the object editor.

To associate groups to a network object:

1. Open the object editor, and go to **Groups** in the navigation tree.
2. For each group you want to add, click the **[+]** sign and select it from the list that shows.

Group with Exclusions

What can I do here?

Use this window to create or edit a group with exclusions.

Select a group, then select objects to exclude from the group.

Getting Here - Object Explorer > New > Network Object > Group > Group with Exclusion

GSN Handover Group

What can I do here?

Use this window to edit or create a GSN Handover Group.

Getting Here - Object Explorer > New > Network Object > Group > GSN Handover Group

Understanding Handover Groups

Handover Groups let you specify sets of IP addresses that can pass control of GSN traffic. Handover Groups typically consist of the IP addresses of a GPRS/UMTS operator's GSNs.

Creating a GSN Handover Group

GSN Handover Groups prevent Session Hijacking and enable secure handover, redirection, and multiple GGSN interface support on Carrier Security. You should create Handover Groups for your own GSNs, and for your roaming partners' GSNs. Typically there will be one GGSN/PGW Handover Group and one SGSN/SGW Handover Group for each operator.

After you define your Handover Groups, include them as source and destination addresses in the rule base in order to allow handover, redirection, and multiple GGSN/PGW interface support for the GSNs that you included in the Handover Groups.

To define a GSN Handover Group:

1. In the **Network Objects** tree, right click on **Groups**, and select **New Groups > GSN Handover Group**.
2. Give the group a name, such as `SG_Home_HG`, where `SG` stands for SGSN/SGW.
3. Add the appropriate GSN objects you created in **Creating GSN Objects**.
4. To rate limit signaling packet from the GSN handover group select **Enforce GTP signal packet rate limit from this group** and enter an integer value (in PDU/sec).

To simplify the Security Policy rule base, it is recommended that you:

- Define a group consisting of your entire home PLMN GSNs.
- For each of your partner networks, define two groups:
- one consisting of all of its SGSNs/SGWs or IP address ranges as appropriate
- one consisting of all of its GGSNs/PGWs or IP address ranges as appropriate

User Authority Server Group

Use this window to edit or create a User Authority Server Group.

Getting Here - Object Explorer > New > Network Object > Group > User Authority Server Group

User Authority Server Groups

In this window you can define a group of UserAuthority servers for use in the rule base, or when working with remote access access communities.

UserAuthority can be used to obtain the user's identity:

- From a SecureAgent
- From SecureClient - If the user authenticated via SecureClient connected to the Check Point Security Gateway.
- From the Security Gateway - If the user authenticated via an HTTP connection to port 900 or Telnet to port 256 on the gateway.

Address Range

What can I do here?

Use this window to create or edit an address range.

Getting Here - Object Explorer > New > Network Object > Address Range > Address Range

Address Ranges

An address range is a range of IP addresses on the network, defined by the lowest and the highest IP addresses. Use an Address Range object when you cannot define a range of IP addresses by a network IP and a net mask. The Address Range objects are also necessary for the implementation of NAT and VPN.

Multicast Address Range

What can I do here?

Use this window to create or edit a multicast address range.

Getting Here - Object Explorer > New > Network Object > Address Range > Multicast Address Range

Entering Address Ranges

IPv4 Multicast Group Addressing

The IPv4 address space is divided into four sections: Class A, Class B, Class C, and Class D. Class A, B, and C addresses are used for unicast traffic. Class D addresses are reserved for multicast traffic and are allocated dynamically.

The IPv4 multicast address range (224.0.0.0 - 239.255.255.255) is only for the group address or destination address of IPv4 multicast traffic. Select an address or range of addresses within this scope. (For more information regarding host extensions for IP multi-casting, see: RFC 1112.)

Every IPv4 datagram whose destination address starts with "1110" is an IPv4 multicast datagram.

IPv6 Multicast Group Addressing

The IPv6 multicast address range is ff00::/8. These are the fields for an IPv6 multicast address:

- FP (Format Prefix) - All multicast IPv6 addresses begin with **ff** (8 bits)
- Flags - Transient flag indicates if the address is permanently assigned by the IANA (Internet Assigned Numbers Authority), or is temporary (4 bits)
- Scope - Indicates the scope of the multicast traffic, for example routing protocols and if the traffic can be forwarded to external networks (4 bits)

Multicast Address Range

Just as a radio is tuned to receive a program that is transmitted at a certain frequency, a host interface can be "tuned" to receive datagrams sent to a specific multicast group. This process is called joining a multicast group.

The remaining bits identify the multicast "group" to which the datagram is sent. Membership in a multicast group is dynamic. Hosts can join and leave multicast groups.

The source address for multicast datagrams is always the unicast source address.

Reserved Local Addresses

Multicast group IPv4 addresses are assigned by the IANA for applications that are never forwarded by a router. The connections remain local on a particular LAN segment. These are the IP address ranges that are reserved for local networks:

- IPv4 - 224.0.0.0/24
- IPv6 - ff02::/16

These IP addresses are called permanent host groups. Some examples of reserved local network multicast groups are shown in the table below.

IPv4 Multicast Address	IPv6 Multicast Address	Purpose
224.0.0.1	ff02::1	All hosts. An ICMP Request (ping) sent to this group should be answered by all multicast capable hosts on the network. Every multicast capable host must join this group at start-up on all its multicast capable interfaces.
224.0.0.2	ff02::2	Routers. All multicast routers must join this group on all its multicast capable interfaces.
224.0.0.4	ff02::4	The group of all DVMRP routers
224.0.0.5	ff02::5	All OSPF routers
224.0.0.13	ff02::d	All PIM routers

Tell me about the fields...

- **IP Address** or **First IP address** or **Last IP address** can in the multicast range:
  - IPv4 - 224.0.0.0 to 239.255.255.255
  - IPv6 - ff00::/8

Dynamic Object

What can I do here?

Use this window to create or edit a dynamic object.

Getting Here - Object Explorer > New > Network Object > Dynamic object

Dynamic Objects

A dynamic object is a "logical" object where the IP address is resolved differently for each Security Gateway, using the `dynamic_objects` command.

For R80.10 Security Gateways and higher, dynamic objects support SecureXL Accept templates. Therefore, there is no performance impact on a rule that uses a dynamic object, or on rules that come after it.

Dynamic Objects are predefined for **LocalMachine-all-interfaces** . The DAIP computer interfaces (static and dynamic) are resolved into this object.

Dynamic Global Network Object

What can I do here?

Use this window to create or edit a Dynamic Global Network Object.

Note -

- The name of the Dynamic Global Object must have a *global* suffix
- For the Global assignment to succeed, make sure the local domain has a dynamic object with the same name

Getting Here - Object Explorer > New > Network Object > Dynamic object > Dynamic Global Network Object

Security Zone

What can I do here?

Use this window to edit or create a security zone.

Getting Here - Object Explorer > New > Network Object > Security Zone

Security Zones

Security Zones let you to create a strong Access Control Policy that controls the traffic between parts of the network.

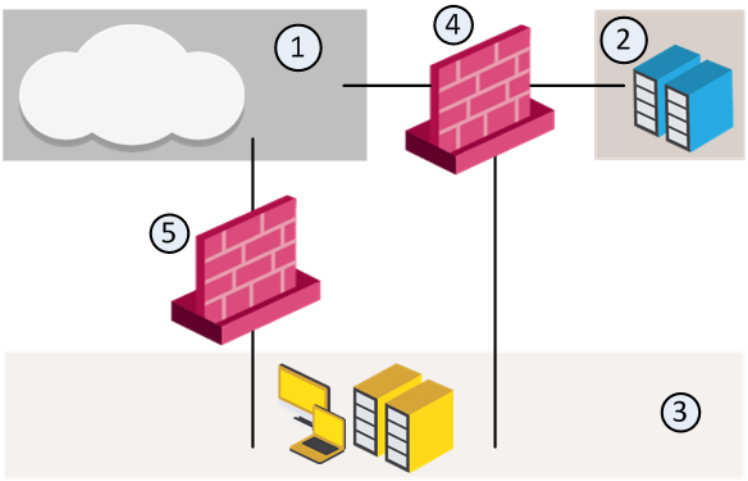
A Security Zone object represents a part of the network (for example, the internal network or the external network). You assign a network interface of a Security Gateway to a Security Zone. You can then use the Security Zone objects in the Source and Destination columns of the Rule Base.

Use Security Zones to:

- Simplify the Policy. Apply the same rule to many Gateways.
- Add networks to Gateways interfaces without changing the Rule Base.

For example, in the diagram, we have three Security Zones for a typical network: *ExternalZone* (1), *DMZZone* (2) and *InternalZone* (3).

- Gateway (4) has three interfaces. One interface is assigned to *ExternalZone* (1), one interface is assigned to *DMZZone* (2), and one interface is assigned to *InternalZone* (3).
- Gateway (5) has two interfaces. One interface is assigned to *ExternalZone* (1) and one interface is assigned to *InternalZone* (3).



A Security Gateway interface can belong to only one Security Zone. Interfaces to different networks can be in the same Security Zone.

Workflow

1. Define Security Zone objects. Or, use the predefined Security Zones.
2. Assign Gateway interfaces to Security Zones.
3. Use the Security Zone objects in the Source and Destination of a rule. For example:

Source	Destination	VPN	Service	Action
InternalZone	ExternalZone	Any Traffic	Any	Accept

4. Install the Access Control Policy.

Creating and Assigning Security Zones

Before you can use Security Zones in the Rule Base, you must assign Gateway interfaces to Security Zones.

To create a Security Zone:

1. In the **Objects bar** (F11), click **New** > **More** > **Network Object** > **Security Zone**.

   The **Security Zone** window opens.
2. Enter a name for the Security Zone.

3. Enter an optional comment or tag.
4. Click **OK**.

To assign an interface to a Security Zone

1. In the **Gateways & Servers** view, right-click a Security Gateway object and select **Edit**.

   The **Gateway Properties** window opens.
2. In the **Network Management** pane, right-click an interface and select **Edit**.

   The **Interface** window opens. The **Topology** area of the **General** pane shows the Security Zone to which the interface is already bound. By default, the Security Zone is calculated according to where the interface **Leads To**.
3. Click **Modify**.

   The **Topology Settings** window opens.
4. In the **Security Zone** area, click **User Defined** and select **Specify Security Zone**.
5. From the drop-down box, select a Security Zone.

   Or click **New** to create a new one.
6. Click **OK**.

Predefined Security Zones

These are the predefined security zones, and their intended purposes:

- **WirelessZone** - Networks that can be accessed by users and applications with a wireless connection.
- **ExternalZone** - Networks that are not secure, such as the Internet and other external networks.
- **DMZZone** - A DMZ (demilitarized zone) is sometimes referred to as a *perimeter* network. It contains company servers that can be accessed from external sources.

  A DMZ lets external users and applications access specific internal servers, but prevents the external users accessing secure company networks. Add rules to the firewall Rule Base that allow traffic to the company DMZ. For example, a rule that allows HTTP and HTTPs traffic to your web server in the DMZ.
- **InternalZone** - Company networks with sensitive data that must be protected and used only by authenticated users.

Large Scale VPN Profile - General

What can I do here?

Use this window to define the LSV Profile.

- **Name** - Enter a name for the LSV profile, as a unique network object.
- **Certificate Authority** - Peers' certificates are signed by CA

Select a Certificate Authority from the list. A CA can sign for only one LSV profile.

Getting Here - Object Explorer > New > Network Object > LSV Profile > General

Large Scale VPN Profile - VPN Domain

What can I do here?

Use this window to define limitations for LSV peers:

Peer Limit

Limit peer's VPN Domain size to - Select to set the maximum number of IP addresses in the VPN domain.

IP addresses allowed in the VPN domain

- **Allow any** - All IP addresses can be included in the VPN domain.
- **Restrict to these groups or networks** - Include only the selected groups or networks in the peer domain.

Getting Here - Object Explorer > New > Network Object > LSV Profile > VPN Domain

Domain

What can I do here?

Use this window to create or edit a domain.

Getting Here - Object Explorer > New > Network Object > More > Domain

Domains

A Domain object lets you define a host or DNS domain by its name only. It is not necessary to have the IP address of the site.

You can use the Domain object in the source and destination columns of an Access Control Policy.

You can configure a Domain object in two ways:

- Select **FQDN**

  In the object name, use the Fully Qualified Domain Name (FQDN). Use the format . `x.y.z` (with a dot "." before the FQDN). For example, if you use . `www.example.com` then the Gateway matches `www.example.com`

  This option is supported for R80.10 and higher, and is the default. It is more accurate and faster than the non-FQDN option.

The Security Gateway looks up the FQDN with a direct DNS query, and uses the result in the Rule Base.

This option supports SecureXL Accept templates. Using domain objects with this option in a rule has no effect on the performance of the rule, or of the rules that come after it.

- Clear **FQDN**

This option enforces the domain and its sub-domains. In the object name, use the format . `x.y` for the name. For example, use . `example.com` or . `example.co.uk` for the name. If you use . `example.com`, then the Gateway matches `www.example.com` and `support.example.com`

The Gateway does the name resolution using DNS reverse lookups, which can be inaccurate. The Gateway uses the result in the Rule Base, and caches the result to use again.

When upgrading from R77, this option is enforced.

VoIP Domain - SIP Proxy

What can I do here?

Use this window to create or edit a SIP Proxy (also known as a SIP server or Registrar).

Getting Here - Object Explorer > New > Network Object > More > VoIP Domain > SIP Proxy

VoIP Domains

There are five types of VoIP Domain objects:

- VoIP Domain SIP Proxy
- VoIP Domain H.323 Gatekeeper
- VoIP Domain H.323 Gateway
- VoIP Domain MGCP Call Agent
- VoIP Domain SCCP CallManager

In many VoIP networks, the control signals follow a different route through the network than the media. This is the case when the call is managed by a *signal routing* device. Signal routing is done in SIP by the *Redirect Server*, *Registrar*, and/or *Proxy*. In SIP, signal routing is done by the *Gatekeeper* and/or *gateway*.

Enforcing signal routing locations is an important aspect of VoIP security. It is possible to specify the endpoints that the signal routing device is allowed to manage. This set of locations is called a *VoIP Domain*. For more information refer to the: *R81.10 VoIP Administration Guide*

Supported SIP Topologies and NAT Support

Below is a list of supported SIP topologies. The table also lists NAT that you can configure with each topology. it with. SIP can use a Proxy (or Registrar). If there is more than one proxy device, signaling passes through one or more of them. After the call is set up, the media can pass from endpoint to endpoint directly, or through one or more of the proxies.

Deployment	Supports No-NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Proxy - Static NAT	Description
SIP Endpoint to Endpoint	Yes	Static NAT only	Not applicable	■ Phones communicate directly without a proxy. ■ Static NAT can be configured for the phones on the internal side of the gateway.

Deployment	Supports No-NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Proxy - Static NAT	Description
SIP Proxy in External Network	Yes	Yes	Not applicable	■ IP phones use the services of a proxy on the external side of the gateway. ■ Enables the use of a proxy that is maintained by another organization. ■ Configure Hide NAT, Static NAT, or no-NAT for the phones on the internal side of the gateway.
SIP Proxy to SIP Proxy	Yes	Yes	Yes	■ Each proxy controls a separate endpoint domain. ■ Configure Static NAT for the internal proxy. ■ Configure Hide NAT or Static NAT for the internal phones.

Deployment	Supports No-NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Proxy - Static NAT	Description
SIP Proxy in DMZ	Yes	Yes	Yes	■ The same proxy controls both endpoint domains. This makes it possible to provide proxy services to other organizations. ■ Static NAT or no-NAT can be configured for the proxy. ■ Hide NAT, Static NAT, or no NAT can be configured for the phones on the internal side of the gateway.

For complete information on NAT configuration, see the *R81.10 Security Management Administration Guide*

Below are some exceptions when you use SIP with NAT:

- NAT is not supported on IP addresses behind an external Check Point gateway interface.
- Calls cannot be made from an external source to two endpoints on the trusted side of a gateway if only one of the endpoints is NAT enabled.
- You can use Automatic NAT for other deployments.

Additional Conditions for Using NAT in SIP Networks

You can use SIP with NAT with these exceptions:

- NAT is not supported on IP addresses behind an external Check Point gateway interface.
- Manual NAT rules are only supported for proxies in DMZ deployments. You can use Automatic NAT as an alternative.

- Calls cannot be made from an external source to two endpoints on the trusted side of a gateway if one of the endpoints is NAT enabled and the other is not.

VoIP Domain - H.323 Gatekeeper

What can I do here?

Use this window to create or edit a H.323 Gatekeeper.

Getting Here - Object Explorer > New > Network Object > More > VoIP Domain > H.323 Gatekeeper > General

Introduction to H.323

H.323 is an International Telecommunication Union (ITU) standard that specifies the components, protocols and procedures that provide multimedia communication services, real-time audio, video, and data communications over packet networks, including IP based networks.

H.323 registration and alternate communication occurs on UDP port 1719, and H.323 call signaling occurs on TCP port 1720. H.323 is a peer-to-peer protocol.

The Security Gateway supports these H.323 architectural elements:

- **IP phones**

  Devices that:

  - Handle signaling (H.323 commands)
  - Connect to an H.323 Gatekeeper

  IP phones are Configured in SmartConsole, usually as a network of IP phones. It is usually not necessary to Configure Network Objects for individual IP Phones.

- **Standard telephones**

  Connect to an H.323 gateway. These are not IP devices. It is not necessary to Configure them in SmartConsole.

- **Gatekeeper**

  Manages a collection of H.323 devices, such as phones. A Gatekeeper converts phone numbers to IP addresses and can provide gateway services as well.

- **Gateway**

  Provides interoperability between different networks. The gateway translates between the telephony protocol and IP.

Supported H.323 Deployments and NAT

Supported H.323 deployments are listed the table. Hide NAT, or Static NAT can be configured for the phones in the internal network, and (where applicable) for the gatekeeper.

- NAT is not supported on IP addresses behind an external Check Point gateway interface.
- Manual NAT rules are only supported in environments where the Gatekeeper is in the DMZ.

Supported H.323 Topology	Supports No NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Gatekeeper - Static NAT	Description
H.323 Endpoint to Endpoint	Yes	Static NAT only	N/A	• The IP Phones communicate directly, without a Gatekeeper or an H.323 gateway. Static NAT can be configured for the phones on the internal side of the gateway.

Supported H.323 Topology	Supports No NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Gatekeeper - Static NAT	Description
H.323 Gatekeeper/ Gateway in External Network	Yes	Yes	N/A	• The IP phones use the services of a Gatekeeper or H.323 gateway on the external side of the gateway. • This topology enables the use of the services of a Gatekeeper or an H.323 gateway that is maintained by another organization.
H.323 Gatekeeper/ Gateway to Gatekeeper/ Gateway	Yes	Yes	Yes	• Each Gatekeeper or H.323 gateway controls a separate endpoint domain. • Static NAT can be configured for the internal Gatekeeper. For the internal phones, Hide NAT or Static NAT can be configured.

Supported H.323 Topology	Supports No NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Gatekeeper - Static NAT	Description
H.323 Gatekeeper/ Gateway in DMZ	Yes	Yes	Yes	• The same Gatekeeper or H.323 gateway controls both endpoint domains. This topology makes it possible to provide Gatekeeper or H.323 gateway services to other organizations. • Static NAT or No-NAT can be configured for the Gatekeeper or H.323 gateway. • Hide NAT or Static (or no NAT) can be configured for the phones on the internal side of the gateway.

VoIP Domain - H.323 Gatekeeper Routing Mode

What can I do here?

Use this window to configure the allowed routing mode.

Getting Here - Object Explorer > New > Network Object > More > VoIP Domain > H.323 Gatekeeper > Routing mode

VoIP Domain - H.323 Gateway

What can I do here?

Use this window to create or edit a H.323 Gateway.

Getting Here - Object Explorer > New > Network Object > More > VoIP Domain > H.323 Gateway > General

VoIP Domain - H.323 Gateway Routing Mode

What can I do here?

Use this window to select the routing mode.

Getting Here - Object Explorer > New > Network Object > More > VoIP Domain > H.323 Gateway > Routing mode

VoIP Domain - MGCP Call Agent

What can I do here?

Use this window to configure an MGCP Call Agent.

Getting Here - Object Explorer > New > Network Object > More > VoIP Domain > MGCP Call Agent

MGCP Rules for a Call Agent in the External Network

An MGCP topology with a Call Agent in the external network is shown in the image. You can configure Hide or Static NAT for the phones in the internal network.

In this image, the IP phones use a Call Agent on the external side of the gateway. This topology enables a Call Agent maintained by another organization. It is possible to configure Hide NAT, Static NAT or no-NAT for the phones on the internal side of the gateway.

This procedure shows how to:

- Allow bidirectional calls between the MGCP phones in the internal network (Net_A) and phones in an external network (Net_B)
- Configure NAT for the internal phones



VoIP rule for this scenario:

Source	Destination	Services & Applications	Action
MGCP_Call_ Agent Net_A	Net_A MGCP_Call_ Agent	mgcp_CA or mgcp_MG or mgcp_ dynamic_ports	Accept

1. Configure the Network Objects (nodes or networks) for IP phones managed by the MGCP Call Agent and their calls, subject to gateway inspection.

   For the example in the image, these are Net_A and Net_B.
2. Configure the Network Object for the Call Agent (MGCP_Call_Agent).
3. Configure the VoIP rule.
4. Configure Hide NAT or Static NAT for the phones in the internal network. Do this by editing the Network Object. See Setting up your network for Network Address Translation.
5. In SmartConsole, install the policy.

VoIP Domain - SCCP Call Manager

What can I do here?

Use this window to configure an SCCP Call Manager.

Getting Here - Object Explorer > New > Network Object > More > VoIP Domain > SCCP Call Manager

Introduction to SCCP Security and Connectivity

SCCP (Skinny Client Control Protocol) controls telephony gateways from external call control devices called Call Agents (also known as Media Gateway Controllers).

Connectivity and network level security for SCCP-based VoIP communication is supported. All SCCP traffic is inspected and legitimate traffic is allowed. Attacks are blocked. Other firewall gateway capabilities are supported, such as anti- spoofing and protection against denial of service attacks.

The validity of SCCP message states is verified for all SCCP messages. For a number of key messages, the existence and validity of the message parameters are also verified.

SCCP Supported Deployments

NAT on SCCP devices is not supported.

The Security Gateway supports SCCP deployments listed in the table.

Supported SCCP Topology	Description
Call Manager in the Internal Network	The IP phones use the services of a Call Manager in an internal network.
Call Manager in the External Network	The IP phones use the services of a Call Manager on the external side of the gateway. This topology enables the use of the services of a Call Manager that is maintained by another organization.
Call Manager in the DMZ	The same Call Manager controls both endpoint domains. This topology makes it possible to provide Call Manager services to other organizations.

Logical Server

What can I do here?

Use this window to create or edit a logical server.

Getting Here - Object Explorer > Network Object > More > Logical server

Logical Servers

A Logical Server is a group of machines that provides the same services. The workload of this group is distributed between all its members.

When a Server group is stipulated in the **Servers group** field, the client is bound to this physical server. In Persistent server mode the client and the physical server are bound for the duration of the session.

- Persistency by Service - once a client is connected to a physical server for a specified service, subsequent connection to the same Logical Server and the same service will be redirected to the same physical server for the duration of the session.
- Persistency by Server - once a client is connected to a physical server, subsequent connections to the same Logical Server (for any service) will be redirected to the same physical server for the duration of the session.

Balance Method

The load balancing algorithm stipulates how the traffic is balanced between the servers. There are several types of balancing methods:

- **Random** - The new connection is assigned to a server at random.
- **Server Load** - The Security Gateway determines which server is best equipped to handle the new connection.
- **Round Robin** - The new connection is assigned to the first available server.
- **Round Trip** - .Not supported.
- **Domain** - Not supported.

Access Point Name

What can I do here?

Use this window to create or edit an access point name.

Getting Here - Object Explorer > New > Network Object > More > Access Point Name

Access Point Name

An Access Point Name provides routing information for SGSNs (Serving GPRS Support Nodes) and GGSNs (gateway GPRS Support Nodes). The APN, which is written as a string, contains the identity of the external service requested (the Operator ID) by the MS, and routing information (the Network ID). The two IDs are written something like this:

Operator ID: *MNC1234.MCC5678.gprs*

Network ID: *example.net*

Check Point has taken APNs a step further, integrating support of domains with APNs. A domain, consisting of addresses, IP subnets, address ranges or groups thereof, may be configured on an APN object. APN Domains specify the range of IP addresses that are assigned to MSs upon connecting to an APN. For example, you can create one APN called *Content_Servers* that assigns a range of IP addresses from 10.1.1.1 to 10.1.10.255, and another called *Internet*, that assigns from a range of 192.168.1.1 to 192.168.10.255.

You can also use APN objects to specify from which networks PDP contexts for enterprise APNs may be created, or to grant the CEO sole access to a specific APN, or to accept Handovers only between specified networks.

Configuring APN Options

Tell me about the fields

- **Name** the APN with a user-friendly name.
- **APN string** is the actual Access Point Name. An example of an **APN string** is **internet.mnc55.mcc243.gprs** , or **example.com** . You can also use an APN object to match multiple APN strings through the use of wildcards. For example, you can create an APN object called *.example.gprs that will match APN object strings like 123.example.gprs and abc.example.gprs.

Intra Tunnel Policy Enforcement

This section of the **APN object** window sets whether the APN allows PDP context activations from specified end user IP addresses in a number of circumstances.

- **Enforce End User Domain** to allow only the address or addresses specified in the **End User Domain** drop-down list. Any PDP context activations using addresses other than the one(s) specified here are blocked and logged.
- To prevent an MS from sending undesirable traffic to another MS, you can block internal GTP tunnel communications between MSs.
- **Block MS to MS traffic between this and other APN End User Domains** to drop and log intra-tunnel traffic between two MSs with server IP addresses *other than the one* specified APN **End User Domain**
- **Block MS to MS traffic within this End User Domains**to drop and log intra-tunnel traffic between two MSs with server IP addresses *that match* the address specified in the **End User Domain** drop-down list.

TCP, UDP, and SCTP Services - General

What can I do here?

Use this window to define general properties for TCP, UDP, and SCTP services.

Getting Here - Object Explorer > New > Service > TCP/UDP/SCTP > General

Understanding TCP, UDP, and SCTP Resources

Use a TCP Resource to perform CVP or UFP content security on any TCP Service, using a third party OPSEC compliant application.

The TCP resource turns on genericid, a generic daemon (security server) that receives data packets and sends them to a CVP or UFP server, as defined by the TCP Resource.

The TCP Resource is triggered when a Rule includes the TCP Resource, and a connection is encountered that matches the Source and Destination of the Rule, and also matches the TCP service that is associated with the TCP resource. If there is a match, then the action specified in the rule is applied.

To create a Rule with a TCP Resource, the TCP Resource must be associated with a particular TCP service. Only TCP services where **Enable for TCP resource** is checked can be associated with a TCP resource.

Match for 'Any' and Source Port

When installing a policy that contains services that have source ports (specified in the Advanced window) that require the **Match for 'Any'** option to be selected, a warning appears. The policy will be installed with a warning (for each such service), since **Match for 'Any'** is not supported for services that contain source port specification.

TCP, UDP, and SCTP General Options

- **Protocol**. Select the protocol type associated with the service, and by implication, the management server (if any) that enforces Content Security and Authentication for the service. Selecting a Protocol Type invokes the specific protocol handlers for each protocol type, thus enabling higher level of security by parsing the protocol, and higher level of connectivity by tracking dynamic actions (such as opening of ports).
- **Protocol Signature**. Check Point has created a unique signature for each protocol and stored it on the gateway. The signature identifies the protocol as genuine. Select this option to limit the port to the specified protocol.
- **Port** is the number of the port used to provide this service. To specify a port range, place a hyphen between the lowest and highest port numbers, for example 44-55.

Understanding SCTP

Stream Control Transmission Protocol (SCTP) is a message-based, multi-streaming transport layer protocol commonly used in telephony applications.

Configuring SCTP Inspection

When a Carrier license is installed, you can specify SCTP services in your Firewall rules. SCTP Inspection occurs in these cases:

- There is a match on a rule containing an SCTP or Diameter SCTP service in the **Service** cell.
- There is a match on a rule with **Service** = **Any** and this SCTP service has **Match for any** selected.

To activate SCTP Inspection:

1. Open **SmartConsole** > **Menu** > **Object Explorer** > **New** > **Service** > **SCTP**.

   The **SCTP Properties** window opens.

   On the **General** page:

   - **Name** - The name of the service. The name assigned here must be the same as the server service name (as in the services file). If NIS is used, the firewall automatically retrieves the information from NIS.
   - **Port** - The number of the port that matches this service.

2. Click **Advanced**.

   - **Source Port** - Port number for the client side service. If specified, only those Source port Numbers will be Accepted, Dropped, or Rejected during packet inspection. Otherwise, the source port is not inspected.
   - **Keep connections open after policy has been installed** - If the connections are not allowed in the new policy, they are still kept. This overrides the settings in the Connection Persistence page. If you change this property, the change does not have effect on open connections, but only future connections.
   - **Virtual session timeout** - set the virtual session timeout or keep the default value (in seconds)

- **Enable Aggressive Aging** - Sets short (aggressive) timeouts for idle connections. When a connection is idle for more than its aggressive timeout value, it is marked as *eligible for deletion*. When memory consumption or connections table capacity exceeds a user-defined threshold (high watermark), aggressive aging starts. Each incoming connection starts to delete *k* (10 by default) connections that are eligible for deletion. This continues until memory consumption or connections capacity decreases below the low value.

- **Synchronize connection on cluster** - Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with **Synchronize connections on cluster** selected are synchronized as they go through the cluster. By default, all new and existing services are synchronized.

1. Click **OK**.
2. Open **Global properties** > **Stateful Inspection**.

   Configure these **Stateful Inspection** options:

Option	Meaning
SCTP start timeout	■ An SCTP connection times out if the interval between the arrival of the first packet and establishment of the connection (STCP four-way handshake) exceeds the SCTP start timeout in seconds. ■ Attribute name in Database Tool (GuiDBEdit Tool): `sctpstarttimeout`
SCTP session timeout	■ Length of time an idle connection remains in the Security Gateway connections table. ■ Attribute name in Database Tool (GuiDBEdit Tool): `sctptimeout`
SCTP end timeout	■ A SCTP connection will only terminate SCTP end timeout seconds after two FIN packets (one in each direction: client-to-server, and server-to-client) or an RST packet. ■ Attribute name in Database Tool (GuiDBEdit Tool): `sctpendtimeout`

Configure these options for **Out of state packets**:

Option	Meaning
Drop out of state SCTP packets	■ Drop SCTP packets that are not consistent with the current state of the SCTP connection. ■ Attribute name in Database Tool (GuiDBEdit Tool): `fw_drop_out_of_state_sctp`

Option	Meaning
Log on drop	■ Generates a log entry when out of state SCTP packets are dropped. ■ Attribute name in Database Tool (GuiDBEdit Tool): `fw_log_out_of_state_sctp`

To deactivate out of state packet drop in SmartConsole:

1. Open **Menu** > **Global properties** > **Stateful Inspection**.
2. Clear the **Drop out of state SCTP packets** option.
3. Save and install the policy.

To deactivate packet inspection using Database Tool (GuiDBEdit Tool):

1. Open **Database Tool (GuiDBEdit Tool)** .
2. Search for: `fw_sctp_packet_inspection`.
3. Set the property to **false**.
4. Save the database and install policy.

Configuring SCTP Acceleration

To enable SCTP acceleration:

```
sim feature sctp on
```

To disable SCTP acceleration, run: `sim feature sctp off`

Note : If SCTP acceleration is activated and SCTP inspection is deactivated, the Performance Pack accelerates all SCTP packet types.

Configuring SCTP NAT

SCTP NAT overrides the defined NAT policy. When this feature is not activated, SCTP connections do not use NAT.

To activate SCTP NAT:

On the Security Gateway, run: `fw ctl set int fwx_enable_sctp_nat 1`

To deactivate SCTP NAT: `fw ctl set int fwx_enable_sctp_nat 0`

TCP Service - Advanced

What can I do here?

Use this window to configure advanced options for the TCP service.

Getting Here - Object Explorer > New > Service > TCP > Advanced

TCP - Advanced Options

Advanced - sets the advanced options for this service.

- **Source Port** - Enter a port number for the client side service. If specified, only those Source port Numbers will be Accepted, Dropped, or Rejected when inspecting packets of this service. Otherwise, the source port is not inspected.
- **Protocol Signature** - A unique signature created by Check Point for each protocol and stored on the gateway. The signature identifies the protocol as genuine. Select this option to limit the port to the specified protocol. To use protocol signature, enable Application & URL Filtering for the layer and Application Control on the gateway.
- **Enable for TCP resource** - Enables the TCP service for a TCP Resource, if checked.
- **Match for Any** - Indicates whether this service is used when 'Any' is set as the rule's service and there are several service objects with the same source port and protocol.

  When there is a rule whose **Service**cell contains **Any**, and a connections protocol and source port match more than one service object, then the service object with the selected **'Match for Any'**option will be used and its properties will be taken for handling this connection
- **Keep connections open after policy has been installed** even if they are not allowed under the new policy. This overrides the settings in the Connection Persistence page. If you change this property, the change will not affect open connections, but only future connections.

Virtual session timeout - Time (in seconds) before the session times out. Select one of the following options:

- **Default** - Use the default value defined on the **Stateful Inspection** page in the **Global Properties** window.
- **Specific** - Manually define a timeout period specifically for this service.

Aggressive aging

- **Enable Aggressive Aging** - Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.

Cluster and Synchronization

- **Synchronize connections on cluster** - Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster.

  Of the services allowed by the Rule Base, only those with **Synchronize connections on cluster** will be synchronized as they pass through the cluster. By default, all new and existing services are synchronized.

- **Start Synchronizing X seconds after connection initiation** - For all TCP services whose Protocol Type is *HTTP* or *None*, enable this option to delay telling the Security Gateway about a connection, so that the connection will only be synchronized if it still exists x seconds after the connection is initiated. Note that delayed synchronization is disabled if the log or account are enabled.

  Some TCP services (HTTP for example) are characterized by connections with a very short duration. There is no point in synchronizing these connections because every synchronized connection consumes gateway resources, and the connection is likely to have finished by the time a failover occurs.

  This capability is only available if a SecureXL-enabled device is installed on the Security Gateway through which the connection passes. The setting is ignored if connection templates are not off-loaded from the SecureXL-enabled device. See the Performance Pack documentation for additional information.

UDP - Advanced Options

What can I do here?

Use this window to configure advanced options for the UDP service.

Getting Here - Object Explorer > New > Service > UDP > Advanced

Advanced Options

Advanced - sets the advanced options for this service.

- **Accept replies** - Specifies if UDP replies are to be accepted for this service.
- **Protocol Signature** - A unique signature created by Check Point for each protocol and stored on the gateway. The signature identifies the protocol as genuine. Select this option to limit the port to the specified protocol. To use protocol signature, enable Application & URL Filtering for the layer and Application Control on the gateway.
- **Enable for TCP resource** - Enables the TCP service for a TCP Resource, if checked.
- **Match for Any** - Indicates whether this service is used when 'Any' is set as the rule's service and there are several service objects with the same source port and protocol.

When there is a rule whose **Service**cell contains **Any**, and a connections protocol and source port match more than one service object, then the service object with the selected **'Match for Any'**option will be used and its properties will be taken for handling this connection

- **Keep connections open after policy has been installed** even if they are not allowed under the new policy. This overrides the settings in the Connection Persistence page. If you change this property, the change will not affect open connections, but only future connections.

Virtual session timeout - Time (in seconds) before the session times out. Select one of the following options:

- **Default** - Use the default value defined on the **Stateful Inspection** page in the **Global Properties** window.
- **Specific** - Manually define a timeout period specifically for this service.

Aggressive aging

- **Enable Aggressive Aging** - Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.

Cluster and Synchronization

- **Synchronize connections on cluster** - Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster.

  Of the services allowed by the Rule Base, only those with **Synchronize connections on cluster** will be synchronized as they pass through the cluster. By default, all new and existing services are synchronized.

- **Start Synchronizing X seconds after connection initiation** - For all TCP services whose Protocol Type is *HTTP* or *None*, enable this option to delay telling the Security Gateway about a connection, so that the connection will only be synchronized if it still exists x seconds after the connection is initiated. Note that delayed synchronization is disabled if the log or account are enabled.

  Some TCP services (HTTP for example) are characterized by connections with a very short duration. There is no point in synchronizing these connections because every synchronized connection consumes gateway resources, and the connection is likely to have finished by the time a failover occurs.

  This capability is only available if a SecureXL-enabled device is installed on the Security Gateway through which the connection passes. The setting is ignored if connection templates are not off-loaded from the SecureXL-enabled device. See the Performance Pack documentation for additional information.

SCTP - Advanced Options

What can I do here?

Use this window to configure advanced options for the SCTP service.

The options are the same as those for *"TCP - Advanced Options" on page 566*.

Getting Here - Object Explorer > New > Service > SCTP > Advanced

RPC

What can I do here?

Use this window to configure RPC general properties.

Getting Here - Object Explorer > New > Service > RPC

SunRPC Overview

What Background Information do I need to know...

RPC-based services do not use pre-defined port numbers. An RPC "connection" is structured as follows:

1. The client queries the server (on port 111), asking for the port number associated with the program.
   - If the query is UDP, the Firewall examines the program number, and allows only those programs allowed by the security policy (in the Services column).
   - If the query is TCP, the Firewall drops the query, unless TCP on port 111 is explicitly allowed by the security policy.

     Note - Allowing TCP on port 111 is considered insecure, because the client can then run any available RPC program through this port
2. The server (portmapper) replies with the port number. The Firewall monitors the reply and opens only the specified port for the RPC traffic.
3. The client connects to that port and the RPC "connection" continues.

Example:

Suppose the security policy allows RPC as follows:

Source	Destination	Service	Action
RPC_Client	RPC_Server	nfsprog	Accept

- If RPC_Client issues a portmapper query on TCP port 111, the Firewall drops the query packet.
- If RPC_Client issues a portmapper query on UDP port 111, the Firewall allows the query only if the program number is 100003, as specified in the RPC Service Properties window for the nfsprog service. Moreover, the Firewall monitors the reply and then allows the nfsprog service only on the port specified in the reply.
- If RPC_Client does not issue a portmapper query, but proceeds to directly communicate on the nfsprog port (100003, as specified in the RPC Service Properties window for the nfsprog service), the Firewall queries portmapper and allows the connection only if the port number (in the portmapper reply) is also 100003.

RPC

Tell me about the fields...

- **Name** - should be identical to the server service name (as it appears in the services file), so that the Firewall will be able to retrieve some properties automatically. If NIS is being used, the Firewall will automatically retrieve the information from the NIS.
- **Program Number** - can be retrieved from the RPC database, if it is a standard service. If the program number is omitted, the Firewall attempts to resolve the program number (based on the service's name) when the policy is installed. If resolution fails, an error message is issued and installation will fail.
- **Keep connections open after policy has been installed** - keeps all control and data connections open until the connections have ended, even if they are not allowed under the new policy. This overrides the settings in the **Connection Persistence** page. If you change this property, the change will not affect open connections, but only future connections.

DCE-RPC

What can I do here?

Use this window to define general properties for DCE-RPC services.

Note - The ALL_DCE_RPC service authorizes all DCE RPC services.

Getting Here - Object Explorer > New > Service > DCE-RPC

The DCE-RPC Protocol

What background information do I need to know?

DCE RPC is a protocol for calling a procedure on a remote machine as if it were a local procedure call. The protocol uses a Universal Unique Identifier (UUID) to connect remote machine Interfaces and operates over TCP/IP and UDP/IP transports.

DCE-RPC Properties

Tell me about the fields...

- **Interface UUID** - identifies the Universal Unique Identifier (UUID) to which the requested service belongs. An interface is a set of remotely callable operations offered by a server and invokable by clients.
- **Keep connections open after policy has been installed** - keeps all control and data connections open until the connections have ended, even if they are not allowed under the new policy. This overrides the settings in the **Connection Persistence** page. If you change this property, the change will not affect open connections, but only future connections.

ICMP

What can I do here?

Use this window to define general properties for the ICMP/ICMPv6 service.

Getting Here - Object Explorer > New > Service > ICMP Service > ICMP/ ICMPv6

ICMP Properties

- **Name** assigned here should be identical to the server service name (as it appears in the services file), so that the Firewall will be able to retrieve some properties automatically. If NIS is being used, the Firewall will automatically retrieve the information from the NIS.
- **ICMP Type** and **Code**, as listed in RFC 792. See http://www.iana.org/assignments/icmp-parameters.
- **Keep connections open after policy has been installed**even if they are not allowed under the new policy. This overrides the settings in the **Connection Persistence** page. If you change this property, the change will not affect open connections, but only future connections.

GTP - General

What can I do here?

Use this window to set the general properties of the GTP service.

Getting Here - Object Explorer > New > Service > GTP > General

Configuring GTP

1. Give the new GTP service filter a name.

   Note - The port numbers of the GTP services cannot be modified.

2. Select a version.
3. Select **Reverse Service** if want to accept PDUs from the GGSN/PGW to the SGSN/SGW on a previously established PDP context even if different ports are used.
4. For **GTP Message Filtering**, select an Interface Profile

   GTP Message Filtering Specifies GTP interface profile which defines associated control messages that match this service. You can create a custom profile or manually customize a service to filter specific message types.

5. Select **Actions**

   - **Allow usage of static IP addresses** lets mobile subscribers with pre-assigned IP addresses to make a connection. While IP addresses are usually allocated by the GGSN, some users may have static, pre-assigned IP addresses. The default is to allow such paths. When this option is set, PDP context activation will be enabled in static mode as well.
   - **Apply Access Policy on user traffic** causes all mobile user traffic encapsulated in G-PDUs to be inspected by the Firewall blade and IPS stateful inspection. This prevents GTP-U acceleration and requires consideration when allocating CPU cores for CoreXL instances and SND.
   - **Add IMSI field to logs generated by user traffic** inserts the value in the IMSI field for any log generated by mobile user data, linking the log to the mobile user.

GTP - Advanced

What can I do here?

Use this window to define a GTP-specific security policy. Set which prefixes or other identifiers to allow onto your network.

Note - We recommend that you create a new service and do not change the pre-defined service **gtp_v1_default** .

Getting Here - Object Explorer > New > Service > GTP > Advanced

Matched PDP Contexts

In addition to the source and destination IP addresses of the GTP traffic, it is possible to further match PDP Contexts according to **IMSI Prefix** , **APN** , **Selection Mode** , **MS-ISDN** , and **LDAP** . Either specify a value for the parameter, or select **Any** .

Tell me about the fields...

Matched PDP Contexts

- **Match specific IMSI Prefix** - to specify an allowable subscriber identity prefix or select **Any** to allow all prefixes access. The subscriber identity prefix is usually of the form Country and Operator, for example, *23477* (where *234* is the MCC and *77* is the MNC). Alternatively, select **Any** to allow all prefixes access.
- **Match specific Access Point Name** - to specify an APN object or select **Any**to allow all APNs access.
- **Match specific Selection Mode** - to specify the origin of the APN that appears in the create PDP context request. There are three types of APN selection modes:
  - *0 - verified* is where either the MS or the network selects the APN, and the system verifies that the MS is subscribed to this APN.
  - *1 - MS - not verified* is where the **MS** selects the APN, and the system **does not** verify whether the MS is subscribed to this APN.
  - *2 - Network - not verified* is where the **network** selects the APN, and the system **does not** verify whether the MS is subscribed to this APN.
- **Match specific MS-ISDN Prefix** - to specify an MS-ISDN prefix or select **Any** to allow all prefixes access. An example of an MS-ISDN prefix is *447788*.
- **Match with LDAP Group** - allows you to specify an LDAP group, sorted by two main attributes.
  - **according to IMSI** or **MS-ISDN** - allows you to identify whether a user belongs to a specific LDAP group by IMSI or MS-ISDN.

GTP - Radio Access Technology

What can I do here?

Use this window to select Radio Access Technologies.

Specify which radio types a request has to match.

You can customize the service to perform these actions on matching GTP traffic.

Getting Here - Object Explorer > New > Service > GTP > Radio Access Technology

GTP - Additional Services

What can I do here?

Use this window to select additional services.

On the **General** page, if you selected V2 as the version, select one or more of these additional service types:

- Trace Management
- CS Fallback and SRVCC
- Restoration and Recovery

Add a rule in the rule base using this service and make sure the rule is above all other GTP-based rules.

Getting Here - Object Explorer > New > Service > GTP > Radio Access Technology

Compound TCP Service

What can I do here?

Use this window to configure a compound TCP Service.

Getting Here - Object Explorer > New > Service > Compound TCP

Compound TCP

Compound TCP (CTCP) is a Microsoft algorithm designed to optimize TCP connections for large bandwidth-delay products without unfairly diverting system resources from applications and users.

Citrix TCP

What can I do here?

Use this window to see general properties for the Citrix Service.

Note - the port field shows the default Citrix ICA port: 1494.

Getting Here - Object Explorer > Service > Citrix TCP

Other Service - General

What can I do here?

Use this window to configure general properties for a service other than TCP, UDP, ICMP, or RPC.

Note - A user defined service requires familiarity with the INSPECT script language.

Getting Here - Object Explorer > New > Service > Other Service > General

Other Service Properties

Tell me about the fields...

- **Name** - assigned here should be identical to the server service name (as it appears in the services file), so that the Firewall will be able to retrieve some properties automatically. If NIS is being used, the Firewall automatically retrieves the information from the NIS.
- **IP Protocol** - specifies the number of IP Protocol. In the four layer network model, the IP Protocol is the top, Transport layer. Types of IP protocols are TCP (IP protocol 6) and UDP (IP protocol 17). IP protocols are listed in *IANA Protocol Numbers*.
- **Keep connections open after policy has been installed** - keeps all control and data connections open until the connections have ended, even if they are not allowed under the new policy. This overrides the settings in the **Connection Persistence** page. If you change this property, the change will not affect open connections, but only future connections.

Other Service - Advanced

What can I do here?

Use this window to set advanced properties for the user defined service.

Getting Here - Object Explorer > New > Service > Other Service > Advanced

User defined Services

What background information do I need to know?

To define a user defined service, you must enter INSPECT code in the Match field, so you must have at least a basic familiarity with INSPECT.

Suppose the **IP Protocol** field has the value of 17 (UDP Protocol) and the Match field has the following value:

```
uh_dport > 33000, ip_ttl < 30
```

To understand the meaning of the Match field, consider the relevant definitions in `$FWDIR/lib/base.def`:

Name	Definition	Meaning
`uh_dport`	`[ 22 : 2, b]`	the UDP destination port
`p_ttl`	`[8 : 1]`	IP Time To Live

The comma operand in INSPECT means "and", so the meaning of Match is:

- AND the destination port greater than 33000
- AND packet's time to live is less than 30

Suppose you wish to pass IP protocol number 53, similar to ospf, egp, and bgp, then define a user-defined service whose **IP Protocol** field is 53.

Other Service Options

Tell me about the fields...

- **Match** - contains an INSPECT expression that defines the matching criteria. The connection is examined against the expression during the first packet.

  Example: `tcp, dport = 21, direction = 0` matches incoming FTP control connections.

- **Action** - contains an INSPECT expression that defines the action to take if a rule containing this service is matched.

  Example: `set r_mhandler &open_ssl_handler` sets a handler on the connection.

  For more on the **Match** and **Action** fields, see: sk109195

- **Show Install Policy verification warning** - removes errors when installing a policy on an R80 gateway. This option only shows after upgrading to R80. Leaving this option selected means that **Match** or **Action**expressions that were not converted before the upgrade to R80 will continue to generate verification warnings during a policy install. The option is selected by default. Once you clear it, the option is no longer available.
- **Protocol Type** - specifies which protocol type is associated with the service, and by implication, the security server (if any) that enforces Content Security and Authentication for the service. Selecting a Protocol Type invokes the specific protocol handlers for each protocol type, thus enabling higher level of security by parsing the protocol, and higher level of connectivity by tracking dynamic actions (such as opening of ports).
- **Accept Replies** - specifies if Other Service replies are to be accepted. To specify that no Other Service replies will be accepted, that is, to define a "one-way" Other service, deselect **Accept Replies** .

  Accept Replies - corresponds to the following field in the **Stateful Inspection** page of the **Global Properties** window: **Accept stateful Other IP Protocol replies for unknown services** . The latter applies to Other services that are not defined in the Check Point Services objects tree.
- **Match for 'Any'** - indicates whether this service is used when 'Any' is set as the rule's service and there are several service objects with the same source port and protocol. When there is a rule whose **Service**cell contains **Any**, and a connections protocol and source port match more than one service object, then the service object with the selected **'Match for Any'**option will be used and its properties will be taken for handling this connection
- **Virtual Session Timeout** - (as well as the Other service session itself) are defined by the Security Gateway, and not by the protocol itself. It is therefore a "virtual" session. The virtual session timeout specifies the number of seconds until the session times out.

  Select the **Default** timeout, which is defined in **Global Properties** , or select **Specific** to override the default timeout.
- **Enable Aggressive Aging** - enables you to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.
- **Synchronize connections on cluster** - means that in a state-synchronized High Availability or Load Sharing gateway cluster, of the services allowed by the Rule Base, only those with **Synchronize connections on cluster** will be synchronized. By default, all new and existing services are synchronized.

Services Group

What can I do here?

Use this window to create a new group for services.

Getting Here - Object Explorer > New > Service > Services Group

Understanding Service Groups

What background information do I need to know?

A Services Objects group is a collection of services and protocols.

Groups are used in cases where you would like to apply the same definitions to a group of users. In addition, Groups are used in cases where you cannot work with single objects.

Groups can greatly facilitate and simplify network management. Groups let you to perform operations only once on the group, instead of repeating them for every service in the group.

Custom Application or Site - General

What can I do here?

Use this window to configure or edit the properties of a custom application/ site used in Application and URL Filtering or Threat Prevention.

Getting Here - Object Explorer > New > Custom Application/Site > Application/Site > General page

Creating Custom Applications and Sites

What background information do I need to know?

In the Application and URL Filtering Database, each application is assigned to one **primary category** based on its most defining aspect. See the category in the description of each application and in the logs.

In the Application and URL Filtering Database, each application can have **additional categories**, which are characteristics of the application. For example, some of the additional categories of Gmail include: Supports File Transfer, Sends mail, and Instant Chat. If an additional category is in a rule, the rule matches all applications that are marked with it.

Note - In the AppWiki, additional categories are called tags.

When you use the AppWiki or add applications to the Rule Base, you can filter by additional category or risk level to see all applications with that characteristic. This is a good way to get ideas of types of applications that you might want to block or allow.

If new applications are added to an additional category that is in an Application Control or URL Filtering rule, the rule is updated automatically when the database is updated.

Custom Application Options

Tell me about the fields...

- In the **General Properties** tab, you can change the details of the site or application.
- In the **URL List**, enter the URLs.
  - Do not include http/https prefixes
  - Select **URLS are defined as Regular Expression** to define more complex domain patterns, or for greater specificity.

    For example, if a news site has these links:

    https://www.news.com

    http://www.news.com

    To allow access only to the https link, use this regular expression:

    ^https:\/\/.\.news\.com*

    Note
    - Custom application/Sites do not apply until a URL or domain in the traffic payload matches those defined for the application/site. For example, the first packet of a connection will not match an application/site. For more, see sk106623
    - Some Regular Expressions may have performance impact on the Security Gateway. For more, see sk165094
    - The application or site URL defined by a regular expression must use the correct syntax

    Note: The application or site URL defined by a regular expression must use the correct syntax.
- In the **Additional Categories** tab, you can create more categories for the Application and URL Filtering or Threat Prevention Software Blade.

Using Regular Expressions in Custom Sites

Before using regular expressions in Custom sites, see: sk165094.

Custom Application or Site - Additional Categories

What can I do here?

Use this window to configure or edit the additional categories of a custom application/ site used in Application and URL Filtering or Threat Prevention.

Getting Here - Object Explorer > New > Custom Application/Site > Application/Site > Additional Categories page

Custom User Category

What can I do here?

In this window you can create a custom category to use in the Rule Base if there is no corresponding category. If category data in the Application and URL Filtering Database for a URL is not applicable for your organization, you can override the categorization.

Getting Here - Object Explorer > New > Custom Application/Site > User Category

Custom Applications/Site Group

What can I do here?

Use this window to see and change the properties of a group of custom applications or sites that you added to Application and URL Filtering .

Getting Here - Object Explorer > New > Custom Application/Site > Application/Site Group

Application Group Properties

You can create a group of applications or sites for use in the Rule Base. The group members can include categories, applications and widgets from the Application and URL Filtering Database and also custom applications, sites and categories.

Override Categorization for URL

What can I do here?

Use this window to manage the list of URLs for which you have overridden their initial categorization.

Getting Here - Object Explorer > New > Custom Application/Site > Override Categorization

Overriding Categorization

When the category data in the Application and URL Filtering Database for a URL is not applicable for your organization, use the override categorization option to update the category and risk definitions of a URL.

This definition overrides the information in the Application and URL Filtering Database and the responses received from the Check Point Online Web Service. The Rule Base will use the newly specified categorization when matching rules with URLs.

Overriding Categorization for a URL

To override categorization for a URL:

1. From the **Objects** tab of SmartConsole, select **New > More > Custom Application/Site > Override Categorization**.

   The **Override Categorization for URL** window opens.
2. Enter a **URL** in the field. You do not need to include the prefix `http:\\`.
3. If the URL contains a regular expression, select **URL is defined as a Regular Expression**.
4. Select a **Primary Category** from the list.
5. Select a **Risk** from the list.
6. To add **additional categories**, click **Add**+.
7. Select the categories. Click **OK**.

   The selected categories are shown in the **Additional Categories** list.
8. Click **OK**.

LDAP Group - New

What can I do here?

Use this window to set the properties of an LDAP Group.

Note - This is a user group whose members are defined on an LDAP directory server. An LDAP group can be used in the security policy in the same way as VPN user group.

Getting Here - Object Explorer > New > Users/Identities > LDAP Group

Understanding LDAP Groups

An LDAP group a user group whose members are defined in a LDAP directory server. An LDAP group can be used in the security policy in the same way as a VPN user group. The only difference between these groups is in the way you define users.

LDAP Group Options

Tell me about the fields...

General Settings

Specify the general attributes including:

Account Unit

Select the Account Unit (LDAP server) on which the users are defined from the drop-down list. The Account Units listed are defined in the **LDAP Account Unit Properties** window and are visible only if **Object Management** is checked in that window.

Groups Scope

There are three possible ways of defining a User Directory group, based on the users defined on the Account Unit:

- **All Account-Unit's Users**
- **Only Sub Tree ([optional prefix], branch)** - you must select a specific Account Unit branch from the drop-down list.
- **Only Group in Branch (DN prefix)** - you must select a specific group of the Account Unit.

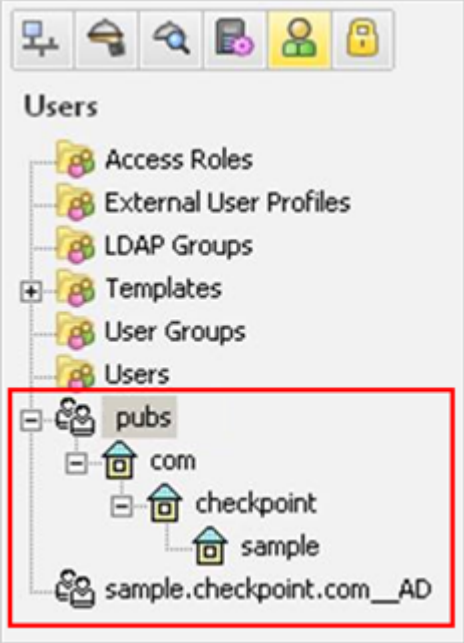
LDAP Filter

Apply filter for Dynamic Group

This field is used to filter LDAP users according to a user-defined filter and to create an LDAP users group.

Viewing the LDAP Tree

To view the LDAP tree, open the **Users** area of SmartDashboard.



IoT Discovery Service - General

What can I do here?

Use this window to configure the hostname, port, and pre-shared secret of the IoT Discovery Service.

Getting Here - Object Explorer > New > IoT Discovery Service> General tab

IoT Discovery Service - Gateways

What can I do here?

Use this window to select the IoT gateway.

To use IoT, you must enable the Identity Awareness blade and the Identity Aware API.

Select Identity Awareness to enable the blade and the API (Identity Web API) on the gateway.

Getting Here - Object Explorer > New > IoT Discovery Service > Gateways

IoT Discovery Service - Policies

What can I do here?

Use this window to select policy packages with an active IoT layer.

Getting Here - Object Explorer > New > IoT Discovery Service > Policies

IoT Discovery Service - Select Objects

What can I do here?

Use this window to select objects from the IoT Discovery Service.

Getting Here - Object Categories > IoT Controllers > Right-click IoT object > Import

Access Role - Networks

What can I do here?

Use this window to configure an access role and its networks.

Getting Here - Object Explorer > New > Users/Identities > Access Role > networks

Using Access Roles

What background information do I need to know?

Before creating access role objects, you must first activate Identity Awareness.

You can use Access Role objects as source and/or destination parameter in a rule. Access role objects can include one or more of these objects:

- Users and user groups
- Computers and computer groups
- Networks
- Remotes Access and VPN Clients

To enforce Identity Awareness, use these access role objects in the Rule Base.

Adding Access Roles

Important: Before you add Active Directory users, machines, or groups to an access role, make sure there is LDAP connectivity between the Security Management Server and the AD Server that holds the management directory. The management directory is defined on the **Objects Management** tab in the **Properties** window of the **LDAP Account Unit**.

To create an access role:

1. In the object tree, click **New> More > Users > Access Role**.

   The **New Access Role** window opens.
2. Enter a **Name** for the access role.
3. Enter a **Comment** (optional).
4. Select a **Color** for the object (optional).
5. In the **Networks** pane, select one of these:
   - **Any network**
   - **Specific networks** - For each network, click + and select the network from the list
6. In the **Users** pane, select one of these:
   - **Any user**
   - **All identified users** - includes any user identified by a supported authentication method (internal users, Active Directory users, or LDAP users).
   - **Specific users/groups** - For each user or user group, click + and select the user or the group from the list
7. In the **Machines** pane, select one of these:
   - **Any machine**
   - **All identified machines** - includes machines identified by a supported authentication method (Active Directory).
   - **Specific machines** - For each machine, click + and select the machine from the list
8. In the **Remote Access Clients** pane, select the clients for remote access.
9. Click **OK**.

Identity Awareness engine automatically recognizes changes to LDAP group membership and updates identity information, including access roles. For more, see the

R81.10 Identity Awareness Administration Guide

Access Role - Users

What can I do here?

Use this window to assign users or user groups to the access role.

Getting Here - Object Explorer > New > Users/Identities > Access Role > Users

Access Role - Users Options

In the **Users** tab, select one of these:

- **Any user**
- **All identified users** -Includes any user identified by a supported authentication method (internal users, Active Directory users or LDAP users).
- **Specific users/Groups** -A window opens. You can search for Active Directory entries or select them from the list.

Access Roles - Machines

What can I do here?

Use this window to assign machines or machine groups to an access role.

Getting Here - Object Explorer > New > Users/Identities > Access Role > Machines

Access Role - Options

In the **Machines** tab, select one of these:

- **Any machine**
- **All identified machines** - Includes machines identified by a supported authentication method (Active Directory).
- **Specific machines** -A window opens. You can search for Active Directory entries or select them from the list.

  Note - To add Active Directory users/machines/groups, the computer running SmartConsole must have LDAP connectivity to the AD server.
- **Enforce IP spoofing protection (requires full identity agent)** - Select this option to activate the packet tagging feature.

Access Role - Remote Access Clients

What can I do here?

Use this window to assign the access role to remote access clients.

	Getting Here - Object Explorer > New > Users/Identities > Access Role > Remote Access Clients

Access Roles for Remote Access

Create a rule in the Access Control Rule Base that handles remote access connections.

1. Go to **Security Policies** and right-click the cell in the VPN column.
2. Select **Specific VPN Communities**.
3. Choose the community and click +.
4. Close the VPN community window.
5. Define **Services & Applications** and **Actions** columns.
6. Install the policy.

Example:

To allow remote access users to access the organization's SMTP server, called SMTP_SRV, create the following rule:

Source	Destination	VPN	Service	Action	Track
Any	SMTP_SRV	Remote_Access_ Community	SMTP	Accept	Log

Remote Access Clients - Allowed Clients

What can I do here?

Use this window to select clients the access role settings will be enforced on when the client connects remotely.

	Getting Here - Object Explorer > New > Users > Access Role > Remote Access Clients > Allowed Client drop-down box > New/ Edit

Specific Remote Access Client

What can I do here?

Use this window to view any comments or tags associated with the specific Remote Access Client.

Getting Here - Object Explorer > New > Users > Access Role > Remote Access Clients > Specific Client drop-down box > New/ Edit > double click on allowed client.

User Group

What can I do here?

Use this window to create a group of users. The group can used in the rule base.

Getting Here - Object Explorer > New > Users/Identities > User Group

Identity Tag

What can I do here?

Use this window to create a new Identity Tag or edit an existing one.

Getting Here - Object Explorer > New > User/Identities > Identity Tag

Using Identity Tags in Access Role Matching

Identity Tags let you include external identifiers (such as Cisco® Security Group Tags, or any other groups provided by any Identity Source) in Access Role matching. These external identifiers act like a tag that can be assigned to a certain user, machine or group.

To use Identity Tags in Access Role matching:

1. Create a new Identity Tag:
    a. Click **Objects** menu > **More object types** > **User** > **Identity Tag**.
    b. Enter a name for the object.

    Note -If you enter the **External Identifier** first, the Identity Tag object gets the same name.

    c. In the **External Identifier** field, enter one of these:
        - A Cisco Security Group Tag, as defined on the Cisco ISE server or acquired through Identity Collector.
        - A custom tag (defined on a third party product) acquired through the Check Point Identity Web API.

    Note - The External Identifier must be a unique name.

    d. Click **OK**.
2. Include the Identity Tag in an Access Role:
    a. Click **Objects** menu > **More object types** > **User** > **New Access Role**.
    b. On the **Users** tab or **Machines** tab, select **Specific users/groups**.
    c. Click the **[+]** icon.
    d. Click on the domain name button in the top left corner and select **Identity Tags**.
    e. Select the Identity Tag created in Step 1.
    f. Click **OK**.
3. Add this Access Role to the **Source** or **Destination** column of an Access Control Policy rule.
4. Install the Access Control Policy.

User - General

What can I do here?

Use this window to create user accounts to use as network objects in Security Policies. On the General page, store the user's contact details, and set an expiration date on the account.

Getting Here - Object Explorer > New > User/Identities > User > Select Template > New User
Or:
Object Explorer Categories > Users > Users > Select User > New/Edit

User Objects

User objects set permissions, such as:

- The services users are allowed to use
- The locations from which users are allowed to access your network
- The network destinations to which users are allowed to connect
- The time frame during which users are allowed to access your network
- How users are authenticated
- How users can work remotely

User - Groups

What can I do here?

Use this window to add users to user groups.

Getting Here - Object Explorer > New > User /Identities> User > Select Template > New User > Groups

User - Group in User Template

What can I do here?

When creating a user template, use this window to add users to user groups.

Getting Here - Object Explorer > New > User/Identities > User > User Template > Groups

User - Authentication

What can I do here?

Use this window to set an authentication method for the user.

Getting Here - Object Explorer Categories > Users/Identities > Users > Select User > Edit > Authentication

User Authentication Options

Select the scheme to be used to authenticate users defined with this template. These schemes are used in authentication rules and in Remote Access (when the user is not identified using a certificate or an IKE preshared secret).

Select one of these authentication methods:

- **Undefined** - means that *either* no authentication is performed and access is always denied, *or* IKE authentication is used, as defined in the **Encryption** tab.

  If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.

- **SecurID** - means that users are challenged to enter the number displayed on the Security Dynamics SecurID card. There are no scheme-specific parameters for this authentication scheme. The Security Gateway acts as an ACE/Agent 5.0.

  SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the RSA AM.

  Using SecurID, the Security Gateway forwards authentication requests by remote users to the AM. The AM manages the database of RSA users and their assigned hard or soft tokens. The gateway acts as an AM Agent and directs all access requests to the RSA AM for authentication. For additional information on agent configuration, refer to RSA Authentication Manager documentation.

  There are no specific parameters required for the SecurID authentication scheme.

- **Check Point Password** - means that users are challenged to enter the internal Check Point password on the gateway.

  The Security Gateway stores a static password in the local user database of each user configured in Security Management Server.

- **OS Password** - means that users are challenged to enter their Operating System password for the Security Management Server. There are no scheme-specific parameters for this authentication scheme.

The Security Gateway can authenticate using the user name and password that is stored on the operating system of the machine on which the Security Gateway is installed. You can also use passwords that are stored in a Windows domain.

- **RADIUS** - means that users are challenged for the response, as defined by the RADIUS server. Select the RADIUS server object here.

  Remote Authentication Dial-In User Service (RADIUS) is an external authentication scheme that provides security and scalability by separating the authentication function from the access server.

  Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users.

  The RADIUS protocol uses UDP to communicate with the gateway. RADIUS servers and RADIUS server group objects are defined in SmartConsole.

- **TACACS** - means that users are challenged for the response, as defined by the TACACS or TACACS+ server. Select the server object here.

  Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

  TACACS is an external authentication scheme that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

User - Location

What can I do here?

Use this window to configure the network objects from which , and to which, the user has access.

Getting Here - Object Explorer Categories > Users/Identities > Users > Select User > Edit > Location

User - Time

What can I do here?

Use this window to set the days and times during which the user is allowed access.

Getting Here - Object Explorer Categories > Users/Identities > Users > Select User > Edit > Time

User - Certificates

What can I do here?

Use this window to create, edit and cancel user certificates.

Getting Here - Object Explorer Categories > Users/Identities > Users > Select User > Edit > Certificates

Managing Certificates

Check Point VPN lets you define many certificates for each user. This lets users connect from different devices without the necessity to copy or move certificates from one device to another. Users can also connect from different devices at the same time.

There are two basic procedures for creating and authenticating using remote access VPN certificates:

Sending a P12 File:

- The administrator creates a p12 certificate file and sends it to users.
- The user saves the p12 file on the device and specifies the certificate using a remote VPN Client.
- Users authenticate by entering a certificate password when starting a remote access VPN connection.

Using a Registration key:

- The administrator creates a registration key and sends it to the user.
- The user enrolls the certificate by entering the registration key in a Remote Access VPN client. The user can optionally save the p12 file to the device. The user must do this in an administrator-defined period of time.

- End users authenticate using this certificate. A password can also be required according to the security policy settings. If the user saves the p12 file to the device, a password is always necessary.

Tell me about the fields...

- **Show box** - Show all certificates or only active certificates. Active certificate are valid for enrollment and for renewed certificates. Renewed certificates are automatically revoked one week after renewal.
- **New** - Create a new certificate.
- **Edit** - Change an existing certificate.
- **Revoke** - Cancel an existing certificate.

Certificate Options

- **Show box** - Show all certificates or only active certificates. Active certificate are valid for enrollment and for renewed certificates. Renewed certificates are automatically revoked one week after renewal.
- **New** - Create a new certificate.
- **Edit** - Change an existing certificate.
- **Revoke** - Cancel an existing certificate.

User - Registration Key for Certificate Enrollment

What can I do here?

Use this window to generate, save, initiate, or revoke certificates.

Getting Here - Object Explorer Categories > Users/Identities > Users > Select User > Edit > Certificates > Click New icon > Registration key for certificate enrollment

Using Registration Keys

- The administrator creates a registration key and sends it to the user.
- The user enrolls the certificate by entering the registration key in a Remote Access VPN client. The user can optionally save the p12 file to the device. The user must do this in an administrator-defined period of time.

- End users authenticate using this certificate. A password can also be required according to the security policy settings. If the user saves the p12 file to the device, a password is always necessary.

Tell me about the fields...

- **Send this registration key to the user** - Automatically generated registration key to send to the user.
- **Send** - Click to send the registration key to the user by email.
- **Template** - Opens the Email Template window. Enter or change the text of the email containing the registration key email.

Registration Key Fields

- **Send this registration key to the user** - Automatically generated registration key to send to the user.
- **Send** - Click to send the registration key to the user by email.
- **Template** - Opens the Email Template window. Enter or change the text of the email containing the registration key email.
- **User must enroll within** - sets a time limit for enrollment.

User - Email Template

What can I do here?

Use this window to change the default email message sent to the user with the registration key.

> **Getting Here** - Object Explorer Categories > Users > Users/Identities > Select User > Edit > Certificates > New > Registration key for Certificate enrollment > Template

User - Certificate File (P12)

What can I do here?

Use this window to configure the certificate password. When you click **OK**, the system creates the certificate and prompts you for a path to save the p12 file.

Note - Deliver the certificate and P12 password to the user in a secure way.

> **Getting Here** - Object Explorer Categories > Users/Identities > Users > Select User > Edit > Certificates > New > Certificate file (P12)

Sending a P12 File

- The administrator creates a p12 certificate file and sends it to users.
- The user saves the p12 file on the device and specifies the certificate using a remote VPN Client.
- Users authenticate by entering a certificate password when starting a remote access VPN connection.

Certificate File (P12) - View Details

What can I do here?

Use this window to view the certificate details.

Getting Here - Object Explorer Categories > Users/Identities > Users > Select User > Edit > Certificates > Select certificate > Edit > View certificate details

User - Encryption

What can I do here?

Use this window to enable Internet Key Exchange (IKE).

IKE is a protocol used to establish security attributes (such as a cryptographic algorithm) shared between two network entities. The shared attributes facilitate secure communication.

Getting Here - Object Explorer Categories > Users/Identities > Users > New/Edit >Encryption

User - IKE Phase2 Properties - Authentication

What can I do here?

Use this window to select an authentication scheme -- password or public key -- for remote connections.

Getting Here - Security Policies > Object Categories > Users/Identities > Users > New/edit > Encryption > Select IKE > Edit > Authentication

Understanding IKE Phase2 Authentication

Remote users need to authenticate to the Security Gateway. This can be achieved through preshared secrets (where both sides know the same password) or certificates (where a trusted third party vouches for the identity of client and gateway).

IKE Phase2 Authentication Options

- **Password (Pre-shared secret)** - the user authenticates using a password (pre-shared secret).
- **Public Key** - the user authenticates using a public key contained in a certificate (PKI).

User - IKE Phase2 Properties - Encryption

What can I do here?

Use this window to select methods for encryption and data integrity.

Getting Here - Security Policies > Object Categories > Users/Identities > Users > New/edit > Encryption > Select IKE > Edit > Encryption

Understanding IKE Phase2 Encryption

The encryption properties are defined for all users in **SmartConsole > Global Properties > Remote Access > VPN - Authentication > section Encryption algorithms**.

Encryption ensures the data remains exclusive to the communicating parties.

Data Integrity methods ensure that the data has not been altered during transit.

IKE Phase2 Encryption Options

- **Encryption Algorithm** - selects one of the algorithms from the drop-down list.
- **Data Integrity** - selects the cryptographic checksum method to be used for ensuring data integrity.

RADIUS Group

What can I do here?

Use this window to create or edit a RADIUS Server Group.

Getting Here - Object Explorer > New > Server > More > RADIUS Group

RADIUS Server Group Options

A RADIUS server group is a High Availability group of identical RADIUS servers which includes any or all the RADIUS servers in the system. A RADIUS (Remote Authentication Dial-In User Service) server is used for user authentication. Check Point uses the RADIUS servers for:

- User Authentication (via Authentication Rules)
- Administrator authentication when administrators log in to SmartConsole
- SecuRemote Users (via IKE Hybrid Mode)

If the server with the highest priority fails, the one with the next highest priority in the group takes over. Set priority by editing the properties of the RADIUS server.

Note - When defining a group of RADIUS servers, all members of the group must use the same protocol.

RADIUS Server - General Properties

What can I do here?

Use this window to create or edit the General properties of a RADIUS server. This network object lets users with RADIUS credentials authenticate to a Security Gateway.

Getting Here - Object Explorer > New > Server > More > New RADIUS > General

Understanding RADIUS Servers

RADIUS (Remote Authentication Dial-In User Service) server is used for authentication of users. Check Point uses the RADIUS servers in these scenarios:

- Administrators logging in to SmartConsole
- SecuRemote Users (via IKE Hybrid Mode)

RADIUS Configuration Fields

- **Host** is where the RADIUS server is deployed.
- **Service** is the port to which the RADIUS server listens. Choose one of two predefined services.
  - **RADIUS** is port number historically used by most installations.
  - **NEW-RADIUS** is the officially registered port number.
- **Shared secret** is the secret between the RADIUS server and the Security Gateway.

- **Version** can be either RADIUS Version 1.0, which is RFC 2138 compliant, and RADIUS Version 2.0 which is RFC 2865 compliant. For more, see:
  - RFC 2138
  - RFC 2865
- **Protocol** is the type of authentication protocol that will be used when authenticating the user to the RADIUS server. This type should be supported and enabled by the server. The MS-CHAP v2 protocol is supported by some servers, including Microsoft IAS and Cisco ACS. This protocol provides higher security and the ability to perform a password change, as an additional challenge in the authentication session, when the user is configured as "User must change password at next logon" on the server.

  Note - When defining a group of RADIUS server objects in Security Management, all members of the group must use the same protocol.
- **Priority** applies when there is more than one RADIUS server in the system. In that case, the order in which the servers are contacted is set by their defined priority number. The lower the number the higher the priority.

RADIUS Server - Accounting

What can I do here?

Use this window to configure the RADIUS server to allocate IP addresses.

Getting Here - Object Explorer > New > Server > More > RADIUS > Accounting

IP Pool Management

IP Pool management makes it possible for a Security Gateway to authenticate RADIUS-defined users, and use the RAS IP pools on the RADIUS server. The RADIUS server is configured to assign an IP address to successfully authenticated users from the internal pool.

- You can use a default RADIUS server for all RADIUS authentications, overriding the specific configuration of a RADIUS server. This may be important when configuring the system to work with one pool.
- Configure the RADIUS server to the correct authentication port as well as the relevant service for RADIUS accounting.
- When a user connects to the Security Gateway, the gateway verifies the user credentials. The RADIUS server then locks the IP assignment associated with this authentication.
- When the user logs out, the RADIUS server releases the lock on the assigned IP address.

Note - Do not use a group of RADIUS servers (for high availability) since it will not be clear from which pool the IP was assigned from. Instead, for high availability, use solutions from the RADIUS server vendor that can synchronize all IP pool information between the servers.

RADIUS IP Pool Management fields

- **Enable IP Pool Management** means that IP addresses will be assigned. The RADIUS server assigns IP addresses to RADIUS-defined users who have successfully authenticated. When the users log out, the Security Gateway notifies the RADIUS server, which returns the IP address to the RADIUS IP pool.

  The Gateways & Servers will use this accounting interface to notify the server when users login and logout.
- **Service** is the port that the RADIUS server uses to communicate with clients.

SecuRemote DNS Server - General

What can I do here?

Use this window to set up a SecuRemote DNS server that maintains a list of resolvable domain names. Specify on which host the SecuRemote DNS server resides.

Getting Here - Object Explorer > New > Server > More > New SecuRemote DNS

Understanding SecuRemote

To enable SecuRemote/SecureClient to resolve IP addresses to Domain names, define a DNS server for remote clients in the Remote access community.

In the **Host** drop down box, select the DNS server for remote access clients.

SecuRemote DNS Server - Domains

What can I do here?

Use this window to configure patterns that match resolvable domain names.

Getting Here - Object Explorer > New > Server > More > New SecuRemote DNS > Domains

SecuRemote DNS Server -- add Domain Patterns

What can I do here?

Use this window to define a domain suffix and select matching criteria. You can match the complete DNS suffix, or a number of labels preceding the suffix.

Getting Here - Object Explorer > New > Server > More > New SecuRemote DNS > Domains > Add

TACACS Server

What can I do here?

Use this window to create or edit a TACACS server so that users with TACACS credentials can authenticate to a Security Gateway.

Getting Here - Object Explorer > New > Server > More > New TACACS

Understanding TACACS

A TACACS (Terminal Access Controller Access Control System) server is used for user authentication.

TACAC Configuration Fields

- **Host** is where the TACACS server is deployed.
- **Server Type** -TACACS+ provides several enhancements to the original TACACS protocol. TACACS+ uses TCP instead of UDP, and separates the authentication, authorization and accounting functions.
  - VPN interfaces only with the authentication aspects of TACACS+
  - Authorization and accounting features are not used
- **Secret Key** can be defined on a TACACS+ server, and is used for communication between the TACACS server and its clients (the Check Point Security Gateway).
- **Service** is the port to which the TACACS server listens. Use the TACACS or TACACSplus service, as appropriate.
- **Priority** applies when there is more than one TACACS server in the system. The order in which the servers are contacted is set by the priority number. The lower the number the higher the priority.

Note - The priority field is mandatory if the TACACS server is a member of a group of TACACS servers

TACACS Group

What can I do here?

Use this window to create a TACACS server group.

What Information do I need to know?

A TACACS (Terminal Access Controller Access Control System) server is used for user authentication.

TACACS servers which are a member of a TACACS group must have a priority set.

Priority applies when there is more than one TACACS server in the system. The order in which the servers are contacted is set by the priority number. The lower the number the higher the priority.

Getting Here - Object Explorer > New > Server > More > New TACACS Group

UFP Group

What can I do here?

Use this window to create or edit a UFP Group, and set the load sharing method.

Getting Here - Object Explorer > New > Server > OPSEC Application > UFP Group

UFP Group Options

Load Sharing occurs when identical UFP servers share the load to increase efficiency. When defining a UFP server, chaining is not available.

CPMI Group

What can I do here?

Use this window to create groups that have permission to install policies on a specified gateway.

Getting Here - Object Explorer > New > Server > OPSEC Application > CPMI Group

Check Point Management Interface

1. Create a group that has permission to install polices on a specified gateway
2. On the specified gateway, open **Gateway Properties > Other > Permissions to Install** and select the group.

New Identity Provider

What can I do here?

Use this window to configure data required and received from the SAML Identity Provider.

Getting Here - Object Explorer > New > User/Identity > Identity Provider

For more information about SAML configuration, see:

- *R81.10 Security Management Administration Guide*
- *R81.10 Identity Awareness Administration Guide*
- *R81.10 Mobile Access Administration Guide*

New Azure AD

What can I do here?

Use this window to create a new Azure AD object.

Getting Here - Object Explorer > New > User/Identity > Azure AD

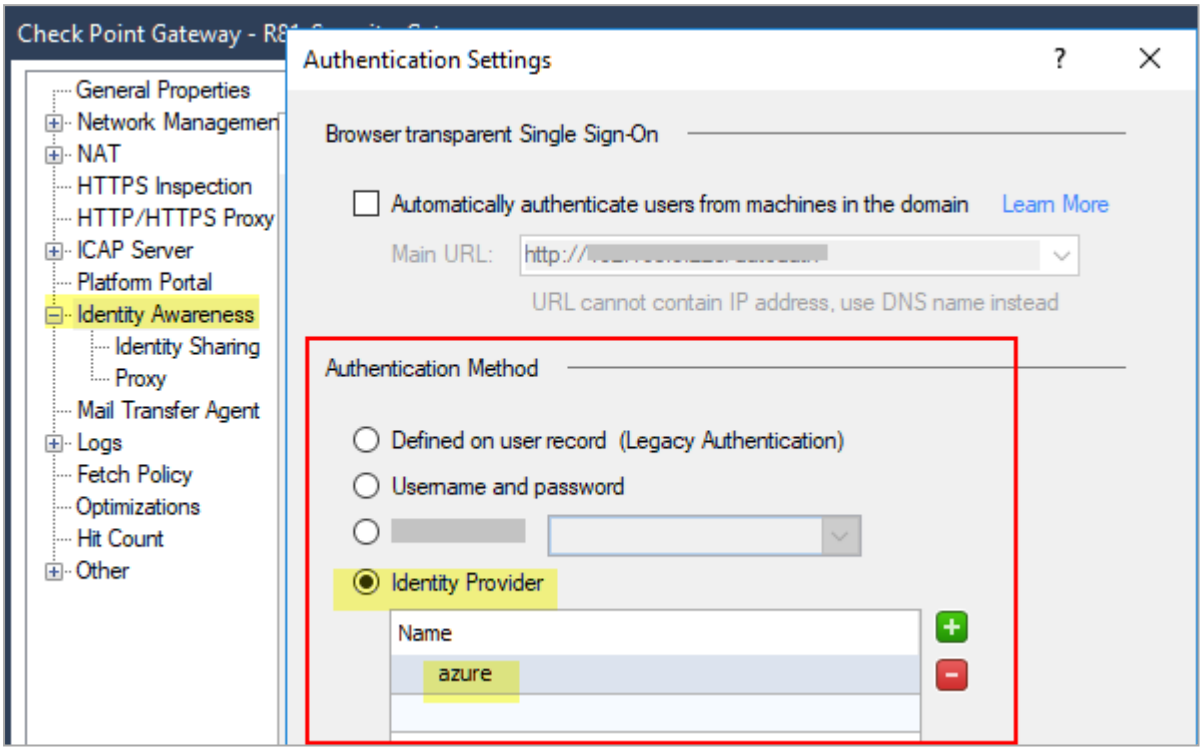
Using Azure AD for Authorization

Azure Active Directory (Azure AD) is a Microsoft cloud-based identity and access management service that offers identity and access capabilities for applications that run in Microsoft Azure and for applications that run in an on-premises environment.

Best Practice:

- If you use Azure both for authentication and authorization, then Azure AD performs the authentication phase through the SAML protocol with SAML Identity Provider.
- If you use Azure for authorization only you can use any authentication method.

Example:



For more, see the *R81.10 Identity Awareness Administration Guide*.

URI - General

What can I do here?

Use this window to create or edit the properties of a URI resource.

Getting Here - Object Explorer > New > Resource > URI > General

Understanding URI Resources

Resources are used to match content that you are looking for, and to run an action on the content.

To specify the content, wildcards and regular expressions can be used.

The Resource is triggered when a Rule includes the Resource, and a packet matches the rule. A Resource is applied per Service.

URI Options

Tell me about the Fields

Use this resource to :

- **Enforce URI Capabilities** - This option diverts the connection to the HTTP security server, and enables all the functionality and parameters of the URI resource, such as schemes, hosts, paths and methods and CVP checking.
- **Optimize URL logging** - Generates extra URL logging information by performing kernel inspection on the HTTP connection, and shows the full path of the requested URL, not just the name of the web server. If selected, fields and tabs of the URI Resource that relate to the security server are disabled.
- **Enhance UFP Performance** - Improves UFP performance by not using the security server. The cost of this improved performance is that UFP caching, CVP checking and authentication cannot be used with this mode, and certain HTTP Header verifications, such as methods and length are not performed.

Connection Methods - configure when this Resource applies.

- **Transparent** - means that the security server is invisible to the client that originates the connection, and to the server. The Transparent connection method is the most secure.
- **Proxy** - means that this Resource is applied when people specify the Check Point Security Gateway as a proxy in their browser. If clients use the Security Gateway as a proxy, connections will leave the gateway with the Security Gateway as the source IP address. No NAT will take place to the IP address of the original client.
- **Tunneling** (**visitor mode**) - means that this Resource is applied when people specify the Security Gateway as a proxy in their browser, and is used for connections where Security Gateway cannot examine the contents of the packets, not even the URL. Only the host name and port number are checked. Tunneling Connection are HTTP connections that use the CONNECT method. An example of this is HTTPS (an SSL encrypted HTTP connection). If Tunneling is specified, all Content Security options of the URI Resource are disabled. The Tunneling connection method is not allowed by default because of the security implications. Avoid creating a Resource that allows only tunneling. It is preferable to define a rule that opens the port used by the visitor mode connections.

URI Match Specification Type - The type can be **Wild Cards** or **UFP,** where a UFP server holds categories of forbidden web sites. For details of the match specification of each, see the **Match** tab.

Exception Track - Configures how to track connections that match this rule but fail the content security checks. An example of an exception is a connection with an unsupported scheme or method.

URI - Match (Wildcards)

What can I do here?

Use this window to configure how a connection is matched to a Resource in a rule. If a connection matches the source and destination of the rule and the match parameters of the Resource, then both the **Action** in the Rule and the **Action** in the Resource are applied.

Getting Here - Object Explorer > New > Resource > URI > General > URI match specification type: Wildcards > Match - Wildcards page shows

URI Wildcards Options

Schemes

- Select the URI **Schemes** to which this resource applies. It is only relevant when the Security Gateway is defined as a proxy for these protocols in the browser of the clients initiating the connection.
- You can specify another scheme in the **Other** field. You can use wildcards. If you use *, all schemes are allowed -including the schemes that are not selected.

Methods

- The **GET** method is used when you request a particular page (or elements on a page). It retrieves whatever information (in the form of an entity) is identified by the URI. It. If the URI refers to a data-producing process, it is the produced data, which is returned as the entity in the response and not the source text of the process, unless that text happens to be the output of the process.
- The **POST** method is used when sending data to a web site (filling out forms, for example). The actual function performed by the POST method is determined by the server and is usually dependent on the URI.
- The **HEAD** method is identical to GET except that the server does not return any Entity-Body in the response. It is usually used by caching servers and web browsers to determine whether or not an element has changed, in order to decide whether or not to download the element. It is also used for testing hypertext links for validity and accessibility.
- The **PUT** method is a less commonly used method for uploading files via HTTP (ftp using a browser).

  You can specify another method in the **Other** field. You can use wildcards. If you specify *, all methods are allowed, including the methods that are not selected.

Methods

The **Host**, **Path**and **Query** parameters break the URI into filterable components. For example

- **Host:**http://www.elvis.com - The functionality of the **Host** parameter depends on the DNS setup of the addressed server. For the host, only the IP address or the full DNS name should be used, (For example: 191.81.23.* or server.{paris,london}.com, but not {paris,london}). For expressions using a host name and port number, the port number must be explicitly specified, for example, the expression paris* matches requests on any port. It is recommended to restrict requests to a known HTTP server (for example, *.paris:80, or paris:80).
- **Path:**/alive/qc.html - For the **Path** , name matching is based on appending the file name in the request to the current working directory (unless the file name is already a full path name) and comparing the result to the path specified in the Resource definition.

  The file path name must include the directory separator character "/". For example, the request "/myfile" is matched to "/<current directory>/myfile". If the Resource path name specifies only "myfile", then the request will not be matched.

  When using wildcard characters for the Path, you must specify either the full path name, or use the directory separator in the wildcard expression. For example, the path name "*/myfile" will match "myfile" in all possible directories.

  Path includes the file name (which can include wildcard characters). For example: "/boys/fred/*" includes all the files in the /boys/fred/ directory, and "/boys/fred/" does not include any of the files in the /boys/fred/ directory. If /boys/fred were a file, it would be included in "/boys/fred/".
- **Query** - are the parameters that are sent to the URI when it is accessed.

URI - Match (UFP)

What can I do here?

Use this window to configure the UFP properties of the URI Resource.

Getting Here - Object Explorer > New > Resource > URI > General > Set URI match specification type to: UFP > "Match - UFP" page shows

UFP Servers

UFP servers are OPSEC certified third party applications that check URLs against a list of permitted categories to determine whether or not access to that URL should be allowed.

When a user requests a URL, the Security Gateway determines if the UFP server must be used. If a UFP server is used, the connection is held until the Firewall determines if the connection is permitted.

This window specifies how a connection is matched to the Resource in a rule. If a connection matches the source and destination of the rule and the match parameters of the Resource, then both the Action in the Rule and the Action in the Resource are applied.

UFP Options

- **General**
  - **UFP server** - Select the server on which the UFP application is installed. The UFP server should already be defined as an OPSEC Application.
  - **UFP caching control** - Specifies if and how caching is to be enabled.

Caching Control	Description
UFP Server	The UFP server controls UFP caching. With this option the server will cache a URL and mask sent by the UFP server in a cache_info format.
Security Gateway (one request)	UFP caching is controlled by the gateway. This option disables the second, IP-based UFP request, increasing performance. With this option the security server caches the UFP server's reply to a CAT (category) request.
Security Gateway (two requests)	UFP caching is controlled by the gateway, and enables the second, IP-based UFP request, thereby increasing cache integrity. With this option the security server sends a second CAT (category) request with the IP address acting as the URL address, after receiving a reply from the first CAT request.
No caching	UFP caching disabled.

- **Categories** - add categories to include in the resource definition.
- **Other**
  - **Ignore UFP server after connection failure** - means that the UFP server will be ignored after numerous UFP server connections were unsuccessful. The UFP server is ignored for a specific period of time, during which the rules in the Rule Base take over for the UFP server. At the end of the specified period of time the connection is attempted again.
  - **Number of failures before ignoring the UFP server** - signifies at what point the UFP server should be ignored.
  - **Timeout before reconnect to UFP server** - the amount of time that must pass before a UFP server connection should be attempted.

URI - Action

What can I do here?

Use this window to configure an action to take when the resource matches a rule.

Getting Here - Object Explorer > New > Resource > URI > Action

URI Action Options

- **Methods** - If the Action in a rule which uses this resource is Drop or Reject, then the **Replacement URI** is displayed instead of the one requested by the user.
- **HTML Weeding** - Use **HTML Weeding** to strip JAVA applets, JAVA scripts, ActiveX tags, FTP links and port strings from HTML code. The problematic HTML is not deleted, but comments are added so that it has no effect. The user may not notice that the page has been altered.
- **Response Scanning**
- **Strip script tags** - removes JAVA code from incoming HTTP. JAVA scripts are removed using HTML Weeding. The user sees a message indicating either that the applet cannot start (when the JAVA code is incorporated in an HTML document), or that the document contains no data (if the JAVA code is directly fetched).

URI - Content Vectoring Protocol (CVP)

What can I do here?

Use this window to configure CVP inspection on HTTP messages. Many CVP servers can inspect the request and response in HTTP connections, and the HTTP headers in message packets.

Getting Here - Object Explorer > New > Resource > URI > CVP

CVP Options

Tell me about the fields

- **Use CVP** to enable CVP - select the **CVP server**from the drop-down menu. The CVP server should already be defined as an OPSEC Application.

- **CVP Server is allowed to modify content** - if the designated CVP server can inspect and repair the message string. CVP servers cannot modify binary files, so if the resource matches on *.exe, you may want to prevent the CVP server modifying it, and just drop it. If you choose not to allow the CVP server to modify content, and the CVP server finds a problem (such as a virus), the message will not be allowed.
- **Send HTTP Headers to CVP server** - select, if you would like the CVP server to check the HTTP headers of the message packets
- **Send HTTP requests to CVP server** - to protect against undesirable content in the HTTP request, for example, when inspecting peer-to-peer connections.
- **Send only unsafe file types to CVP server** - improves the performance of the CVP server. This option does not send to the CVP server traffic that is considered safe. Check Point Security Gateway considers files that are not executable to be safe, because they do not normally contain viruses. Picture and video files are considered safe.

  The Check Point Security Gateway security server identifies safe content by actually examining the contents of the packet. It does not rely on examining the URL (for file extensions such as *.GIF) nor does it rely on checking the MIME type (such as image/gif) in the server response.
- **Reply Order** - designates when the CVP server returns data to the Security Gateway security server.

  The CVP server checks the file one packet at a time. After the CVP server has inspected the whole file, it sends a Validation Result message to the security server. If the Validation Result is that the file is approved, the security server sends the file back to the Inspection gateway, which sends the file on to the client.
- **Return data after content is approved** - the CVP server sends the file back security server after checking the whole file.
- **Return data before content is approved** - the CVP server sends packets to the security server as soon as it checks them. **Return data before content is approved** gives better response times to users, but may mean that the CVP server sends virus infected files to the security server.

URI - SOAP

What can I do here?

Use this window to configure how the Security Gateway inspects and tracks SOAP requests.

Getting Here - Object Explorer > New > Resource > URI > General > Set URI match inspection type to: wildcards > "SOAP" page shows

Simple Object Access Protocol

SOAP is a communication protocol for accessing web services and sending messages (in XML format) between applications.

The Check Point gateway uses a security server to prevent potential attacks by verifying that the HTTP, XML, SOAP methods in SOAP requests conform to the RFC. The Gateway also makes sure that only a predefined list of acceptable methods is being passed in the SOAP packet.

When the gateway detects SOAP packets, it can accept them or accept only the Methods specified in a predefined file.

The SOAP processing defined in the URI resource is performed only if the HTTP connection carrying the SOAP message is Accepted by the rule in which the URI resource is used. The connection must match the rule, and the rule Action cannot be Reject or Drop.

SOAP Options

To define how the Check Point Security Gateway inspects SOAP requests, in the URI Resource **Match Wildcards** window, select **HTTP** in the **Schemes** section.

In the SOAP window, **Allow all SOAP Requests**, or **Allow only SOAP requests specified in the following File**, and select the file.

Defining the Allowed SOAP Methods file

The name of the SOAP file must be one of a predefined list of 10 files, from scheme1 to scheme10. The file must reside in **$FWDIR/conf/XML/** directory in the Security Management Server. If Management High Availability is used, the same file should be duplicated on both Security Management Servers.

The file must contain a two column list separated by a space:

```
namespace method
```

For example...

```
http://tempuri.org/message/ EchoString
http://tempuri.org/message/ SubtractNumbers
```

The file must be defined very precisely. It is best to copy and paste the namespace and method name from the log file. If there is a syntax error, the SOAP packets will be dropped.

URI for QoS

What can I do here?

Use this window to set the URI properties for the QoS resource.

A security policy lets you allocate bandwidth resources to specific types of traffic. You can define bandwidth rules for TCP and UDP based traffic.

Use a URI for QoS Resource to search for a URL string that will be matched to an HTTP connection, and then use the URI for QoS Resource in a QoS rule.

Getting Here - Object Explorer > New > Resource > URI for QoS

URI for QoS Options

In the **Search for URL field** , describe the URL string using wildcards or a regular expression. The URL string must be either the name of a site with a wildcard, for example, **www.checkpoint.com/*** , or a specific file name such as *.gif, which is any gif from any site.

SMTP - General

What can I do here?

Use this window to create or edit an SMTP resource.

Getting Here - Object Explorer > New > Resource > SMTP > General

Understanding URI Resources

Resources are used to match content that you are looking for, and to run an action on the content.

To specify the content, wildcards and regular expressions can be used.

The Resource is triggered when a Rule includes the Resource, and a packet matches the rule. A Resource is applied per Service.

SMTP Options

Tell me about the fields

In both the **Mail Delivery** section, and the **Error Mail Delivery** sections, specify the **server**to which mail is forwarded. Error mail delivery happens if the SMTP security server is unable to deliver the message within the abandon time, and **Notify Sender on Error** is checked.

If the **server** fields are empty, mail is forwarded to the server specified under **default_server** in **$FWDIR/conf/smtp.conf** . If this too is empty, then mail is forwarded to the server specified in the original mail message. If multiple servers are defined, they are tried one after the other until successful. To specify multiple mail servers, use the format **{errormailserver1, errormailserver2, ...}** . For more detailed information, see Using Regular Expressions and Wildcards in Resources.

An MX (Mail eXchange) query is a kind of DNS resolving. The Security Gateway receives the name of a recipient (for example: fred@example.com) and asks the DNS server to resolves its MX and DNS domains, and the DNS returns the IP address. Firewall also maintain a cache to make the DNS lookup more efficient.

This is a kind of a proxy mode for SMTP, and it enables the SMTP security server to be the last among the SMTP entities handling the mail for outbound traffic. If a mail file has recipients in more than one domain, the Security Gateway will split the original message by domain.

In the **Mail Delivery** section, if **Deliver messages using DNS/MX records** is selected, MX record resolving is used to set the *destination* IP address of the connection.

In the **Error Mail Delivery** section, if **Deliver messages using DNS/MX records** is selected, MX record resolving will be used to set the *source* IP address of the connection used to send the error message. Messages are sent after the IP address is resolved.

All the resource actions, such as header rewriting and CVP, are decided according to the last rule matched. The new resolved IP address will be fetched from the MX record resolving or from the server IP address.

For mail delivery within the organization using an SMTP security server, it is recommended to use a static mail server configuration. do this by configuring **Mail Deliver Server** or **Error Mail Delivery Server** in the SMTP Resource, and unchecking the MX resolving option.

If **Check Rule Base with new destination** or **Check Rule Base with new error destination** are selected, the Rule Base will be rechecked with the new resolved IP address for mail or error mail delivery.

For example, if a user sends an email to fred@example.com, and the original connection is from Client_A to Outgoing_Mail_Server_B. The SMTP security server intercepts the email and the resource specifies **Deliver messages using DNS/MX record** and **Check Rule Base with new destination**. The SMTP security server asks the DNS server to resolve fred@example.com. The DNS server returns the IP address of Example mail server that is different to the original destination (Outgoing_Mail_Server_B). If **Check Rule Base with new destination**is checked, the Rule Base is rechecked to see if there is another rule that can match this mail - maybe sent Example emails should be Encrypted rather than Accepted.

Exception Track determines if an action specified in the **Action 2** and **CVP** tabs taken as a result of a resource definition is logged. For example, if the user attempts to send a message that is too large, the tracking specified here is performed. The **Rewriting Rules** defined in the **Acion1** tab are logged by setting the **Track** column in the Rule Base. This makes it possible for example to log mails that have been changed in **Action2** or had viruses (**CVP**), while not logging Rewriting Rules.

SMTP - Match

What can I do here?

Use this window to set the Match properties for the SMTP resource.

Sender and Recipient can be matched with wildcards and Regular expressions.

Getting Here - Object Explorer > New > Resource > SMTP > Match

SMTP - Action 1

What can I do here?

Use the **Rewriting Rules** to rewrite **Sender** and **Recipient** headers in emails.

The left field is a match field for the original header. The right field is for the rewritten header.

You can also rewrite other email headers:

- **Field** - the name of the header
- **Contents** - the name of the original field and the replacement field.

You can use wildcards and regular expressions to specify and rewrite the **Sender** and **Recipient** headers, and the **Field** and **Contents** headers.

Getting Here - Object Explorer > New > Resource > SMTP > Action 1

SMTP - Action 2

What can I do here?

Use this window to configure mail inspection for the SMTP Resource.

Getting Here - Object Explorer > New > Resource > SMTP > Action 2

SMTP - Action 2 Options

- **Attachment handling**
  - **Strip MIME of type** - specifies the MIME type to strip from the message. Allowed types are defined in RFC 1521. The **message/partial** type allows multi-part messages, which are a security risk. If you configured CVP or you configured weeding or stripping in the resource, and did not specify **message/partial**, SmartConsole asks if you want to strip it.
  - **Strip file by name** - strips file attachments of the specified name from the message. This field enables the user to strip UU-ENCODE and MIME file attachments whose names match any of the defined expressions. Consider the three expressions: **{+love*, *.pic, a*.+}** . In the following examples, the defined file attachments will be stripped:

Expression	**+love***	***.pic**	**a*.+**
For Example:	**IloveYou!, XloveY**	**a.pic, abc.pic**	**ab.2, a.1, aa.1**

- **Mail Capacity**
  - **Do Not send mail larger than** - Restrict the size of incoming email attachments. This setting does not apply to the processed (after encoding and stripping) email attachments.
- **Allowed Characters** - The MIME email headers can consist of 8 or 7 bit characters (7 ASCII and 8 for sending Binary characters) in order to encode mail data. For example, "Content-Transferring-Encoding: 7bit". The firewall provides the administrator with the ability to block 8 character bits.
- **Weeding** - Use Weeding to strip JAVA applets, JAVA scripts, ActiveX tags, FTP links and ports strings from the HTML code in the email messages. The problematic HTML is not deleted, but comments are added so that it has no effect.

SMTP - CVP

What can I do here?

Use this window to configure CVP inspection on mail messages.

 **Getting Here** - Object Explorer > New > Resource > SMTP > CVP

SMTP and CVP

In SMTP, the client sends a request to the server asking to send or receive an email. The email itself passes in the response, so the CVP server always performs checks on the response. The connection request/response process is:

1. Client to server (request)
2. Server to CVP (response)
3. CVP to Client (response)

SMPT - CVP Options

- **Use CVP** - Enables the Content Vectoring Protocol. Select the **CVP server** from the drop-down menu.

  Note - Make sure the CVP server is already be defined as an OPSEC Application.
- **CVP Server is allowed to modify content** - Configures the CVP server to inspect but not modify content. If this option is not selected and the CVP server discovers a problem, such as a virus, the email message or attachment will not be allowed.

- **Reply Order** - designates when the CVP server returns data to the Security Gateway security server. The CVP server checks the file one packet at a time. After the CVP server has inspected the whole file, it sends a Validation Result message to the security server. If the Validation Result is that the file is approved, the security server sends the file back to the Inspection module, which sends the file on to the client.
  - **Return data after content is approved** - The CVP server sends the file back security server after checking the whole file.
  - **Return data before content is approved** - The CVP server sends packets to the security server as soon as it checks them. This option gives better response times to users, but can also result in virus infected files being sent to the security server.

FTP

What can I do here?

Use this window to configure general properties for an FTP Resource.

Getting Here - Object Explorer > New > Resource > FTP

FTP Resource Tracking Options

Exception Track options determine how to log actions taken as a result of a match on the resource. For example, if a virus is detected and Use CVP (Content Vector Protocol) in the CVP tab is enabled, the action is tracked in the way configured here.

FTP - Match (Wildcards)

What can I do here?

Use this window to configure how the FTP Resource is matched.

Getting Here - Object Explorer > New > Resource > FTP - Match Wildcards

FTP - Match Wildcard Options

Resource Path

Refers to a location on the FTP server. It is possible to allow downloads from a certain location on the server, but not others.

The file path name must include the directory separator character "/". For example, the request "/myfile" is matched to "/<current directory>/myfile". If the Resource path name specifies only "myfile", then the request will not be matched.

When using wildcard characters for the Path, you must specify either the full path name, or use the directory separator in the wildcard expression. For example, the path name "*/myfile" will match "myfile" in all possible directories.

Path includes the file name (which can include wildcard characters). For example: "/boys/fred/*" includes all the files in the /boys/fred/ directory, and "/boys/fred/" does not include any of the files in the /boys/fred/ directory. If /boys/fred were a file, it would be included in "/boys/fred/".

Note - Only lower case characters are allowed.

Resource Matching Method

- **GET** allows
  - Downloads from the server to the client
  - The commands RETR (retrieve), RNFR (rename from), and XMD5 (MD5 signature).
- **PUT** allows
  - Uploads from the client to the server.
  - The commands STOR (store), STOU (store unique), APPE (append), RNFR (rename from), RNTO (rename to), DELE (delete), MKD (make directory), RMD (remove directory).

FTP - CVP

What can I do here?

Use this window to create a new FPT- CVP resource.

Getting Here - Object Explorer > New > Resource > FTP - CVP

FTP - CVP Options

- **Use CVP** - Select to enable the Content Vectoring Protocol, and select the **CVP server** from the drop-down menu.

  Note - Make sure the CVP server is already be defined as an OPSEC Application.
- **CVP Server is allowed to modify content** - Configures the CVP server to inspect but not modify content. If this option is not selected and the CVP server discovers a problem, such as a virus, the email message or attachment will not be allowed.

- **Reply Order** - Designates when the CVP server returns data to the Security Gateway security server. The CVP server checks the file one packet at a time. After the CVP server has inspected the whole file, it sends a Validation Result message to the security server. If the Validation Result is that the file is approved, the security server sends the file back to the Inspection module, which sends the file on to the client.
  - **Return data after content is approved** - CVP server sends the file back security server after checking the whole file.
  - **Return data before content is approved** - CVP server sends packets to the security server as soon as it checks them. This option gives better response times to users, but can also result in virus infected files being sent to the security server.

TCP - General

What can I do here?

Use this window to configure CVP or UFP content security on any TCP Service using a third party OPSEC compliant application.

Getting Here - Object Explorer > New > Resource > TCP - General

Understanding TCP Resources

The TCP resource turns on **genericid** , a generic daemon (security server) that receives data packets and sends them to a CVP or UFP Server, as defined by the TCP resource.

The URL sent to a UFP Server is not a full URL but rather IP-based only. Before using the TCP Resource for UFP filtering, verify that the UFP Server supports IP-based URLs and can categorize specific protocols for which the TCP resource is to be implemented.

The TCP Resource is triggered when a Rule includes the TCP Resource, and a connection is encountered that matches both the Source and Destination of the Rule, and the Resource. If there is a match, then the action specified in the rule is applied.

TCP - UFP

What can I do here?

Use this window to configure the UFP properties of a URI Resource.

Getting Here - Object Explorer > New > Resource > TCP > UFP

TCP - Understanding UFP

UFP servers are OPSEC certified third party applications that check URLs against a list of permitted categories to determine whether or not access to that URL should be allowed.

When a user requests a URL, the Security Gateway determines if the UFP server must be used. If a UFP server is used, the connection is held until the Firewall determines if the connection is permitted.

This window specifies how a connection is matched to the Resource in a rule. If a connection matches the source and destination of the rule and the match parameters of the Resource, then both the Action in the Rule and the Action in the Resource are applied.

UFP Options

Tell me about the fields...

- **UFP server** - Select the UFP server, on which the UFP application is installed. The UFP server should already be defined as an OPSEC Application.
- **UFP caching control** - Configure if and how caching is to be enabled.

Caching Option	Description
No caching	UFP caching is disabled
Security Gateway (One Request)	UFP caching is controlled by the Check Point Security Gateway. This option disables the second, IP-based UFP request, thereby increasing performance. With this option the security server caches the UFP server's reply to a CAT (category) request.
Security Gateway (Two Request)	UFP caching is controlled by the Check Point Security Gateway, and enables the second, IP-based UFP request, thereby increasing cache integrity. With this option the security server sends a second CAT (category) request with the IP address acting as the URL address, after receiving a reply from the first CAT request.
UFP Server	The UFP server controls UFP caching. With this option the security server will cache a URL and mask sent by the UFP server in a cache_info format.

- **Ignore UFP server after connection failure** - UFP server is ignored after numerous unsuccessful UFP server connections. The UFP server is ignored for a specific period of time, during which the rules in the Rule Base take over for the UFP server. At the end of the specified period of time the connection is attempted again.
- **Number of failures before ignoring the UFP server** -configures at what point the UFP server should be ignored.
- **Timeout before reconnect to UFP server** - configures the amount of time that must pass before an attempt is made to reconnect to the UFP server.

TCP - CVP

What can I do here?

Use this window to specify what CVP inspection to perform on the TCP connection of the service that uses this Resource.

Getting Here - Object Explorer > New > Resource > TCP > Type: CVP. Move to CVP window

TCP Resource Properties - CVP

The CVP Server checks files one packet at a time. After the CVP Server has inspected the whole file, it sends a Validation Result message to the security server. If the Validation Result is that the file is approved, the security server sends the file back to the Inspection module, which sends the file on to the client.

Workflow

Select the CVP server from the drop-down menu. The CVP server must already be defined as an OPSEC Application.

Tell me about the fields...

CVP Server is allowed to modify content should be checked if the designated CVP Server can inspect and repair the message string. CVP servers cannot modify binary files, so if the resource matches on *.exe, you may want to prevent the CVP server modifying it, and just drop it. If you choose not to allow the CVP server to modify content, and the CVP server finds a problem (such as a virus), the TCP connection will not be allowed.

Reply Order

- **Return data after content is approved** means that the CVP Server sends the file back to the security server after checking the whole file.
- **Return data before content is approved** means that the CVP server sends packets to the security server as soon as it checks them. This option gives better response times to users, but may mean that the CVP server sends virus infected files to the security server.

CIFS

What can I do here?

Use this window to configure the properties of a CIFS resource.

Getting Here - Object Explorer > New > Resource > CIFS

Understanding CIFS

CIFS (Common Internet File System) is a protocol used to request file and print services from server systems over a network. The protocol is often implemented over the NETBIOS session service over TCP using port 139. In Windows networking, CIFS is used over the Microsoft-DS protocol (port 445) for networking and file sharing. The Security Gateway secures Microsoft Networking Services in the Inspection module, without requiring a security server. This meets the high performance requirements of LAN security.

Configuring CIFS Stateful Inspection

1. Define a new CIFS Resource: **Object Explorer** > **New** > **More** > **Resource** > **CIFS**.
2. Enter a name for the resource to be a network object.
3. In the **Allowed Disk\Print Shares** list, add CIFS servers and disk shares.
4. In **Type**, select log and block options.
5. Click **OK**.
6. Add a new Access Control Policy rule. In **Services & Applications**, add **nbsession** or **Microsoft-DS**, and associate the service with the configured CIFS Resource.

   Important - Do not delete or change the protocol type of the service objects that run content inspection. If the service is changed in this way, the protection will not work.
7. Install the policy.

CIFS Options

- **Allowed Disk\Print Shares** - Add or delete from the list of Allowed Disk and Print Shares. Wildcard characters are permitted. Many CIFS client implementations also try to map a pseudo share called IPC$. Allow access to this share to permit CIFS connections.

  For example, to allow access to the disk share PAUL on the CIFS server BEATLES:

  1. Click + and enter `BEATLES` in the **Server Name** field.
  2. Enter `IPC$` in the **Share Name** field.
  3. Click + again and enter `BEATLES` in the **Server Name** field and `PAUL` in the **Share Name** field.
- **Type**

- **Log mapped shares** - logs each share map attempt.
- **Log access violation** - logs any attempt to violate the restrictions imposed by the Resource. This includes attempts to access restricted disk shares as well as any malformed CIFS message issued by the client.
- **Block remote registry access** - blocks the ability to remotely manipulate a the window's registry.

MMS

What can I do here?

Use this window to configure the general settings of an MMS Resource object.

Note - To create a Rule with an MMS Resource, the MMS Resource must be associated with a particular WAP service.

Getting Here - Object Explorer > New > Resource > MMS

The Multimedia Messaging Service

Multimedia Messaging Service (MMS) is a communications technology developed by 3GPP (Third Generation Partnership Project) that lets users exchange -- over capable mobile phones and other devices -- messages with multimedia content.

MMS Options

- **Name** - Enter a name for the MMS Resource.
- **Action** - *Accept* or *Drop* traffic that matches a Firewall Rule using the MMS Resource.
- **Track** - *Log* the activity, to send an *Alert*, or take no action (*None*) when a packet matches on a Firewall Rule with the MMS Resource.

Time

What can I do here?

Use this window to create or edit a time object for use in rules based on a time limitation.

Getting Here - Object Explorer > New > Time > Time

Using Time Objects

A time object is used to represent a specific time frame. If you want a certain process to take place at a specific time, you can create a time object for the time at which the process should take place. The process will begin at the time specified by the time object.

A rule using a time object applies only to connections that begin during the time object's time frame. If the connection extends past that time frame, it is allowed to continue. The relevant time zone is that of the Security Gateway enforcing the rule.

Note - Security Gateways located in different time zones enforce the same object rules at different times. The lack of synchronization can cause problems. For example: one gateway may encrypt connections before the other is ready to decrypt them.

If you do not include a Time object in a rule, the rule is always active.

Multiple Time Objects

You can include multiple Time objects in a rule in these ways:

- Select each Time object to include it.
- Create a **Time Group** that includes multiple Time objects.

When you have multiple Time objects or a Time Group, each Time object works independently. For example, if a rule has two Time objects:

- One shows that the rule is active on Mondays.
- One shows that the rule is active from 9:00 - 17:00.

The rule is active each day from 9:00 - 17:00 and all day on Mondays. For the rule to be active from 9:00 - 17:00 on Mondays only, make one Time object that contains all of the criteria.

Time Object Options

- **Time period** - configures a range during which the time object is valid. When specifying an expiration date, a rule using that time object will not be enforced once the defined date has passed.
- **Recurring Hour Ranges** - Configures ranges during which the object is enforced.
- **Day Recurrence** - Configures if the time object will be enforced on a daily, weekly, or monthly basis.

Time Group

What can I do here?

Use this window to create or edit a group of time objects.

Getting Here - Object Explorer > New > Time > Time Group

Limit

What can I do here?

Use this window to create or edit a bandwidth limit object to use in rules for Application Control.

Getting Here - Object Explorer > New > Limit

Bandwidth Rate Limits

Use the Limit object in the **Action** column to restrict the bandwidth that is permitted for traffic matched on a rule with a Limit object. Configure a maximum throughput for uploads and downloads. The Limit object is permitted for an Application & URL Filtering Layer.

You can add one Limit object to a rule.

It can include upload and download rates.

For each option, select a number and unit to define the maximum permitted bandwidth for that action.

- **Download** - From the internet to the organization.
- **Upload** - From the organization to the internet.

When the limit is reached, the gateway starts to drop packets. Dropped packets show in the Application Control logs.

Important:

- In ClusterXL Load Sharing modes, the specified bandwidth limit is divided between all configured Cluster Members, regardless of the cluster state. For example, if a maximum limit requirement is 30 Gbps, and there are three Cluster Members, you must configure the Limit object in the rule to 30 Gbps / 3 = 10 Gbps.
- In a Scalable PlatformSecurity Group, the specified bandwidth limit is divided between all Security Group Members, regardless of their state. For example, if a maximum limit requirement is 30 Gbps, and there are three Security Group Members, you must configure the Limit object in the rule to 30 Gbps / 3 = 10 Gbps.

Internet

What can I do here?

This is the default destination for Application and URL Filtering rules, and applies to traffic heading outside the corporate network - to the DMZ and external interfaces.

Note - You can only use this object in the destination column of Application and URL Filtering enabled rules and layers. The object distinguishes between internal and external addresses.

Getting Here - Object Explorer > Search for Internet
Or:
Security Policies > Access Control > Policy > Destination > add new items > Internet

Group Membership

What can I do here?

Use this window to add the object you are editing to one or more groups.

Getting Here - Open an object for editing. Not all objects have this feature. Host and Network objects do.

Network Groups

A network group is a collection of hosts, gateways, networks or other groups. Groups can be used to facilitate and simplify network management. When you have the same set of objects which you want to use in different places in the Rule Base, you can create a group to include such set of objects and reuse it. Modifications are applied to the group instead of to each member of the group.

Groups are also used where SmartConsole lets you select only one object, but you need to work with more than one. For example, in the gateway editor > **Network Management** > **VPN Domain** > **Manually defined**, you can only select on object from the drop-down menu. If you want to select more than one object for your VPN Domain, you can create a group, add the required objects to the group, and select the group from the drop-down menu.

Grouping Network Objects

To create a group of network objects:

1. In the **Objects** tree, click **New** > **Network Group**.

   The **New Network Group** window opens.

2. Enter a name for the group
3. Set optional parameters:
   - Object comment
   - Color
   - Tag (as custom search criteria)
4. For each network object you want to add, click the [+] sign and select it from the list that shows.
5. Click **OK**.

From R80.20.M2, you can also associate groups to a network object directly from the object editor.

To associate groups to a network object:

1. Open the object editor, and go to **Groups** in the navigation tree.
2. For each group you want to add, click the [+] sign and select it from the list that shows.

Multi-Domain Security Management

Check Point Multi-Domain Security Management is a centralized management solution for large-scale, distributed environments with many discrete network segments, each with different security requirements. This solution lets administrators create Domains based on geography, business units or security functions to strengthen security and simplify management.

Each Domain has its own Security Policies, network objects and other configuration settings. You use the Global Domain for common Security Policies that apply to all or to specified Domains. The Global Domain also includes network objects and other configuration settings that are common to all or to specified Domains.

The Multi-Domain View

What can I do here?

The **Multi Domain** view is the management control center for Multi-Domain Security Management environments.

Use the **Multi Domain** view to:

- Configure and manage Domains
- Configure and manage Domain Management Servers
- Define and manage policies for Domain Management Server Security Gateways and other objects
- Define and manage Global Domains and Global policies
- Configure and manage administrators and Permissions Profiles
- Configure and manage trust for SmartConsole clients
- Configure other Multi-Domain Security Management system parameters
- Install Policy

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Domains

The Multi-Domain Server

A **Multi-Domain Server** is a physical server that contains the Domain Management Servers, Security Policies, system data, and Multi-Domain Security Management system software. You connect to a Multi-Domain Server to work with Multi-Domain Security Management features, objects, and configuration settings. This includes:

- Domain Management Servers and their configuration settings
- Global Policies and objects
- Administrators and permission profiles
- Logs and monitoring features
- System configuration settings

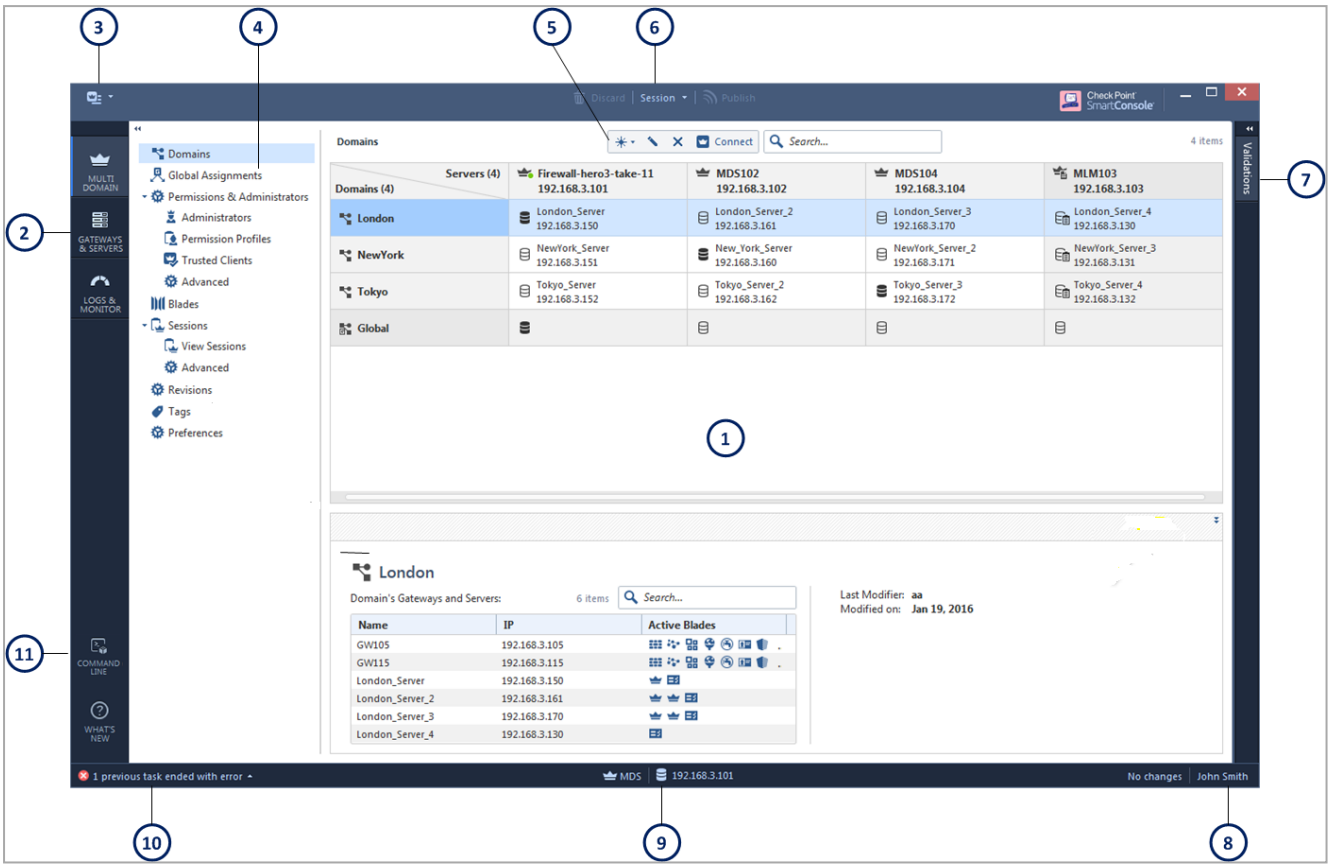
You can create a High Availability and/or Load Sharing deployment with two or more, synchronized Multi-Domain Servers.

Multi-Domain View

Use the *Multi-Domain view* to manage Multi-Domain Servers, Domains, system objects, configuration settings and other features. You must log into a Multi-Domain Server to see the Multi-Domain view.

For a guided tour of **Multi-Domain** view, click the **What's New** button  at the bottom left of the window. Click the **<** and **>** icons to scroll between the different What's New screens.

Multi-Domain view elements



Item	Description
1	View, as selected from the **Navigation Toolbar** and **View** tree (This example shows the **Multi-Domain** > **Domains** view)
2	Navigation toolbar
3	Menu
4	View tree
5	Actions toolbar
6	Session Management toolbar
7	Validation tab
8	Logged in administrator
9	Server details area
10	Task information area

Item	Description
11	Management script commands and API

Domain Management Servers

A *Domain* is a virtual object that defines a network or a collection of networks related to an entity. You can define a Domain for a company, business unit, department, branch or geographical location. For example, a cloud service provider typically has one Domain for each customer. A bank can have one Domain for each geographical region, state, or country.

A *Domain Management Server* is the functional equivalent of a Security Management Server in a single-domain environment. You connect directly to a Domain Management Server with SmartConsole to manage a Domain and its components:

- Domain Security Gateways
- Domain Security Policies, rules, and other Domain level security settings
- Domain system objects, such as services, users, and VPN Communities.
- Domain Software Blades and their related configuration settings

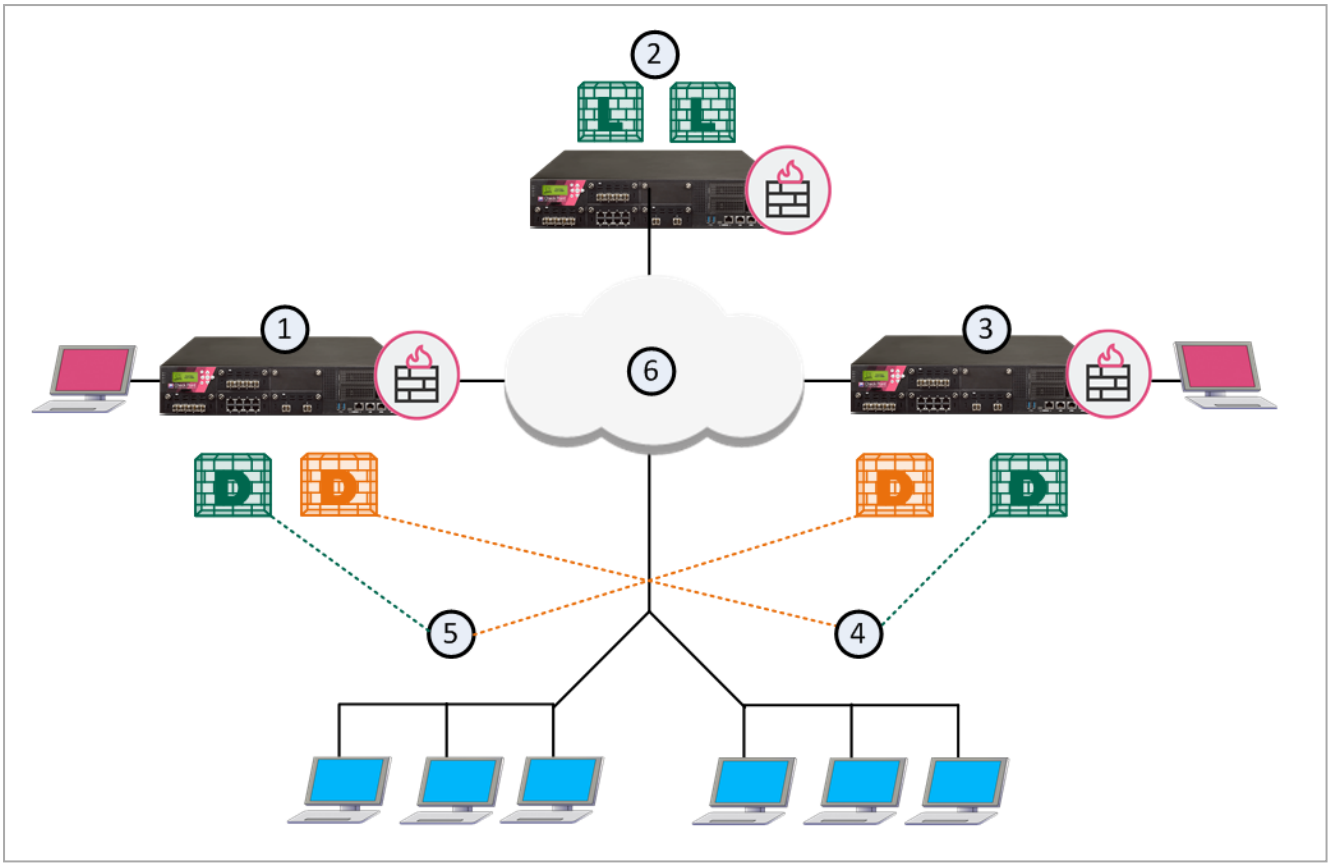
To learn more about working with SmartConsole to manage Domains, see the *R81.10 Security Management Administration Guide*.

There can be more than one Domain Management Server for a Domain in a High Availability deployment, each on a different Multi-Domain Server. One Domain Management Server is *Active*, and the other, fully synchronized Domain Management Servers are *Standby*.

Domain Log Servers

A typical Multi-Domain Security Management deployment includes, at least one Multi-Domain Log Server to hold log files generated by Domain Security Gateways. Each Domain can have its own Domain Log Server on the Multi-Domain Log Server. This deployment strategy keeps log traffic isolated from other network traffic for better throughput.

This illustration shows a sample deployment with two Multi-Domain Servers and two Domains. The Multi-Domain Log Server contains two Domain Log Servers, one for each Domain.



Item	Description
1	London Multi-Domain Server with an Active Domain Management Server for London and a Standby Domain Management Server for Tokyo
2	Multi-Domain Log Server with Domain Log Servers for London and Tokyo
3	Tokyo Multi-Domain Server with an Active Domain Management Server for Tokyo and a Standby Domain Management Server for London
4	Tokyo network
5	London network
6	Internet
	Active Domain Management Server
	Standby Domain Management Server
	Domain Log Server

Connecting to SmartConsole

Use SmartConsole to connect to a Multi-Domain Server when you work with Multi-Domain Security Management objects and settings. Use SmartConsole to connect to a Domain Management Server when you work with Domain Security Policies, rules, objects and configuration settings. You can also connect to Domains or specified Domain Management Servers from within the Multi-Domain view.

To connect to a Multi-Domain Server:

1. Run SmartConsole.
2. Enter your user name and password.
3. Enter the Multi-Domain Server IP address, and then click **Login**.
4. In the **Welcome** screen, select MDS from the list, and then click **Proceed**.

   SmartConsole opens in the **Domains** view.

To connect directly to a Domain:

1. Run SmartConsole.
2. Enter your user name and password.
3. Enter the Multi-Domain Server IP address, and then click **Login**.
4. In the **Welcome** screen, select a Domain from the list, and then click **Proceed**.

SmartConsole opens with the selected Domain Management Server.

To connect to a Domain Management Server from the SmartConsole Multi-Domain view:

1. Connect to a Multi-Domain Server with SmartConsole.
2. In the **Multi-Domain** > **Domains** view, right-click the required Domain Management Server in the grid.
3. Select **Connect to Domain Server**.

Note - In a High Availability deployment, you can only make changes to a Domain from the active Domain Management Server. The active Domain Management Server shows with a black icon. If you connect to a standby Domain Management Server (white icon), SmartConsole opens in the Read Only mode.

Gateways & Servers View

The **Gateways & Servers** view shows all Security Gateway, Domain Management Server, and Domain Log Server objects in the Multi-Domain Security Management environment. This feature lets administrators, with applicable permissions, see and work with them in one convenient location.

You can double-click an object in this view to open its configuration window in the Domain's SmartConsole. For example, if you double-click, **GW105** on the example below, the **London_Server** Domain Management Server opens in SmartConsole and shows the **GW105** configuration window.

The Gateways & Servers view

Status	Name	Domain	IP	Version	Active Blades	Hardware
–	GW105	London	192.168.3.105	R77.20	...	4000 Appliances
–	GW106	NewYork	192.168.3.106	R77.20	...	12000 Appliances
–	GW107	Tokyo	192.168.3.107	R77.20	...	13000 Appliances
–	GW115	London	192.168.3.115	R77.30	...	21000 Appliances
–	GW116	NewYork	192.168.3.116	R77.30	...	13000 Appliances
–	GW117	Tokyo	192.168.3.117	R77.30	...	61000 Appliances
–	London_Server	London	192.168.3.150	R80		Open server
–	London_Server_2	London	192.168.3.161	R80		Open server
–	London_Server_3	London	192.168.3.170	R80		Open server
–	London_Server_4	London	192.168.3.130	R80		Open server
–	New_York_Server	NewYork	192.168.3.160	R80		Open server
–	NewYork_Server	NewYork	192.168.3.151	R80		Open server
–	NewYork_Serve...	NewYork	192.168.3.171	R80		Open server
–	NewYork_Serve...	NewYork	192.168.3.131	R80		Open server
–	Tokyo_Server	Tokyo	192.168.3.152	R80		Open server
–	Tokyo_Server_2	Tokyo	192.168.3.162	R80		Open server
–	Tokyo_Server_3	Tokyo	192.168.3.172	R80		Open server
–	Tokyo_Server_4	Tokyo	192.168.3.132	R80		Open server

Global Object Explorer

What can I do here?

Use this window to search for an object, view unused objects and see where an object is used across all domains.

Getting Here - Menu > Open Global Object Explorer

Cross Domain Search

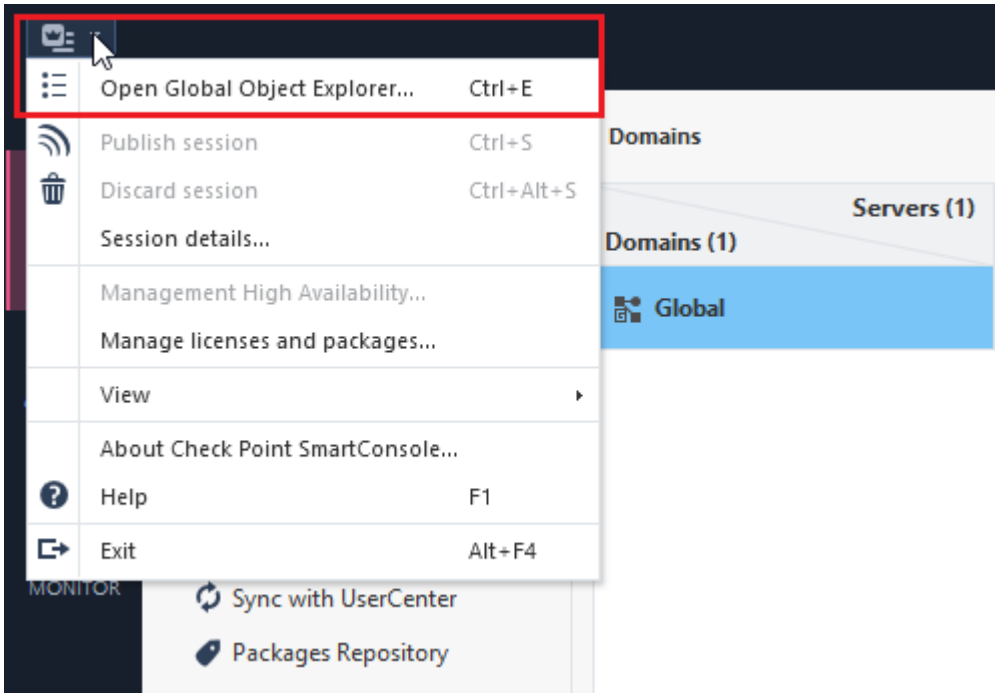
Starting from R81, you can do these actions from the Multi-Domain view across all Domains, without logging into each Domain:

- Search an object
- View unused objects
- See where an object is used

For information on how to do these actions in a specific domain, see the *R81.10 Security Management Administration Guide*.

To do a cross-domain search:

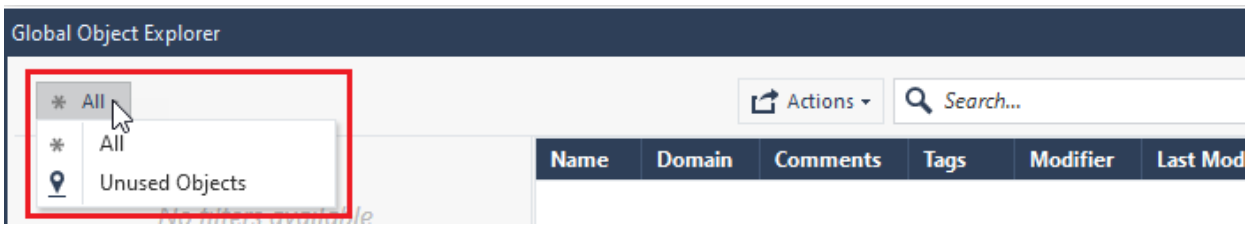
1. In the Multi-Domain view, click the drop-down arrow in the main menu and select **Open Global Object Explorer**.



   The **Global Object Explorer** window opens.

2. In the search box, enter what you are searching. A list appears which shows all the applicable objects which fit your search in all the Domains.

   You can select to see all search results or only results of unused objects.



To view unused objects:

1. In the Multi-Domain view, click the drop-down arrow in the main menu and select **Open Global Object Explorer**.

   The **Global Object Explorer** window opens.

2. In the upper left corner, select **Unused Objects**.

A list appears with all the unused object in all the Domains..

To see where an object is used

1. In the Multi-Domain view, click the drop-down arrow in the main menu and select **Open Global Object Explorer**.

   The **Global Object Explorer** window opens.

2. Navigate to the applicable object.

3. Right-click the object and select **Where Used**.

A list appears with all the places where the object appears in all the Domains.

Notes:

- Cross-Domain Search is supported only on Domains defined on a Multi-Domain Server, to which the user is connected with SmartConsole.
- Cross-Domain Search is supported only on Domains, for which the connected user has Read or Read/Write permissions.

Multi-Domain Server - Install Policy

What can I do here?

Use this window to install the policy on gateways in the selected domain.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Domains > right-click Domain > Install Policy

Multi-Domain Server General

What can I do here?

Use this window to configure the general properties for a Multi-Domain Server or Multi-Domain Log Servers.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > New > Multi-Domain Server > General page
Or:
SmartConsole for Multi-Domain Server > Multi Domain > New > Multi-Domain Log Servers > Multi-Domain page

Multi-Domain Server General

Basic Details:

- **Type Object Name** - Enter a unique name for this Multi-Domain Server or Multi-Domain Log Servers.
- **Type Object Comment** - Optional: Enter a textual description or comment for this Multi-Domain Server or Multi-Domain Log Servers.
- **IP Address** - Enter the Multi-Domain Server or Multi-Domain Log Servers IP address

  Important - You must always assign an IPv4 address to a Multi-Domain Server or Multi-Domain Log Servers.
- **Connect** - Click to establish SIC trust
- **Revoke** - Click to revoke a certificate
- **View** - Click to see SIC details

Platform

- **OS** - Select an operating system
- **Version** - Select a release version
- **Hardware** - Select the appliance model or computer type

Note - Platform details are not automatically entered when the Primary MDS is created. You can select the correct details but the fields have no functionality.

Creating a Secondary Multi-Domain Server

This section shows you how to create a new secondary Multi-Domain Server.

Important: Before you start this procedure, make sure to define the physical server as the correct server type (Secondary Multi-Domain Server, or Multi-Domain Log Server) during installation. An incorrect definition can cause deployment failure.

To create a new, secondary Multi-Domain Server:

1. If you did not do so, install a new R81.10 Secondary Multi-Domain Server.

   Make sure to define this server as a secondary Multi-Domain Server in the First Time Wizard. Connect to the Primary Multi-Domain Server with SmartConsole and go the **Multi-Domain** > **Domains** view.

2. In the Multi-Domain navigation toolbar, click **New** > **Multi-Domain Server**.
3. Enter a unique name for this Multi-Domain Server.

   To get the IP address automatically, the name must be in the DNS.

4. Enter the IPv4 address or click **Resolve IP** to get the IP address from the DNS.
5. Select the platform operating system, software version, and hardware type.
6. Click **Connect** to establish SIC trust.

The new Multi-Domain Server automatically synchronizes with all existing Multi-Domain Servers and Multi-Domain Log Servers. The synchronization operation can take some time to complete, during which a notification indicator shows in the task information area.

Changing an Existing Multi-Domain Server

You can change the settings for an existing Multi-Domain Server or Multi-Domain Log Server.

To change the settings for an existing Multi-Domain Server:

1. Double-click the Multi-Domain Server or Multi-Domain Log Server in the top row of the **Domains** grid.
2. In the **Multi-Domain Server** window, change the parameters in the **General**, **Multi Domain** and **Log Settings** views.

Note -You cannot change the Multi-Domain Server name.

Re-Establishing SIC Trust for a Secondary Multi-Domain Server

Important - You can only re-establish SIC trust on a Secondary Multi-Domain Server or Multi-Domain Log Servers. There is no option to establish SIC trust on the Primary Multi-Domain Server.

It is occasionally necessary to re-establish trust between a Primary and secondary Multi-Domain Server or Multi-Domain Log Server. This can occur for many reasons, including:

- Changes to the IP address of the Primary Multi-Domain Server, Secondary Multi-Domain Server or Multi-Domain Log Server

- Failure and recovery of the Primary Multi-Domain Server
- Promotion of a Secondary Multi-Domain Server to Primary Multi-Domain Server
- Internal Certificate Authority (ICA) failure on the Primary Multi-Domain Server

To re-establish SIC trust:

1. Open a command line interface to the Secondary Multi-Domain Server or Multi-Domain Log Server.
2. Log in and run: `mdsconfig`
3. Enter the number for **Secure Internal Communication**, and then press **Enter**.
4. Enter `y` to confirm.
5. Enter and confirm the activation key.
6. Enter the number for **Exit**.
7. Wait for Check Point processes to stop and automatically restart.
8. In the SmartConsole **Multi Domain** view, double-click a Secondary Multi-Domain Server or Multi-Domain Log Server object.
9. In the **Multi-Domain Server** window, click **Connect**.
10. In the **Initialize SIC** window, enter activation key that you entered in step 5 above.

    If successful, the **Certificate State** field shows **Trust established**.

Deleting a Secondary Multi-Domain Server or Multi-Domain Log Server

To delete a secondary Multi-Domain Server:

1. Move each Active Domain Management Server on the secondary Multi-Domain Server to another Domain Management Server.
2. Connect to the command line on the Multi-Domain Server to be deleted and run: `mdsstop`
3. In SmartConsole, right-click the secondary Multi-Domain Server, and then select **Delete Multi-Domain Server**.
4. Confirm the action and click **OK**.
5. Publish the SmartConsole session.

Note - This procedure deletes all standby and non-primary Domain Management Servers on the Secondary Multi-Domain Server. You cannot delete the Primary or Active Domain Management Server.

Overview of High Availability

High Availability is redundancy and database backup for management servers. Synchronized servers have the same policies, rules, user definitions, network objects, and system configuration settings.

Multi-Domain Security Management implements High Availability at these levels:

- **Multi-Domain Server High Availability** is an Active/Active redundancy solution that uses two or more fully synchronized Multi-Domain Servers for continuous redundancy. All Multi-Domain Servers are Active. You can log into and work with the primary or secondary Multi-Domain Servers.
- **Domain Management Server High Availability** is both a redundancy and a Load Sharing solution for Domains. You create a Domain Management Server on two or more Multi-Domain Servers. These Domain Management Servers synchronize fully for continuous redundancy.

  One Domain Management Server is Active and the others are Standby. Each Multi-Domain Server can have both Active and Standby Domain Servers. You can configure the Active Domain Management Server on different Multi-Domain Servers for effective load sharing.

All High Availability deployments include one Primary Multi-Domain Server and one or more Secondary servers. Synchronization occurs automatically when administrators publish sessions with changes to Policies, objects or configuration settings.

Primary and Secondary Multi-Domain Servers

The order in which you install Multi-Domain Servers is significant. You must define the first physical server as a Primary Multi-Domain Server in the First Time Wizard. You must define all other Multi-Domain Servers as Secondary in the First Time Wizard.

Active and Standby Domain Management Servers

You can only use the Active Domain Management Server to manage Domain Security Gateways, networks, Security Policies objects and system configuration. Standby Domain Management Servers synchronize fully for redundancy. You can connect to a Standby Domain Management Server in the Read Only mode to look at current object configurations and Rule Base.

In the standard configuration, there is only one Active Domain Management Server for each Domain. All others are Standby Domain Management Servers. If the Active Domain Management Server fails, you must manually change a Standby Domain Management Server to Active.

Important - Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

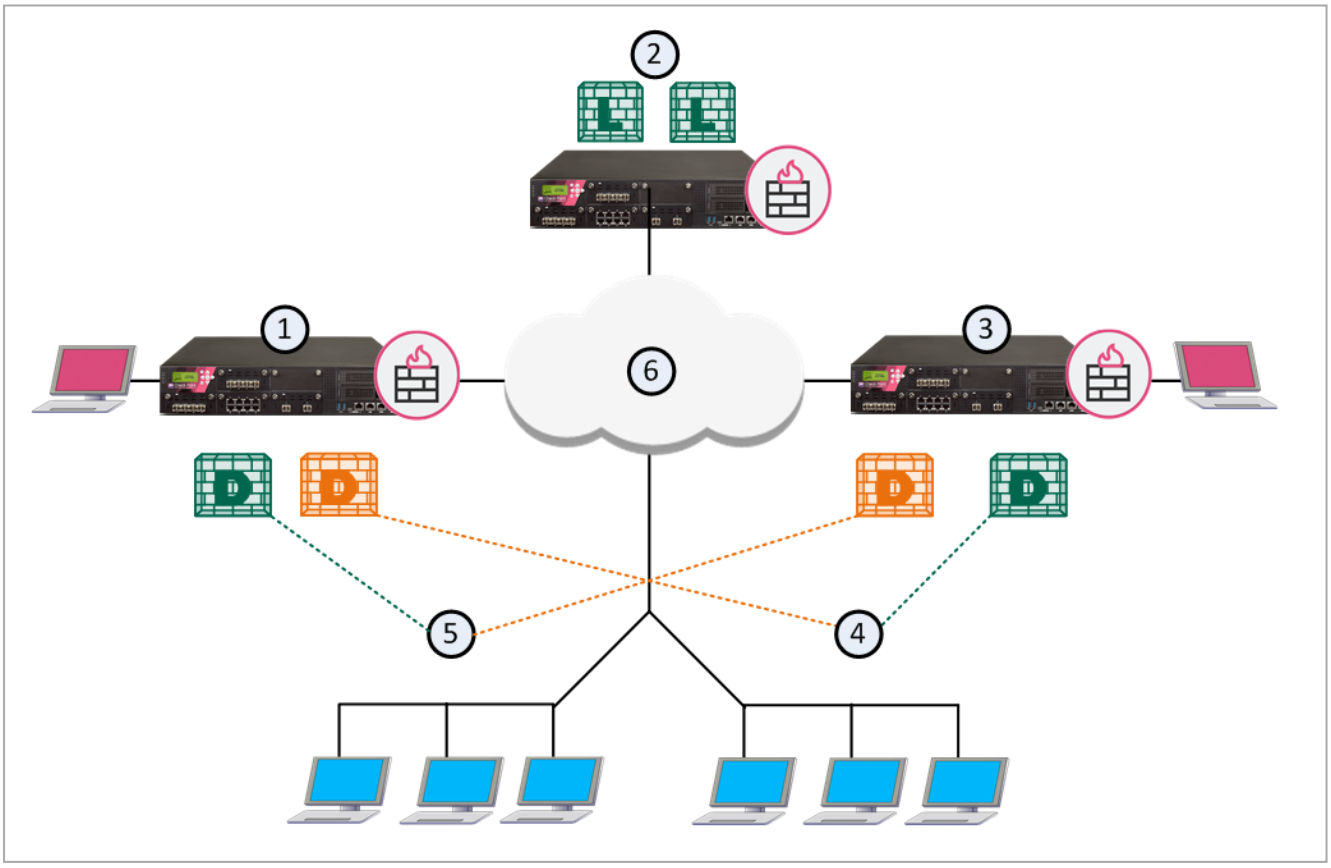
For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81.10 Gaia Administration Guide*.
- About the `migrate export` and `migrate import` commands, see the *R81.10 CLI Reference Guide*.
- About the `mds_backup` and `mds_restore` commands, see the *R81.10 Multi-Domain Security Management Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Multi-Site High Availability Deployment Example

This example shows a Multi-Site, High Availability deployment with two Multi-Domain Servers and one Multi-Domain Log Server. A real-life deployment will have many more assets.

Each Multi-Domain Server has two Domains configured for Load Sharing, where a different Domain Management Server is Active at each location. Administrators can connect to all Multi-Domain Servers. For best performance, connect to the Multi-Domain Server nearest to your geographical location.



Item	Description
1	London Multi-Domain Server with an Active Domain Management Server for London and a Standby Domain Management Server for Tokyo
2	Multi-Domain Log Server with Domain Log Servers for London and Tokyo
3	Tokyo Multi-Domain Server with an Active Domain Management Server for Tokyo and a Standby Domain Management Server for London
4	Tokyo network
5	London network
6	Internet
	Active Domain Management Server
	Standby Domain Management Server
	Domain Log Server

This illustration shows the configuration grid in the SmartConsole **Multi Domain** view for the example deployment:

The system automatically creates the Global Domain when you install Multi-Domain Security Management.

Synchronization

In a multi-domain environment, the Multi-Domain Servers work in active-active mode. All Multi-Domain Servers are active and synchronize each other.

The Domains managed by the Multi-Domain Server work in active-standby mode, where the Active Domain Server synchronizes all the standby Domain Servers.

The system automatically synchronizes periodically and when an administrator publishes changes to the configuration.

How Synchronization Works

During synchronization, the system performs these steps without user intervention:

On periodic synchronization:

1. The Active exports the delta data between the Active server and the Standby server to compressed files.
2. The compressed files are transferred to the Standby server.
3. The Standby Server replays the delta data from the uncompressed files.

On manual synchronization:

1. The Active Server exports the public data to compressed files.
2. The compressed files are transferred to the Standby Server.
3. The Standby server overrides the existing data with the uncompressed files.

The data that is transferred during synchronization includes:

- Postgres database
- Solr
- ICA database
- Configuration files
- Domain licenses and contracts. Multi-Domain Server licenses and contracts are not transferred.

Multi-Domain Server ICA Database Synchronization

When you create a new secondary Multi-Domain Server, the Internal Certificate Authority (ICA) on the Primary Multi-Domain Server generates a certificate when you establish SIC trust. The ICA can generate a certificate for a new administrator, if required by the authentication method. In a High Availability deployment with more than one Multi-Domain Server, the system synchronizes the ICA databases as necessary.

Initial Synchronization

Initial synchronization occurs automatically when you create a secondary Multi-Domain Server, Multi-Domain Log Server, or Domain Management Server. The system generates a task to copy all databases and system information from the connected server to the new server.

Multi-Domain Server and Multi-Domain Log Server synchronization tasks show in the **Task Information** area, in the Multi-Domain Server SmartConsole. Domain synchronization tasks show in the Domain SmartConsole.

Periodic Synchronization

Multi-Domain Servers synchronize with all other peers and Multi-Domain Log Servers. Periodic synchronization occurs automatically, and when an administrator publishes a session. Private (non-published) sessions do not synchronize.

Periodic synchronizations are incremental. Only database changes synchronize with peers. Active Domain Management Servers synchronize to the standby Domain Management Servers.

Manual Synchronization

Manual synchronization is a full synchronization that overwrites all data on the peers. It disconnects all connected clients and overrides active sessions and running tasks.

When changes made in a session are published on the Active server (made public), the changes are synchronized to the Standby server. Unpublished, private sessions are not synchronized.

Best Practice - Use this option with caution, and only in cases of synchronization error. We recommend that you publish changes before initiating full sync.

For Domain Management Servers, you can only run a manual synchronization from the active Domain Management Server to the standby peers.

Manually Synchronizing a Multi-Domain Server

You can manually synchronize the connected Multi-Domain Server with a peer Multi-Domain Server.

To manually synchronize Multi-Domain Servers:

1. Click the **Synchronization Status** area at the bottom of the SmartConsole window.
2. In the **High Availability Status** window, select a peer Multi-Domain Server to synchronize.
3. Click **Sync Peer**.

Synchronization starts immediately and the status shows in the window. The synchronization operation can take many minutes to complete.

Warning - Use manual synchronization with caution. This can overwrite all data on the peer Multi-Domain Server if they do not synchronize correctly.

Manually Synchronizing Domain Management Servers

You can manually synchronization a Standby Domain Management Server with the Active Domain Management Server on a different Multi-Domain Server.

To manually synchronize Domain Management Servers for a Domain:

1. Open SmartConsole for the active Domain Management Server.
2. Click **Menu** > **High Availability**.
3. In the **High Availability Status** window, click **Actions** > **Sync Peer**. .

Synchronization starts immediately and the status shows in the window. The synchronization operation can take many minutes to complete.

Looking at High Availability Status

To see Multi-Domain Server and Multi-Domain Log Server High Availability status:

1. Select **Management High Availability** from the **SmartConsole menu**.

   The **High Availability Status window** shows all Multi-Domain Servers and Multi-Domain Log Servers in your environment, together with their synchronization status.

Icon	Status
	Multi-Domain Server (that you are connected to) - Synchronization OK
	Multi-Domain Server Synchronization OK
	Multi-Domain Log Server Synchronization OK
	Multi-Domain Server - Not synchronized - No connection with peer

To see Domain Management Server High Availability status:

1. Connect to a Domain with SmartConsole.

   By default, SmartConsole connects to the Active Domain Management Server.

2. Select **Management High Availability** from the **SmartConsole menu**.

   The **High Availability Status** window shows the status of all Domain Management Servers for the selected Domain. You can manually synchronize the peer servers with the Domain Management Server to which you are connected. You can also connect with SmartConsole to a peer Domain Management Server in the Read Only mode.

Icon	Status
	Active Domain Management Server - Synchronization OK
	Standby Domain Management Server - Synchronization OK
	Domain Log Server - Synchronization OK
	Domain Management Server not synchronized - No connection with peer

Icon	Status
	Domain Management Server synchronization in process or has a problem

Note - Domain servers' status is reflected also in the Domains view in the SmartConsole connected to the Multi-Domain Server..

Domain Management Server High Availability and Load Sharing

This section includes procedures for configuring the Multi-Domain Security Management environment for secondary Multi-Domain Servers and a Multi-Domain Log Server. When you install Multi-Domain Security Management for the first time, select **Primary Multi-Domain Server** in the First Time Wizard. For High Availability and Load Sharing, select **Secondary Multi-Domain Server** in the First Time Wizard.

Each Domain has one Active and one or more Standby Domain Management Servers. For example, if a deployment has three Multi-Domain Servers, each Domain can have one Active and two Standby Domain Management Servers. This lets the Domains load be shared between several physical Multi-Domain Servers.

Example of Domain Management Server High Availability with Load Sharing:

Domains (4) \ Servers (3)	MDS110 192.168.3.110	MDS104 192.168.3.104	MDS111 192.168.3.111
DOM155	192.168.3.155	192.168.3.176	192.168.3.166
DOM165	192.168.3.156	192.168.3.178	192.168.3.165
DOM175	192.168.3.158	192.168.3.175	192.168.3.167
Global			

By default, the Primary Domain Management Server is Active. All other Domain Management Servers for that Domain are Standbys. You can change a Standby Domain Management Server to Active as necessary.

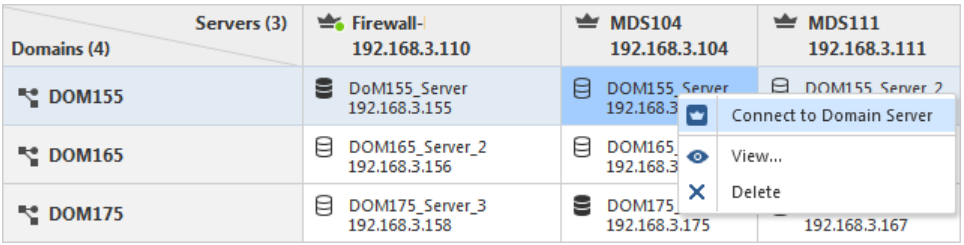
All Domain management operations, such as working with Security Policies, users, networks and other objects, occur on the Active Domain Management Server. Standby Domain Management Servers automatically synchronize with the Active Domain Management Server. Security Gateways can get a Security Policy and a Certificate Revocation List (CRL) from either the Active or Standby Domain Management Servers.

Changing the Active Domain Management Server

If the current Active Domain Management Server is responsive, use this procedure to set a different Domain Management Server to Active.

To change an Active Domain Management Server:

1. Right-click the cell for a Standby Domain Management Server, and then select **Connect to Domain Management Server**.



2. In the Domain SmartConsole instance, click **Menu** > **High Availability**.
3. In the **High Availability Status** window, click a Standby Domain Management Server **Actions** > **Set Active**.
4. Close SmartConsole and re-connect to the newly Active Domain SmartConsole.

The Standby Domain Management Server changes to Active. The Standby Domain Management Servers automatically synchronize, and a confirmation message shows in the **High Availability Status** window. The synchronization operation can take many minutes to complete.

To manually set the Active Domain Management Server to Standby

1. Right-click the cell for the Active Domain Management Server, and select **Connect to Domain Management Server**.
2. Click **Menu** > **Management High Availability**.
3. In the **High Availability Status** window, click **Actions** > **Set Standby**.
4. Confirm when prompted.

The Active Domain Management Server changes to Standby. Continue the procedure to set a different Domain Management Server to Active. Until you do this, Domain SmartConsole clients open in the Read Only mode and you cannot work with Domain objects or Policies.

Note - SmartConsole clients connected to the Active Domain Management Server will be disconnected during the procedure for changing the Active Domain Management Server.

Multi-Domain Server - Multi-Domain

What can I do here?

Use this window to define the server type and a range of valid IPv4 addresses.

Settings and Parameters:

- **Server Type** - Select Management for a Multi-Domain Server or Logging a Multi-Domain Log Servers.
- **IP Range** - Enter a range of valid IP addresses that can assigned automatically to new Domain Management Servers.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > New > Multi-Domain Server > Multi-Domain page
Or:
SmartConsole for Multi-Domain Server > Multi Domain > New > Multi-Domain Log Servers > Multi-Domain page

Configuring Automatic Domain IP Address Assignment

You can configure a Multi-Domain Server to assign an IP address to Domain Management Servers managed by this Multi-Domain Server from a predefined pool of IP addresses. This makes sure that the assigned IP address is not in use by other Multi-Domain Servers or Domain Management Servers.

To configure a Multi-Domain Server to assign IP addresses to Domain Management Servers:

1. In the **Multi-Domain** view, right-click a Multi-Domain Server and select **Edit**.

   The **Multi-Domain Server** window opens.
2. From the navigation tree, select **Multi-Domain**.
1. In the **IP Range** section, enter the first and last IP address in the range.
2. Click **OK**.

Configuring Security Gateways to Send Logs to a Log Servers

Logs are not automatically forwarded to a Log Server. You must manually configure each relevant Security Gateway to send its logs to the new Domain Log Server.

To configure Domain Security Gateways to send logs to a Log Server:

1. Connect to the applicable Domain Management Server with SmartConsole, and then double-click the applicable Security Gateway.
2. In the **Logs** section, select the new Log Server from the list.

   You can delete or ignore other Log Servers in the list as necessary.

3. Click **OK**.
4. Configure other log settings as applicable.
5. Install Policy on the applicable Security Gateways.
6. Install the database on the Log Servers.

Multi-Domain Log Settings - General

What can I do here?

Use this window to set disk space cleanup and alert options.

> **Getting Here - Getting Here** - SmartConsole for Multi-Domain Server > Multi Domain > New > Multi-Domain Server > Log Settings > General
> Or:
> SmartConsole for Multi-Domain Server > Multi Domain > New > Multi-Domain Log Servers > Log Settings > General

Creating a Multi-Domain Log Server with Domain Log Servers

This section shows you how to create a new Multi-Domain Log Server and its related Domain Log Servers.

Important : Before you start this procedure, make sure that you define the physical servers as the correct server type (Secondary Multi-Domain Server or Multi-Domain Log Server) during installation. An incorrect definition can cause deployment failure.

To create a new Multi-Domain Log Server:

1. If you did not do so, install a new R80.30 Multi-Domain Log Server.

   Make sure to define this server as a Multi-Domain Log Server in the First Time Configuration Wizard.
2. Connect with SmartConsole to the primary Multi-Domain Server - the **MDS** context.
3. From the left navigation panel, click **Multi Domain > Domains**.
4. From the top toolbar, click **New** > **Multi-Domain Log Server**.
5. Enter a unique name for this Multi-Domain Log Server.
6. Enter the IPv4 address or click **Resolve IP** to get the IP address from the DHCP Server.
7. Click **Connect** to establish SIC trust.

Enter the same Activation Key you entered during the First Time Configuration Wizard of the Multi-Domain Log Server.

8. In the **Platform** section:
   - In the **OS** field, select **Gaia**
   - In the **Version** field, select the correct version
   - In the **Hardware** field, select the applicable option
9. Click **OK**.

To create Domain Log Servers:

1. Connect with SmartConsole to the primary Multi-Domain Server - the **MDS** context.
2. From the left navigation panel, click **Multi Domain > Domains**.
3. In the **Multi-Domain Log Server** column, right-click the Domain **Log Server** cell for each Domain and click **New Domain Server**.
4. Accept the default name or enter a different, unique name.
5. Enter the IPv4 address or click **Resolve IP** to automatically assign the IPv4 address.
6. Click **OK**.

   Wait for the cell to show the new Domain Log Server.
7. Configure Security Gateways in each Domain to send its logs to the new Domain Log Server on the Multi-Domain Log Server.

   The Domain Log Servers synchronize automatically.

The new Multi-Domain Log Server automatically synchronizes with all existing Multi-Domain Servers. The synchronization operation can take many minutes to complete, during which a notification indicator shows in the task information area.

Configuring Security Gateways to Send Logs to a Log Servers

Logs are not automatically forwarded to a Log Server. You must manually configure each relevant Security Gateway to send its logs to the new Domain Log Server.

To configure Domain Security Gateways to send logs to a Log Server:

1. Connect to the applicable Domain Management Server with SmartConsole, and then double-click the applicable Security Gateway.
2. In the **Logs** section, select the new Log Server from the list.

You can delete or ignore other Log Servers in the list as necessary.

3. Click **OK**.
4. Configure other log settings as applicable.
5. Install Policy on the applicable Security Gateways.
6. Install the database on the Log Servers.

Deleting a Domain Log Server

To delete a Domain Log Server in SmartConsole:

1. Connect with SmartConsole to the primary Multi-Domain Server - the **MDS** context.
2. From the left navigation panel, click **Multi Domain > Domains**.
3. In the Multi-Domain Log Server column, right-click the Domain Log Server and then select **Delete**.

Log Management Settings

In the **General** view, configure these settings:

- **Cleanup when free disk space is below** - Start the disk cleanup procedure when available disk space is less than the specified quantity. Select to enable (default). Clear to disable. Enter the minimum disk space and unit of measure (Default is 5GB)
- **Run the following script before cleanup** - Enter a predefined script to run before the cleanup starts.
- **Send Alert when free disk space is below** - Send an alert when available disk space is less that the specified quantity. Select to enable (default). Clear to disable.

  Enter the minimum disk space and unit of measure (Default = 3 GB).
- **Daily Log Retention Configuration** - Set a log retention policy, how many days to keep indexed logs or keep for an additional number of days.

Multi-Domain Log Settings - Advanced

What can I do here?

Use this window to set logging options.

Getting Here - Getting Here - Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > New > Multi-Domain Server > Log Settings > Advanced
Or:
SmartConsole for Multi-Domain Server > Multi Domain > New > Multi-Domain Log Servers > Log Settings > Advanced

Log Management Advanced Settings

Configure these settings:

- **General** - Configure whether to accept syslog messages and when to stop logging (according to free disk space).
- **Log Files** - Set the threshold, in terms of file size, for creating a new log.

Domain Editor - General

What can I do here?

Use this window to create new Domains and change existing Domain configuration.

Getting Here - SmartConsole for Multi-Domain Server > MDS > Domains > New > Domain

Domain Servers - General

Settings and Parameters:

- **Type Object Name** - Enter a unique name for this Domain
- **Type Object Comment** - Optional: Enter a textual description or comment for this Multi-Domain Server
- **+** - Add a new a domain to the list of Domains assigned to this Global Domain
- **X** - Remove a Domain from list of Domains assigned to this Global Domain

Creating a New Domain

Use this procedure to create a new Domain together with the first Domain Management Server for this Domain.

To create a new Domain:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Multi-Domain** > **Domains** view, click **New**.

3. In the **Domain** window, enter a unique Domain name.
4. Click the **+** icon in the **General** > **Domain Servers** section.

   In a High Availability deployment, you must select a Multi-Domain Server from the list.

   a. Enter a unique Domain Management Server name or accept the default name.

   b. Enter the Domain Management Server IP address, or click **Resolve IP** to get the IP Address from the Multi-Domain Server address pool.

   c. Accept the default Domain Management Server type and click **OK**.

   d. Click **Trusted Clients** and select one or more trusted clients from the list that can connect to this Domain Management Server.

   e. Optional: Click **Additional Information** and enter contact information for the person responsible for this Domain Management Server.
5. Click **OK** to save the new Domain and Domain Management Server.

Notes :

- When you create a new Domain, you must always create at least one new Domain Management Server with it.
- You can also use this procedure to create Standby Domains and Domain Management Servers for Domain Management Server for redundancy and Load Sharing. To do this, there must be at least one Secondary Multi-Domain Server in the deployment.
- To create a Log Server, you must have a Multi-Domain Log Server or a Secondary Multi-Domain Server in your environment. .

Assigning Trusted Clients to Domains

You must assign all Domains to one or more trusted SmartConsole clients before you can connect to them. If you do not do this, an error message will show when you try to connect.

Each Domain assignment identifies trusted SmartConsole clients based on one of these criteria:

- An IP address
- A host name
- A range of IP addresses
- Net mask
- IP addresses with wildcard characters
- **Any** - All SmartConsole clients can connect

To assign a trusted client to a Domain:

1. Connect to the Multi-Domain Server with SmartConsole
2. Select **Multi-Domain** > **Permissions & Administrators** > **Trusted Clients**.
3. Click **New**.
4. In the **New Trusted Client** window, enter a unique name for this Domain assignment.
5. Select an identification criterion from the **Type** list and enter the applicable information.
6. Add one or more Domains to the **Domain Assignment** list.
7. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.

To add another Domain to an existing trusted client:

1. Select **Multi-Domain > Permissions & Administrators > Trusted Clients**.
2. Double-click the trusted client name.
3. In the **Trusted Client** window, add one or more Domains to the **Domains Assignment** list.

To change a Domain assignment:

1. Select **Multi-Domain** > **Permissions & Administrators** > **Trusted Clients**.
2. Double-click an existing trusted client name.
3. Select an identification criterion from the **Type** list and enter or change the applicable information.
4. Add or delete one or more Domains in the **Domain Assignment** list.
5. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.

Changing an Existing Domain Configuration

To change an existing Domain configuration:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Multi-Domain** > **Domains** view, double-click the applicable Domain.
3. In the **Domain** window, select the Domain Management Server and click the pencil icon (edit).

Note - You cannot change the Domain name. If you try to do this, an error message shows.

4. Add, delete or change the other Domain definitions as necessary.

Deleting a Domain

To delete a Domain:

1. In the **Domains** section, right-click a Domain.
2. Select **Delete** from the context menu.

This action automatically deletes the active and secondary Domain Management Servers, Domain Log Servers, and the Domain object.

Deleting a Domain Management Server

To Delete a Domain Management Server:

1. Connect to the Multi-Domain Server with SmartConsole and go to the **Domains** view.
2. Right-click a Domain Management Server in the grid, and then select **Delete**.

Creating a New Domain Management Server for an Existing Domain

You can add another Domain Management Server to an existing Domain on a different Multi-Domain Server. Typically, this is a standby Domain Management Server in a High Availability environment. A Domain can have only one Domain Management Server on each Multi-Domain Server.

To create a new Domain Management Server for an existing Domain, follow the procedure in Adding a Secondary Domain Management Server, which is in the *Working with High Availability* chapter.

Global Assignments View

What can I do here?

Use this window to:

- Configure and manage Global Domains
- Assign Domain Management Servers to Global Domains
- Connect to SmartConsole for Domain Management Servers or Global Domains

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Global Assignments

The Global Domain

The **Global Domain** is a collection of rules, objects and settings shared with all Domains or with specific Domains. The system automatically creates the Global Domain when you install Multi-Domain Security Management. You cannot delete the Global Domain.

You organize global rules, objects and settings into *global configurations*. Each global configuration can include one or more of these components:

- One **Global Access Control Policy** - Global rules that control access to network resources. This includes rules for Firewall, Application Control , URL Filtering , and IPsec VPN. The **Network** Policy Layer is created automatically after installation or upgrade. You can manually create an Application or other Global Policy Layers as necessary.
- One **Global Threat Prevention Policy** - Global rules that prevent malware, intrusions and other threats. This includes rules for IPS, Anti-Bot, Anti-Virus, and other Threat Prevention features. The Threat Prevention Policy Layer is created automatically after installation or upgrade.
- **Global Objects** - System objects and configuration settings that are common to all or to specific Domains. Connect to the Global Domain with SmartConsole to create and configure global objects.

Connecting to the Global Domain

To connect to the Global Domain:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Domains** view, right-click the Global Domain, and then click **Connect to Domain**.

   A SmartConsole instance opens for the Global Domain.

Changing the Global Domain

This section includes basic procedures for working the contents of the Global Domain.

When connected to the Global Domain you can:

- Create, delete or change Global Access Control and Threat Prevention Policies.
- Create, delete or change rules in Global Policies.
- Create, delete or change global objects.

These activities are not supported in this release:

- Create a new Global Domain.
- Define Security Gateways as installation targets in global configuration rules. You must use local Policies to do this.

Working with Global Configuration Rules

This section is a general overview of the procedure for defining rules in the Global Policies. To learn more about Policy rules and their configuration procedures, see the *R81.10 Security Management Administration Guide*

Global Policy Layers have one placeholder for local Domain rules. You can create global rules above and below this placeholder. In the local Domain Policy Layer, you define local rules in the placeholder. If there are no local Domain rules, the placeholder can be empty.

The position of rules in Domain Policy Layers defines the order in which they are enforced. It is important to put rules in the correct sequence. Global Policy Layers do not have implied rules, but implied rules can be inherited from global properties in local Domains.

Best Practice - Define a global cleanup rule in each Policy Layer.

There is no NAT Rule Base in the Global Domain and you cannot define NAT settings there. You must define NAT rules manually in Domain Policy Layers.

Workflow for global Domain Policy Layers:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Domains** view, right-click the Global Domain, and then click **Connect to Domain**.

   A SmartConsole instance opens for the Global Domain.
3. Select **Access Control** and **Threat Prevention Policy Layers** and configure their rules.
4. Publish the SmartConsole session.
5. Go to **Multi-Domain** > **Global Assignments**, and assign the configuration to the local Domains. If you assigned the configuration before, and made changes to the Global Domain Policy, reassign the global domain configuration to the local Domains.

   The system creates a task, during which these actions occur:

   - Makes sure that all Global and local Domain Layer rules are consistent and work together correctly. For example, it makes sure that new local Policy Layers are connected to existing local Domain Policy Layers.
   - Updates the local Domain and its Rule Base.
   - Publishes the changes again.
   - Changes the assignment status to **Up to Date**.
6. Install Policies on the local Domains.

Working with Global Objects

Use global objects in global configuration rules. Global objects work much in the same way as objects in local Policy rules.

The Global Domain includes many, predefined global objects for your convenience. These default global objects are visible (read only), in the Global Domain. You cannot delete or change them.

You can create, change or delete user-defined global objects in the Global Domain only. Global objects are visible in local Domains in the read-only mode.

Important - Before you delete a global object, make sure that no global or local policy rules use this global object. This can cause errors when you reassign global configurations.

To add a new global object:

1. Connect to the Global Domain with SmartConsole.
2. Click the **Objects** menu, and then select an object type from the menu.

   You can also create a new global object with the **Object Explorer**.
3. Configure the required parameters.
4. Click **OK** to save the new object.

To change a user-defined global object, select it in the **Object Explorer**, and then change the applicable settings.

To delete a user-defined object, select it in the **Object Explorer** and click **Delete**.

Important - After you complete the global object task, reassign the global configuration to the applicable Domains.

This action automatically:

- Publishes the changes that were done on the Multi-Domain Server
- Updates the local Domain and its Rule Base

Updating IPS Protections

Check Point continuously develops and improves its protections against emerging threats. You can manually update the database with latest IPS protections. You must also configure the Global Domain to automatically download contracts and other important data.

Note - Security Gateways with IPS enabled only get the updates after you install Policy.

For troubleshooting or for performance tuning, you can revert to an earlier IPS protection package.

To manually update the IPS protections:

1. Connect to the Global Domain with SmartConsole.
2. Click **Security Policies** > **Threat Prevention**.
3. In the **Related Tools** section, click **Updates**.
4. In the **IPS** section, click **Update Now**.
5. Connect to the Multi-Domain Server with SmartConsole.
6. Reassign the global configuration.

To revert to an earlier protection package:

1. Connect to the Global Domain with SmartConsole.
2. Click **Security Policies** > **Threat Prevention**.
3. In the **IPS** section of the **Threat Prevention Updates** page, click **Switch to version**.
4. In the window that opens, select an **IPS Package Version**,.
5. Click **OK**.
6. Connect to the Multi-Domain Server with SmartConsole.
7. Reassign the global configuration.

To make sure that Contract Downloads is enabled:

1. In each Domain, go to the main menu > **Global Properties**.
2. From the navigation tree, select **Security Management**.
3. Make sure that **Automatically download contracts and other important data** is selected.

   This parameter is enabled by default. If it is not enabled, select it.

Updating the Application and URL Filtering Database

Check Point constantly develops and improves its protections against the latest threats. You can manually update the Application and URL Filtering database with the latest applications and URLs.

To manually update the Application and URL Filtering protections:

1. Connect to the Global Domain with SmartConsole.
2. Click **Security Policies** > **Access Control**.

3. In the **Related Tools** section, click **Updates**.
4. In the **Application and URL Filtering** section, click **Update Now**.
5. Connect to the Multi-Domain Server with SmartConsole.
6. Assign or reassign the global configuration.

Global Assignment - Remove or Reassign.

What can I do here?

Use this window to:

- Reassign or Remove global assignments
- Install policies after a successful assignment

> **Getting Here** - SmartConsole for Multi-Domain Server > Multi Domain > Global Assignments > Remove/Reassign

Global Assignment - Reassign Install Mode

What can I do here?

Use this window to select the install mode.

- Install on each selected gateway independently
- Install on all selected gateways

> **Getting Here** - SmartConsole for Multi-Domain Server > Multi Domain > Global Assignments > Reassign > Install Policy > Configure

Install Policy Presets

What can I do here?

Use this window to create, delete, or edit a policy preset.

> **Getting Here** - SmartConsole for Multi-Domain Server > Multi Domain > Install Policy Presets

SmartConsole lets you create Policy Presets for better policy installation planning. A Policy Preset is a collection of Security Gateways or Policy Packages for policy installation purposes. After you define a Preset, you can install policy on all the items which are included in the Preset at the same time. You also have the option to define a policy installation schedule for a specific Preset. In a large deployment Multi-Domain Server environment, Policy Presets help you save time and manage the policy installation process more efficiently.

You can create 2 types of Policy Presets:

- **By Gateways** - Policies are installed on all Security Gateways in the Preset. The applicable policy is installed on each Security Gateway in the Preset. A Preset can include Security Gateways from different Domains, from the same Domain, Security Gateways with different policies or identical policies.
- **By Policy Packages** - All Policy Packages included in the Preset are installed on the Security Gateways that enforce it at the same time.

Note - A Preset by Policy Packages installs policy only on Security Gateways which enforce the selected Policy Packages included in the Preset. It does not necessarily install policy on all Security Gateways in a Domain.

You can use Presets for policy installation only after you installed policy on the installation targets for the first time. Security Gateways with no policy installed on them are skipped during the installation process.

To create a Policy Preset:

1. In the Multi-Domain view, go to **Multi-Domain** > **Install Policy Presets** > **New**.
2. In **Installation Targets**, select one of these options:
   - **By Gateways** - This Policy preset is installed on the Security Gateways that you select.
   - **By Policy Packages** - This Policy preset is installed on the Security Gateways which enforce the selected Policy Packages.
3. In **Scheduling**:

   You can schedule the policy installation to specific days and hours.

   The hour of the policy installation is set to the time zone of:

   - The SmartConsole client - for a one-time installation.
   - The Multi-Domain Management Server - for a recurring installation.

Use Case - Time Set for a Recurring Installation

In a one time installation, the installation time is according to the SmartConsole client. In a recurring installation, the installation time is according to the Multi-Domain Server. This affects how you set both the hour and the day on your local SmartConsole client.

Example 1:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 2 PM Israel time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 14:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 2 PM New York time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 21:00**

  Recurrence > **Configure** > **Days in week** > **Saturday**

Example 2:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 6 PM Israel time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 18:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 6 PM New York time (18:00):

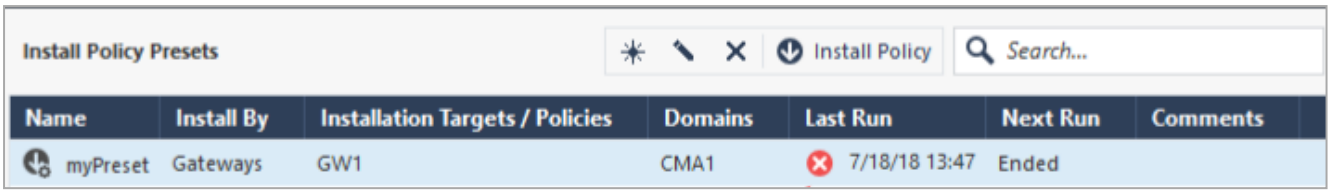
  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 01:00**

  Recurrence > **Configure** > **Days in week** > **Sunday**

Note - The hour of the policy installation is set to the time zone of:
- The SmartConsole client - for a one-time installation.
- The Multi-Domain Management Server - for a recurring installation.

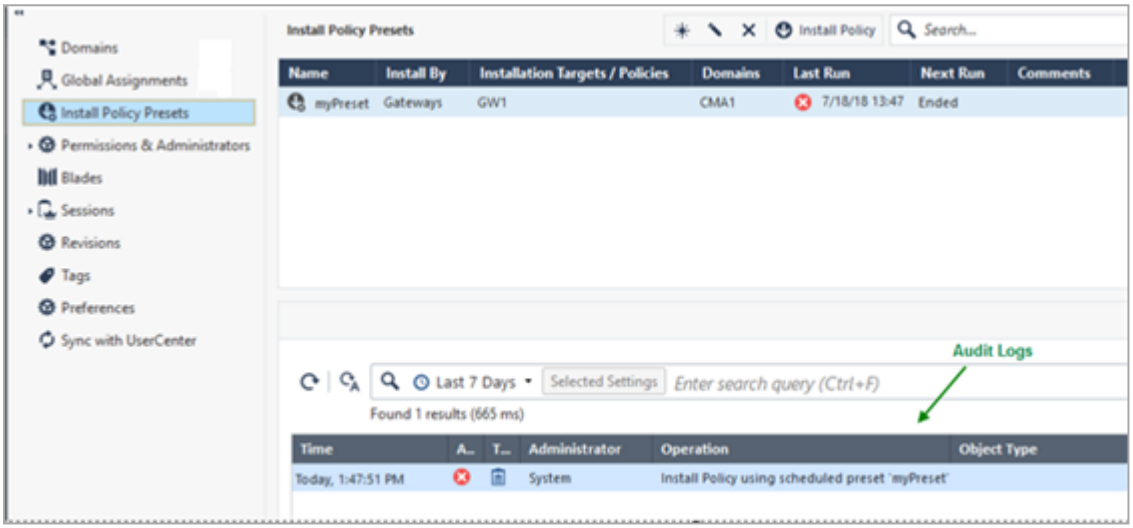
4. Publish the SmartConsole session.

You can see the next policy installation schedule in the **Next Run** column:



At any time, you can select a Preset and click **Install Policy**, regardless of the preset schedule.

The audit logs of your Preset activity show at the bottom of the **Install Policy Presets** page and in the Logs & Monitor view.



Note - The policy preset is installed on the Multi-Domain Server with the active global Domain. If a domain has no domain server on the Multi-Domain Server with the active global Domain, then the policy preset is not installed on this Domain.

Use Case - Installation on multiple Multi-Domain Servers

In this example, the Global policy will not be installed on Domain 2, because Domain 2 has no server in Multi-Domain Server2.

Servers Domains	Multi-Domain Server 1	Multi-Domain Server 2
Domain1	Domain1_Server (Active)	Domain1_Server_2 (Standby)
Domain2	Domain2_Server (Active)	No Server
Global	Standby	Active

Use Case - Time Set for a Recurring Installation

In a one time installation, the installation time is according to the SmartConsole client. In a recurring installation, the installation time is according to the Multi-Domain Server. This affects how you set both the hour and the day on your local SmartConsole client.

Example 1:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 2 PM Israel time (14:00):

  In your SmartConsole client > **New Install Policy Preset**> **Scheduling**, select:

  Install policy at 14:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 2 PM New York time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 21:00**

  Recurrence > **Configure** > **Days in week** > **Saturday**

Example 2:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 6 PM Israel time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 18:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 6 PM New York time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 01:00**

  Recurrence > **Configure** > **Days in week** > **Sunday**

Use Case - Mail Security Servers

You are the administrator for a corporation that has five branches, each branch in a different city. You manage the Security Gateways from a Multi-Domain console. In the Multi-Domain console, each branch is represented by a Domain. Each Domain has a mail security server. When there is a mail-related update, you must update the policy on all mail security servers (no update is required for the other Security Gateways in each Domain). How can you make the policy installation process more efficient?

Create a Preset which includes the mail security server in each Domain. After you create this Preset, each time it is necessary to update the Policy on the mail security servers, you can select this preset for installation. This way, you do not need to search and filter for each mail security server separately.

You can also schedule the policy installation for specific days and hours, for example, in the evening hours, when there are fewer employees at work.

Install Policy Preset

What can I do here?

Use this window to select installation targets for policy presets and schedule installations.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Install Policy Presets > New/edit

Policy Presets

SmartConsole lets you create Policy Presets for better policy installation planning. A Policy Preset is a collection of Security Gateways or Policy Packages for policy installation purposes. After you define a Preset, you can install policy on all the items which are included in the Preset at the same time. You also have the option to define a policy installation schedule for a specific Preset. In a large deployment Multi-Domain Server environment, Policy Presets help you save time and manage the policy installation process more efficiently.

You can create 2 types of Policy Presets:

- **By Gateways** - Policies are installed on all Security Gateways in the Preset. The applicable policy is installed on each Security Gateway in the Preset. A Preset can include Security Gateways from different Domains, from the same Domain, Security Gateways with different policies or identical policies.
- **By Policy Packages** - All Policy Packages included in the Preset are installed on the Security Gateways that enforce it at the same time.

Note - A Preset by Policy Packages installs policy only on Security Gateways which enforce the selected Policy Packages included in the Preset. It does not necessarily install policy on all Security Gateways in a Domain.

You can use Presets for policy installation only after you installed policy on the installation targets for the first time. Security Gateways with no policy installed on them are skipped during the installation process.

To create a Policy Preset:

1. In the Multi-Domain view, go to **Multi-Domain** > **Install Policy Presets** > **New**.
2. In **Installation Targets**, select one of these options:
   - **By Gateways** - This Policy preset is installed on the Security Gateways that you select.
   - **By Policy Packages** - This Policy preset is installed on the Security Gateways which enforce the selected Policy Packages.
3. In **Scheduling**:

   You can schedule the policy installation to specific days and hours.

   The hour of the policy installation is set to the time zone of:

   - The SmartConsole client - for a one-time installation.
   - The Multi-Domain Management Server - for a recurring installation.

   Use Case - Time Set for a Recurring Installation

   In a one time installation, the installation time is according to the SmartConsole client. In a recurring installation, the installation time is according to the Multi-Domain Server. This affects how you set both the hour and the day on your local SmartConsole client.

   Example 1:

   Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

   - You want to schedule a recurring installation on Saturday 2 PM Israel time (14:00):

     In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

     Install policy at 14:00

     Recurrence > **Configure** > **Days in week** > **Saturday**
   - You want to schedule a recurring installation on Saturday 2 PM New York time (14:00):

     In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 21:00**

     Recurrence > **Configure** > **Days in week** > **Saturday**

   Example 2:

   Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 6 PM Israel time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 18:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 6 PM New York time (18:00):

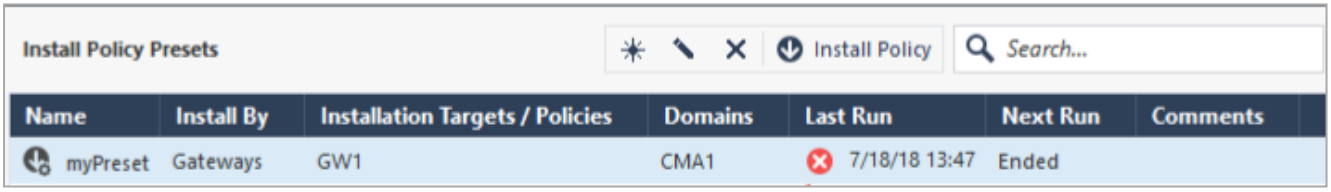
  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 01:00**

  Recurrence > **Configure** > **Days in week** > **Sunday**

Note - The hour of the policy installation is set to the time zone of:
- The SmartConsole client - for a one-time installation.
- The Multi-Domain Management Server - for a recurring installation.

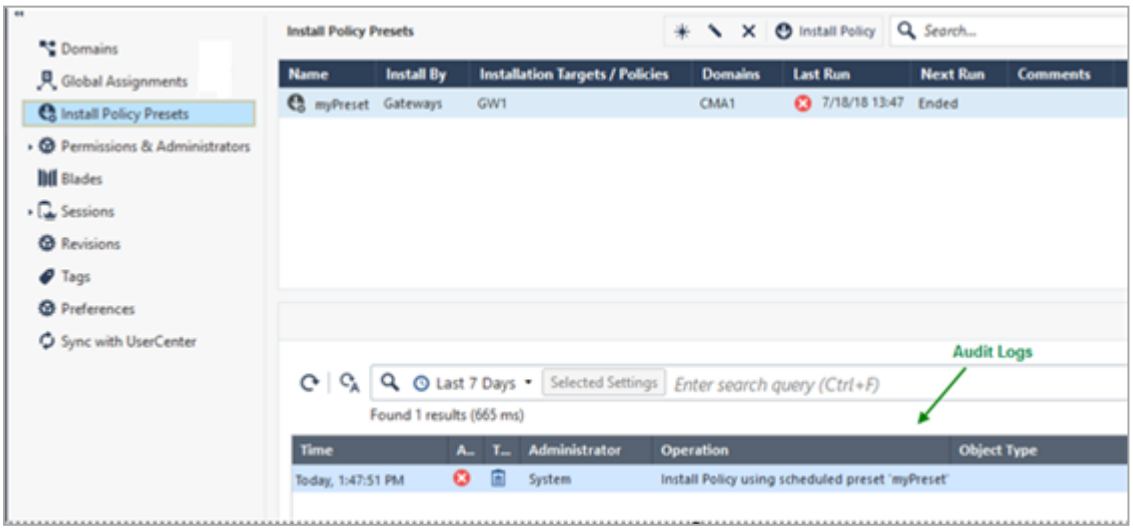
4. Publish the SmartConsole session.

You can see the next policy installation schedule in the **Next Run** column:



At any time, you can select a Preset and click **Install Policy**, regardless of the preset schedule.

The audit logs of your Preset activity show at the bottom of the **Install Policy Presets** page and in the Logs & Monitor view.



Note - The policy preset is installed on the Multi-Domain Server with the active global Domain. If a domain has no domain server on the Multi-Domain Server with the active global Domain, then the policy preset is not installed on this Domain.

Use Case - Installation on multiple Multi-Domain Servers

In this example, the Global policy will not be installed on Domain 2, because Domain 2 has no server in Multi-Domain Server2.

Servers Domains	Multi-Domain Server 1	Multi-Domain Server 2
Domain1	Domain1_Server (Active)	Domain1_Server_2 (Standby)
Domain2	Domain2_Server (Active)	No Server
Global	Standby	Active

Use Case - Time Set for a Recurring Installation

In a one time installation, the installation time is according to the SmartConsole client. In a recurring installation, the installation time is according to the Multi-Domain Server. This affects how you set both the hour and the day on your local SmartConsole client.

Example 1:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 2 PM Israel time (14:00):

  In your SmartConsole client > **New Install Policy Preset**> **Scheduling**, select:

  Install policy at 14:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 2 PM New York time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 21:00**

  Recurrence > **Configure** > **Days in week** > **Saturday**

Example 2:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 6 PM Israel time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 18:00

Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 6 PM New York time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 01:00**

  Recurrence > **Configure** > **Days in week** > **Sunday**

Use Case - Mail Security Servers

You are the administrator for a corporation that has five branches, each branch in a different city. You manage the Security Gateways from a Multi-Domain console. In the Multi-Domain console, each branch is represented by a Domain. Each Domain has a mail security server. When there is a mail-related update, you must update the policy on all mail security servers (no update is required for the other Security Gateways in each Domain). How can you make the policy installation process more efficient?

Create a Preset which includes the mail security server in each Domain. After you create this Preset, each time it is necessary to update the Policy on the mail security servers, you can select this preset for installation. This way, you do not need to search and filter for each mail security server separately.

You can also schedule the policy installation for specific days and hours, for example, in the evening hours, when there are fewer employees at work.

Install Policy Presets - Recurrence

What can I do here?

Use this window to schedule when the installation of a policy preset should repeat.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Install Policy Presets > New/edit > Scheduling > Recurrence

You can schedule the policy installation to specific days and hours.

The hour of the policy installation is set to the time zone of:

- The SmartConsole client - for a one-time installation.
- The Multi-Domain Management Server - for a recurring installation.

Use Case - Time Set for a Recurring Installation

In a one time installation, the installation time is according to the SmartConsole client. In a recurring installation, the installation time is according to the Multi-Domain Server. This affects how you set both the hour and the day on your local SmartConsole client.

Example 1:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 2 PM Israel time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 14:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 2 PM New York time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 21:00**

  Recurrence > **Configure** > **Days in week** > **Saturday**

Example 2:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 6 PM Israel time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 18:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 6 PM New York time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 01:00**

  Recurrence > **Configure** > **Days in week** > **Sunday**

Domain - Trusted Clients

What can I do here?

Use this window to select SmartConsole clients trusted to manage the domain.

To create a trusted client, see: *"Trusted Client - General" on page 448*

Getting Here - SmartConsole for Multi-Domain Server > MDS > Domains > New > Domain > Trusted Clients

Assigning Trusted Clients to Domains

You must assign all Domains to one or more trusted SmartConsole clients before you can connect to them. If you do not do this, an error message will show when you try to connect.

Each Domain assignment identifies trusted SmartConsole clients based on one of these criteria:

- An IP address
- A host name
- A range of IP addresses
- Net mask
- IP addresses with wildcard characters
- **Any** - All SmartConsole clients can connect

To assign a trusted client to a Domain:

1. Connect to the Multi-Domain Server with SmartConsole
2. Select **Multi-Domain** > **Permissions & Administrators** > **Trusted Clients**.
3. Click **New**.
4. In the **New Trusted Client** window, enter a unique name for this Domain assignment.
5. Select an identification criterion from the **Type** list and enter the applicable information.
6. Add one or more Domains to the **Domain Assignment** list.
7. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.

To add another Domain to an existing trusted client:

1. Select **Multi-Domain > Permissions & Administrators > Trusted Clients**.
2. Double-click the trusted client name.
3. In the **Trusted Client** window, add one or more Domains to the **Domains Assignment** list.

To change a Domain assignment:

1. Select **Multi-Domain** > **Permissions & Administrators** > **Trusted Clients**.
2. Double-click an existing trusted client name.
3. Select an identification criterion from the **Type** list and enter or change the applicable information.
4. Add or delete one or more Domains in the **Domain Assignment** list.
5. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.

Domain - Additional Info

What can I do here?

Use this window to add contact details for the domain.

Getting Here - SmartConsole for Multi-Domain Server > MDS > Domains > New > Domain > Additional

New Global Assignment

What can I do here?

Use this window to configure a new Global assignment.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Global Assignments > Assign > New Assignment

Global Assignments

A *global assignment* is a Multi-Domain Security Management system object that assigns a global configuration to one specified Domain. You create global assignments to assign different combinations of Global Access Control Policies, Global Threat Prevention Policies, and global object definitions to different Domains.

When you create a new global assignment, it automatically assigns the specified global configuration to the specified Domain. It also publishes the assignment and updates local Domain Policies.

Best Practice - When you create a new Domain, create a global assignment for that Domain at the same time.

When you do one or more of these actions, you must publish the Global Domain session and *reassign* the global configuration:

- Add, delete, or change rules in a global configuration
- Add, delete, or change user-defined objects in a global configuration
- Define the SmartEvent object in the global database
- Change the definition of a global assignment

The assign/reassign action does not automatically install Policies.

Best Practice - Install Policies after you assign or reassign a global assignment.

New Global Assignment

Settings and Parameters:

Global Domain Assignment

- **Global Domain** - Select a Global Domain from the list.
- **Domain** - Select a Domain to assign to the Global Domain.

Access Control

- **Global Access Policy** - Select an Access Control Policy for this assignment.

Threat Prevention

- **Global Threat Prevention Policy** - Select a Threat Prevention Policy for this assignment.
- **Manage protection actions** - Selecting this options aligns the IPS version of the local domain with the IPS version of the Global domain. Protection activations on the Global domain are applied to local domain activations - except for those deliberately overridden.

  Note - If the local domain has a higher IPS version than the global domain, the assignment operation fails. To resolve, run IPS update on the global domain and try again.

Global Assignment - Access Control / Threat Prevention - Advanced

What can I do here?

Use this window to assign a:

- Global Access control/Threat Prevention policy for all the policies in the domain
- Global Access Control/Threat Prevention policy for specific domain policies
- Exclude Access Control/Threat Prevention from the Global Assignment

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Global Assignments > Assign > New Assignment > Access Control / Threat Prevention > Select Global policy> Advanced button.

Global Assignment - Advanced

By default, the Global Access Control or Threat Prevention Policy is automatically selected for a global configuration. You can optionally click **Advanced** to open the **Advanced Assignment** window and assign these Policies:

- Only to the specified, local Domain Policies
- To all local Domain Policies, except for those explicitly specified

Administrators Accounts

What can I do here?

Use this window to create or edit an administrator account.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Administrators > New, or edit existing account.

Administrator - General

Authentication

- **Name** - Enter a unique administrator name.
- **Authentication Method** - Select an authentication method and enter other authentication parameters as necessary. To learn more about the various authentication methods, see the *R81.10 Security Management Administration Guide*

  To set a default value for this parameter, go to **Permissions & Administrators** > **Advanced** > **Administrator Settings** > **Authentication Default Values**. Select a default authentication from the list.
- **Certificate Information** - Optional: Click **Create** to generate a new certificate.

- You can use a certificate with or without an authentication method.
- For an existing administrator definition, you can revoke an existing certificate and create a new one.

Permissions

- **Multi-Domain Permission Profile** - Select a Multi-Domain permission profile from the list.

  Accept the default permission profile or select a different one. You can also create a new permission profile to assign. For an existing administrator, the currently selected permission profile shows.

  Click the **View** icon to see details of the currently assigned permission profile.

  If the **Edit** icon shows, you have permissions to see and change the currently selected permission profile. Click the **Edit** icon to change the settings.

  Permission Profiles per Domain -Select one or more Domains, and then select a Domain permission profile for each one.

  + - Click to select a Domain to add to the profile.

  X - Click to remove the selected Domain from the profile.

  Note - The **Permission Profiles per Domain Section** does not show for Superusers, because Read/Write Domain permission profiles are assigned automatically to all Domains.

- **Expiration** -Define when this administrator account expires.
  - **Never** - The administrator account does not expire.
  - **Expire at** - Select an expiration date for this administrator.

  To set a default value for this parameter, go to **Permissions & Administrators** > **Advanced** > **Administrator Settings** > **Default Expiration Values**.

Contact Options

You can optionally add contact information for this user:

- **Email** - Enter the administrator email address.
- **Contact Details** - Enter additional contact information.
- **Phone** - Enter the administrator telephone number.

Note - If you upgraded from an earlier release, the system copies these values into the new release.

Configuring Administrators

To configure an administrator:

1. Connect to the Multi-Domain Server with SmartConsole, and go to **Permissions & Administrators** > **Administrators**.
2. Click **New**, or select an existing administrator and then click **Edit**.
3. In the **Administrator** view, configure the settings described in the next sections.

Multi-Domain Permission Profile

What can I do here?

Use this window to configure Multi-Domain Permission Profiles.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Permissions & Administrators > Permission Profiles > New > Multi-Domain Permission Profile

Predefined Multi-Domain Permission Profiles

Multi-Domain Security Management includes predefined Multi-Domain and Domain permission profiles that are ready to use. You cannot delete or change these profiles. You can create custom permission profiles as necessary for your environment.

These are the predefined Multi-Domain permission profiles available in this release. In the **Permissions Profile** view, double-click each profile to see the permissions it includes:

Permission Profile	Permissions
Multi-Domain Superuser	Manage all elements of the Multi-Domain Security Management environment, including: Multi-Domain Servers, Multi-Domain Log Servers, Domains, Domain Management Servers, Global Policies, administrators and permission profiles. Multi-Domain Superusers manage all Domain objects, including Security Gateways, Policies, rules, networks and other objects.
Domain Superuser	Manage all Domains, Domain Management Servers, Domain networks, global objects, and global configurations. They manage Domain objects, including Security Gateways, Policies, rules, networks and other objects. Domain Superusers can create and manage other administrators, manage other administrators' sessions, and manage permission profiles at the same or lower levels. Domain Superusers cannot create or change the settings for Multi-Domain Servers or Multi-Domain Log Servers.

Global Manager	Manage Global Domains, global configurations, global rules, and global assignments. Global Managers can manage Domains, but not add or delete domains or manage Multi-Domain Servers. Global managers can manage administrators with equal or lower permissions. Global Managers can create new global assignments and can assign Global Policies to Domains that they have permissions to manage. Domain-Level permissions are based on the assigned Domain permission profile.
Domain Manager	Manage Domain Policies, networks and objects based on their permission profile. Domain Managers can manage administrators with equal or lower permissions. Domain Managers can reassign Global Policies to Domains that they have permissions to manage. They cannot create new global assignments. Domain-Level permissions are based on the assigned Domain permission profile.
Domain Level Only	Manage Domain Policies, networks and objects based on their permission profile. These administrators cannot manage the Multi-Domain Security Management system or its configuration settings, or login to the Multi-Domain Servers. Domain-Level permissions are based on the assigned Domain permission profile.

Pre-Defined Domain Permission Profiles

When you assign an administrator to Domain, you must also assign a Domain Permission Profile. You can assign a predefined Permission Profile or a custom Permission Profile for this administrator.

Permission Profile	Permissions
Read/Write	Read and write permissions for all Domain settings and data without session management or DLP confidential data. The **Read/Write** option lets the administrator see and configure an item.
Read Only	Read only permissions for all Domain data. Read Only lets the administrator see an item, but not change it.

Working with Multi-Domain Permission Profiles

Use this procedure to create or change customized Multi-Domain permission profiles. Only administrators with Superuser permissions can do this.

To create a custom permission profile:

1. Connect to the Multi-Domain Server with SmartConsole, and go to **Permissions & Administrators** > **Permission Profiles**.
2. In the **Permission Profile** page, click **New**.
3. Select **New Multi-Domain Permission Profile**.
4. In the **New Multi-Domain Permission Profile** window, select an administrator role and configure the permission settings. The next section explains the available settings and parameters.

To change an existing Multi-Domain permission profile:

1. Select a permission profile on the **Permission Profiles** page.
2. Click **Edit** and change the administrator role and permission settings as necessary.

To delete an existing Multi-Domain permission profile:

1. Select a permission profile on the **Permission Profiles** page.
2. Click **Delete**.

Multi-Domain Permission Profile Parameters

Multi-Domain Levels

Select an administrator role:

- **Superuser** - Manage all aspects of the Multi-Domain Security Management environment.
- **Manager** - Manage Domains as specified in the **Permissions** section of Administrator definition.
- **Domain Level Only** - Same as Manager, but with no Multi-Domain permissions. .

The selected role affects the permissions that you can configure in the next parts: **Multi Domain Management**, **Global Management**, and **Domain Management**. For example, Superusers always have Domain Management permissions.

Multi-Domain Management Activities

Enable or disable permissions for these activities:

- **MDS Provisioning** - Create and manage Multi-Domain Servers and Multi-Domain Log Servers. Only Superusers can select this option.

- **Manage All Domains** - Create and manage all Domains and Global Domains. This option is enabled by default for Superusers. Managers can select it.
- **Manage Administrators** - Create and manage Multi-Domain Security Management administrators with the same or lower permission level. For example, a Domain manager cannot create Superusers or global managers. This option is enabled automatically for Superusers. Managers can select it.
- **Manage Sessions** - Connect/disconnect Domain sessions, publish changes, and delete other administrator sessions.
- **Management API login** - Lets an administrator log in to the Security Management Server and run api commands using these tools
  - *mgmt_cli*(Linux and Windows binaries)
  - *Gaia CLI*(clish)
  - *Web Services* (REST)

    Useful if you want to *prevent* administrators from running automatic scripts on the Management.

    Note: This permission is not required to run commands from within the API terminal in SmartConsole.
- **Global VPN Management** - Lets the administrator select **Enable global use** for a Security Gateway shown in the MDS **Gateways & Servers** view. (To see the option, right-click on the gateway object).
- **Cloud Management Extension (CME) Operations** - permission to read or read / edit the Cloud Management Extension (CME) configuration.

Global Management Activities

All options are enabled automatically for Superusers. Managers can select them.

- **Manage Global Assignments** - Create, update and delete global assignments.
- **Default profile for all Global Domains** - Change the default permission profile for all global Domains.
- **View global objects in Domains** - Lets an administrator with no global objects permissions view the global objects in the domain. This option is required for valid domain management.

Domain Management

This profile defines the default Domain permissions that automatically apply when you create a new administrator account. After you create the administrator account, you can change its Domain profile as necessary.

Select a default profile from the list. This option is enabled automatically for Superusers, and Managers can optionally select it.

Deleting a Permission Profile

You can only delete customized Permission Profiles.

To delete an existing Permission Profile:

1. In SmartConsole for Multi-Domain Server, select **Multi-Domain > Permission Profiles**.
2. In the **Permission Profile** window, select a profile and then click **Delete**.
3. Click **Yes** to confirm.

Domain Permission Profile - Custom

What can I do here?

Use this window to configure gateway settings for a domain permission profile.

Getting Here - SmartConsole for Multi-Domain Server > Multi Domain > Permission Profiles > New > Domain Permission Profile > Gateways page

Creating Custom Domain Permissions

Customized Domain permission profiles are a set of granular permissions for Domain level activities in SmartConsole.

To configure custom permission profiles:

1. In the **Permission Profiles** window, click **New Domain Permission Profile**.

   The **New Domain Permission Profile** window opens.
2. Configure read/write permissions for each Software Blade, feature, resource, and the API in these categories as necessary:
   - **Overview** -Select default or custom permission options
   - **Gateways** - Work with Security Gateway management tasks and VSX provisioning
   - **Access Control** - Work with Access Control rules and install Access Control Policies
   - **Threat Prevention** - Work with Threat Prevention rules, profiles, and protections. Install Threat Prevention Policies

- **Others** - Work with different features not in other categories
- **Monitoring and Logging** - See and manage logs, monitoring features and related reports
- **Events and Reports** - Work with SmartEvent events, policy and reports
- **Management** - Manage sessions and High Availability options

To prevent administrators from working with an item, clear its option.

Notes :

- You cannot prevent administrators from seeing some resources. You cannot change their options.
- Some resources do not have **Read** or **Write** options. You can only select or clear them.

Multi-Domain Server Task Details - Domain

What can I do here?

Use this window to see the details and progress of the task.

Getting Here - SmartConsole for Multi-Domain Server > Domains > Create or delete a domain > open the task window > click Details

Multi-Domain Server Task Details - New, Reassign or Remove Global Assignment

What can I do here?

Use this window to see the details and progress of the task.

Getting Here - SmartConsole for Multi-Domain Server > Global Assignments > Reassign or remove a global assignment > Open the task window > click Details.
or:

SmartConsole for Multi-Domain Server > Global Assignments > New assignment > Open task window > click Details.

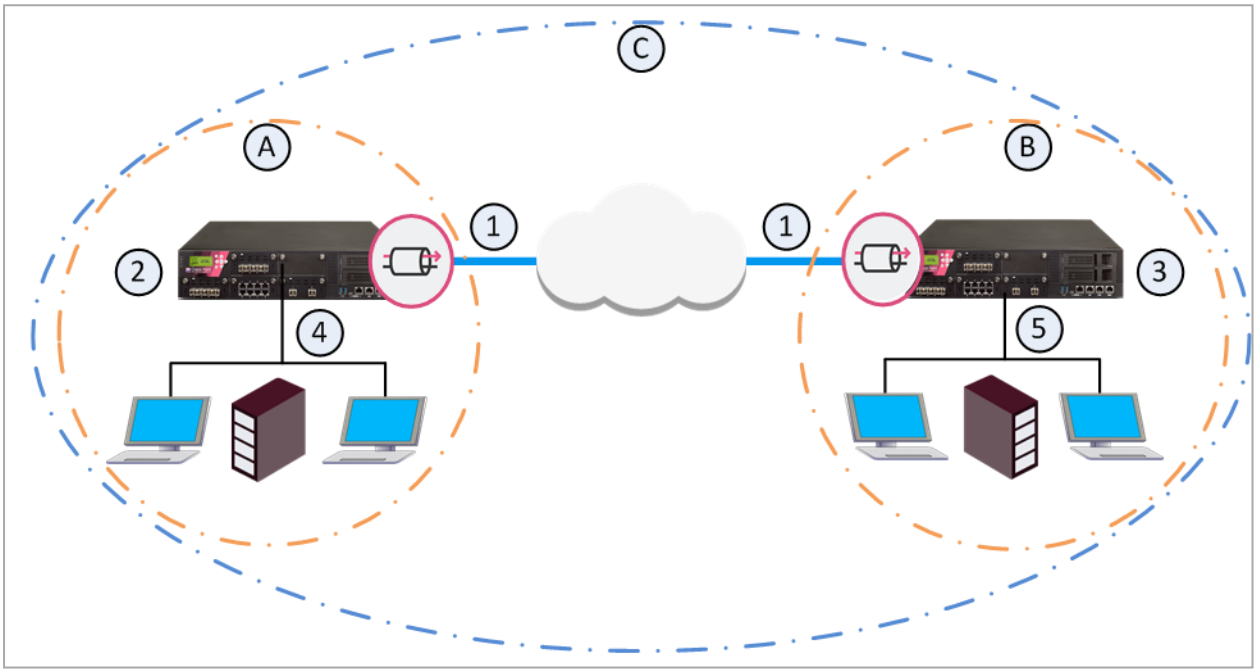
VPN and Multi-Domain Security Management

This section covers the configuration of Global VPN communities.

Global VPN Communities

Large enterprises often have branches in different cities or countries. With each branch managed by a different Domain, the enterprise can use a central management system to centrally manage all the various Domains. When connectivity is established, the connections must be secure and have high levels of privacy, authentication, and integrity.

A Global VPN Community connects the enterprise's Security Gateways through VPN and lets the enterprise manage them under one network. You define the Global VPN Community in the Global Domain. The Multi-Domain Server utilizes its knowledge about the different Domain Management Server environments to create a VPN community which can manage them.



Item	Description
A	Domain A on Multi-Domain Server
B	Domain B on Multi-Domain Server
C	Global VPN Community
1	VPN tunnel
2	Security Gateway configured in Domain A
3	Security Gateway configured in Domain B
4	VPN Domain of Security Gateway 2
5	VPN Domain of Security Gateway 3

VPN Connectivity

When you establish a Global VPN Community, it replaces part of the configuration of Externally Managed Security Gateways and automates the exchange of certificates for each Domain Management Server.

These trusted entities create VPN trust in a Multi-Domain Security Management deployment:

- Certificates issued by a Domain Management Server Internal Certificate Authority (ICA).
- External third party Certificate Authority servers (using OPSEC connectivity).
- Pre-shared secrets.

The ICA of the Domain Management Server issues certificates used by Domain Security Gateways to create SIC trust. Each Security Gateway supports certificates issued by the CAs of the other Domains.

Configuring Global VPN Communities

Workflow for Creating a Global VPN Community

To create a Global VPN Community:

1. Configure a VPN Domain on each participating Security Gateway.
2. Enable each participating Security Gateway for global use.
3. In the Global Domain, define a VPN Community, and add the Global Security Gateway objects to the Global VPN Community. The Global Security Gateway objects represent the participating Domain Security Gateways.
4. Define a Security Policy - You can create a Global policy and assign it to the Local Domains, or you can create the Security Policy rules only in the Local Domains.
5. Assign the Global configuration to the applicable Domains. After assignment, you must also install the policy on the participating Security Gateways.

Step 1 - Configuring a VPN Domain on Each Security Gateway

You define the Domain Security Gateways in the Domain SmartConsole.

To define a VPN Domain on a Security Gateway:

In the Security Gateway editor:

1. In **General Properties**, enable **IPSec VPN**.
2. In **Network Management** > **VPN Domain**, configure the settings for the VPN Domain. You must define a VPN Domain and specify if the VPN Domain is based on the network topology or a specific IP address range.

Multi-Domain Server holds these IP address ranges used by the Security Gateways. During the assignment of the Global configuration, the Multi-Domain Server transfers this information to all the Domains with participating Security Gateways in the Global VPN Community.

Step 2 - Enabling Gateways for Global Use

Repeat this step for all Security Gateways that are to participate in the Global VPN Community:

In the Multi-Domain Server SmartConsole > **Gateways & Servers** view, right-click a Security Gateway and select **Enable Global Use**.

A global Security Gateway object and a VPN Domain object are created for the Security Gateway in the Global Domain. Different Domains can coincidentally contain Security Gateways with the same name. Because each global Security Gateway object must have its own unique **Global Name,** the **Global Names Template** automatically assigns a unique name for each global Security Gateway. The default global name format is: *<Name of Security Gateway>_of_<Name of Domain>*.

For example:

- Security Gateway name = **MyGateway**
- Domain name = **MyDomain**
- Global name = **MyGateway_of_MyDomain**

Enabling clusters for global use

You can enable a cluster for global use in the same way that you enable a Security Gateway. A global cluster object and a VPN Domain object will be created for the cluster in the Global Domain.

Step 3 - Creating the VPN Global Community

After you enabled VPN on the Security Gateways, and enabled the Security Gateways for global use, you can create the Global VPN Community.

To create a Global VPN Community:

1. In the Global Domain, go to **Security Policies** > **Access Control** > **Access Tools** > **VPN Communities** > **New**.
2. Add the global Security Gateway objects, defined in step 1, as participating Security Gateways in the community.

Step 4 - Defining a Security Policy

The configuration of Security Gateways into a Global VPN Community does not automatically let the Security Gateways access each other. For the Security Gateways to communicate with each other you must define an Access Control Security Policy.

You can define the Access Control Security Policy in the Global Domain or in the Local Domains or both.

To define a Global Security Policy, see Global Policy Management.

Step 5 - Assigning the Global Configuration to the Local Domains

After you create the Global VPN Community, and in some case, also the Global Policy, you must assign the Global configuration to the Local Domains. After assignment, install policy on the Local Domains.

To assign the global configuration to the Local Domains:

1. Make sure you published all the changes made in the Global Domain.
2. In the Multi-Domain Server SmartConsole > **Multi-Domain** view > **Global Assignments**, assign the Global objects to the Local Domains
3. Install policy on the Security Gateways.

Note - All Security Gateways which participate in the Global VPN Community must use a Simplified VPN Policy.

For each Domain with Security Gateways in the Global VPN Community, a global **CA Server** object is created in the Global Domain. During the assignment process, the Multi-Domain Server automatically exports relevant Domain ICA information (such as the CA certificate) to all the Domain Management Servers with Security Gateways that participate in the community. This way, all the Security Gateways in the community can trust the others' ICAs.

After the assignment, the Global VPN Community object shows in each Domain with Security Gateways in the community. If you assign a Global Policy to a Domain that has no Security Gateways in the community, this Domain does not show the community object and the community Security Gateway objects.

Reassigning the Global Configuration to One or More Local Domains

If you make changes to the global configuration, reassign the configuration to the Domains.

To reassign the Global configuration to the Local Domains:

1. In the Multi-Domain Server SmartConsole > **Multi-Domain** view > **Global Assignments**, select the Domains that have Security Gateways which participate in the Global VPN Community and click **reassign**.
2. In the **Reassign** window, select **Install policy on successful assignment**. This installs the Global Policy on the Security Gateways which participate in the Global VPN Community.

Note - This operation assigns the Policy to all selected Domains, and then installs the Policy on all Domain Security Gateways, in one step. It does not let you select specific Security Gateways on which to install the Policy. The selected Policy is installed on all Security Gateways in the selected Domains. Assigning the Policy to many Domains and all their Security Gateways can take some time. Use this option with caution.

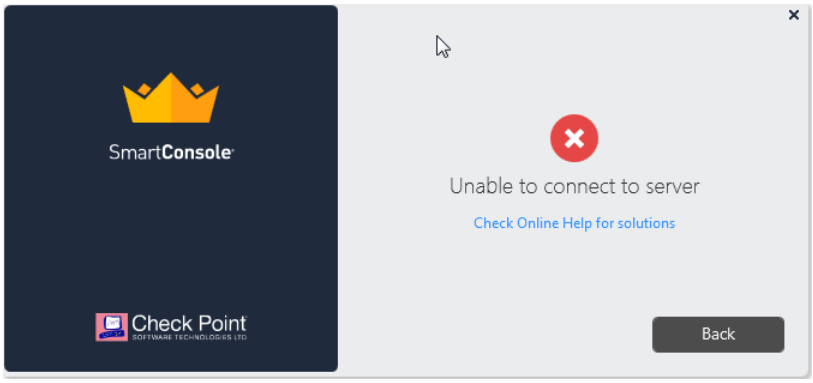
General Troubleshooting

Use the information here to help trouble-shoot SmartConsole issues.

"Unable to Connect to Server" below

"Client Server Mismatch" on page 688

Unable to Connect to Server



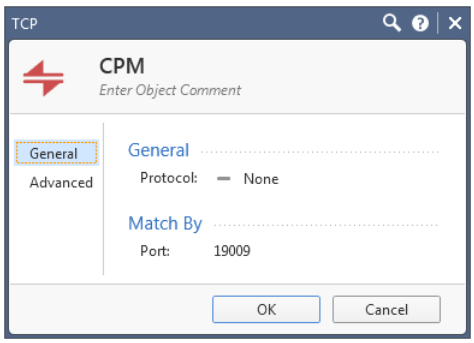
A connection to the management server will fail in these cases:

A Firewall between the computer with SmartConsole installed and the Management Server blocks connections on TCP port 19009

The TCP port 19009 is used for a new service in R80 and higher.

Allow traffic on this port for all clients and Management Servers.

SmartConsole contains the predefined object for the CPM connections on the TCP port 19009:



No GUI clients are assigned

Connect to the Gaia Portal on the Management Server.

- If the First Time Configuration Wizard opens, complete it.
- If the First Time Configuration Wizard has already run, open **User Management > GUI Clients** and add a client.

  Note - When using Multi-Domain Security Management, connect with SmartConsole to the Multi-Domain Server and make sure the Domains have GUI clients assigned to them.

No administrator is defined, or it has insufficient permissions

1. Connect to the command line on the Management Server.
2. Log in to Gaia Clish or the Expert mode.
3. Run this command:
   - On a Security Management Server:

     ```
     cpconfig
     ```

   - On a Multi-Domain Server:

     ```
     mdsconfig
     ```

4. Select the option **Administrators**.
   - If the menu shows "**Do you want to add an administrator (y/n)**", then do so.
   - If the menu shows a defined administrator, then make sure the assigned permissions are sufficient.
5. Exit from the menu.

The required processes are not running

1. Connect to the command line on the Management Server.
2. Log in to the Expert mode.
3. Run this command:

   ```
   cpwd_admin list | grep -v grep | egrep "COMMAND|CPM|FWM"
   ```

4. The output must show these processes:
   - `CPM`
   - `FWM`

5. The output must show "**E**" (means *executing*) in the "**STAT**" column for these processes.

Example output:

```
[Expert@MyMgmtServer:0]# cpwd_admin list | egrep
"COMMAND|CPM|FWM"
APP         PID    STAT   #START   START_TIME              MON
COMMAND
FWM         17704  E      1        [16:41:24] 29/11/2019   N     fwm
CPM         18044  E      1        [16:41:26] 29/11/2019   N
/opt/CPsuite-R81.10/fw1/scripts/cpm.sh -s
[Expert@MyMgmtServer:0]#
```

Operation time out

Your connection to the Management Server (cloud demo or network server) might be slow or blocked.

Check network settings, and try again.

Incompatible SmartConsole

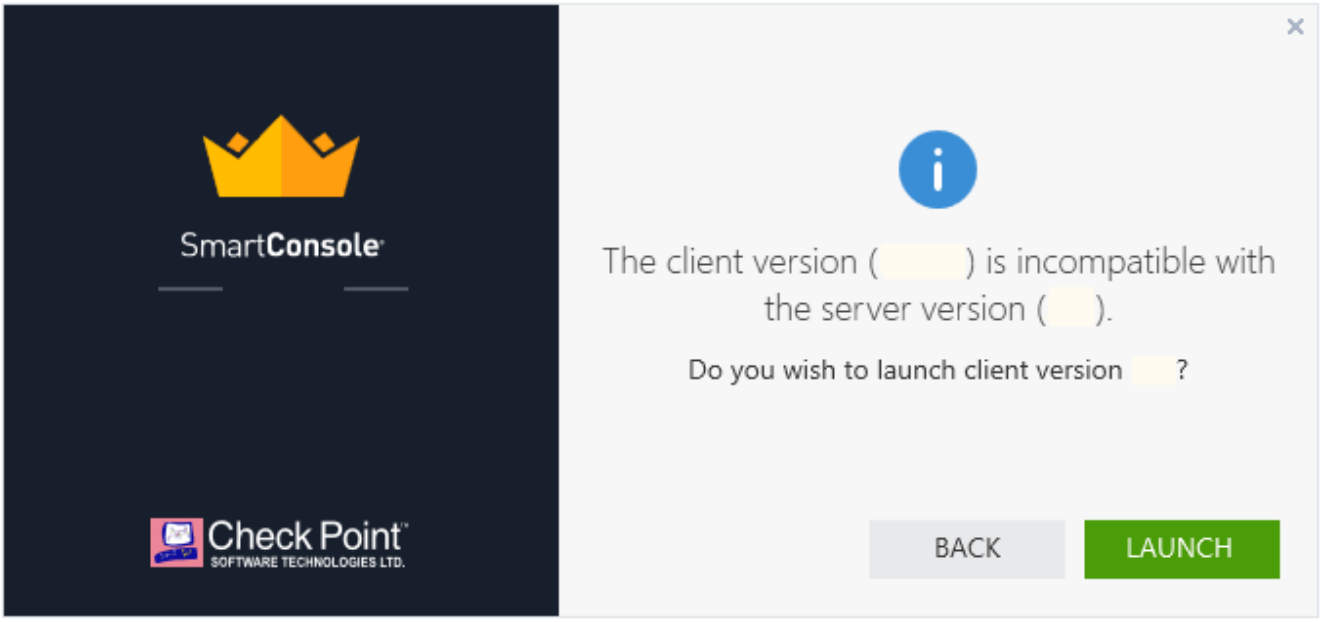
You are trying to use a SmartConsole of version R80 or higher to connect to a management server of R77.30 or lower.

This type of connection is not supported.

For R77.30 and below, use the matching *SmartDashboard* version.

Client Server Mismatch

If you see a message of the type:



Click **Launch** to open the compatible client version or:

- Download the R81.10 client from sk170461
- Download the R81 client from: sk166715
- Download the R80.40 client from: sk160736
- Download the R80.30 client from: sk144293
- Download the R80.20.M1 and R80.20.M2 client from: sk123473
- Download the R80.20 client from: sk122485
- Download the Endpoint Cloud Management client from: sk164415

Blade Deactivation Survey

What can I do here?

Use this window to tell Check Point why you deactivated a blade. You can help us to do better by providing as much detail as possible.

Getting Here - In Gateway Properties > General > disable one or more of the Threat Prevention blades.

Cloud Demo

Cloud Demo lets you test security management features without the need to deploy a Security Management Server.

When you start a new Demo:

- A new exclusive Demo server is created and assigned to you.
- The new Demo server is identified by a Demo ID.
- The Demo ID lets you join an existing Demo at a later time.
- The Demo ID supports multiple users.
- Demo servers are time-limited. After the time period expires, the server is discarded.
- Internet connectivity is required.

For more about the Cloud Demo, see: sk103431

For a list of known limitations, see: sk103431

To run:

1. Open SmartConsole.
2. Select **Demo Mode** in the SmartConsole Login window.
3. Click **Next**.
4. Select one of these:
   - **Start a new demo**
   - **Join existing demo**
5. Click **Login**.

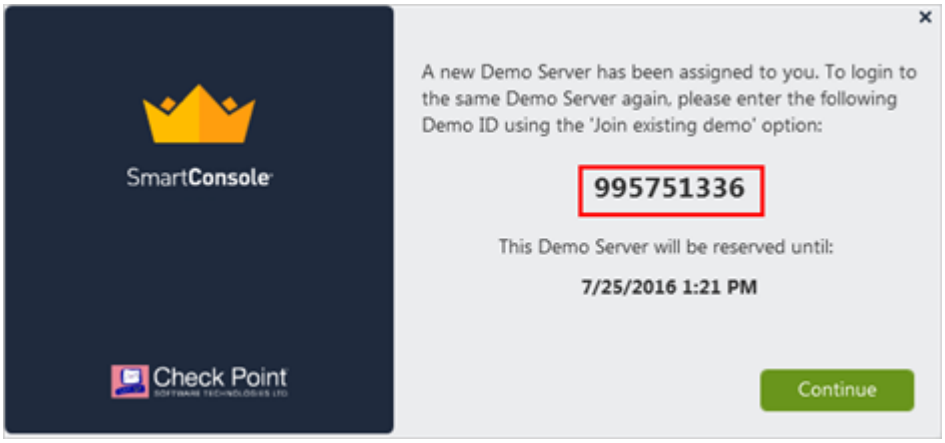
Note - A popup message will inform you when the demo is about to expire.

Starting a New Demo

If you selected **Start a new demo**, a Security Management Server is created and assigned to you.

To log into the same demo server later, enter the Demo ID shown in the window.

Example:



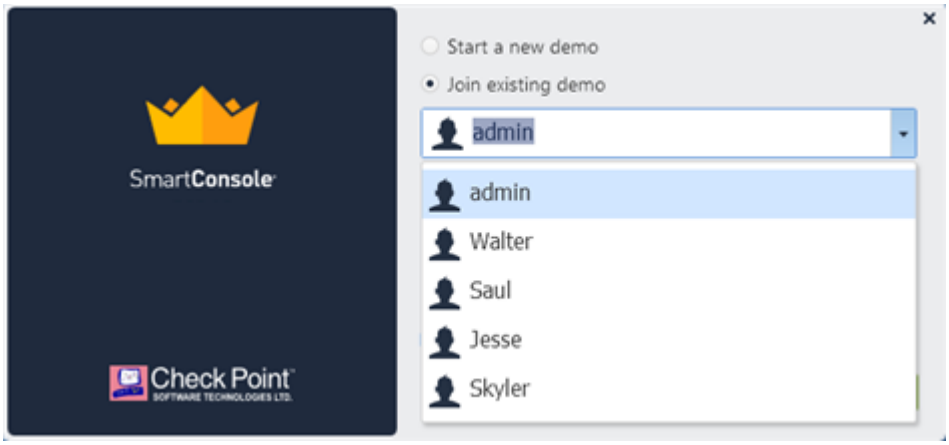
1. Click **Continue**.
2. When the fingerprint shows, click **Proceed**.

Join Existing Demo

To join an existing demo:

1. Select one of the built-in user names.

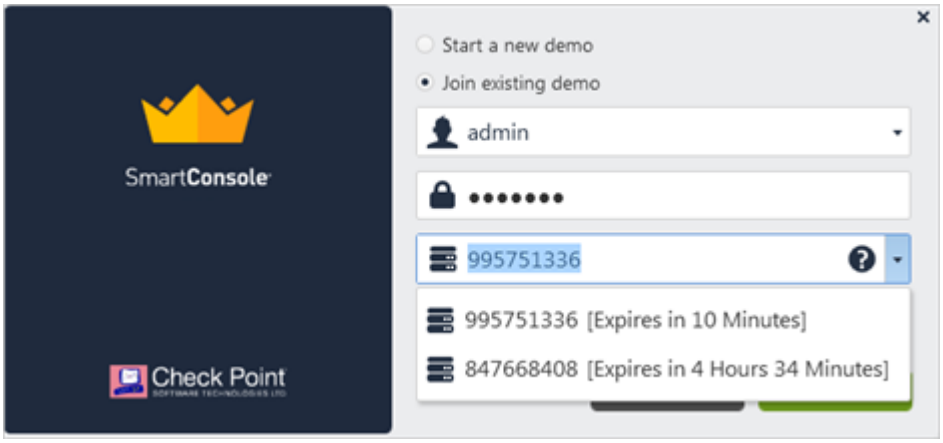
   Example:

   Note - You can also enter a user that you previously created in **Manage & Settings** > **Permissions & Administrators**.

2. Enter a Demo ID or select one from the list.

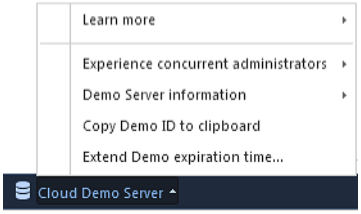
   Example:



3. Click **Login**.

Cloud Demo Menu Options

Clicking Cloud Demo Server opens a number of options.



Cloud Demo Server Option	Description
Learn More	■ Management API Reference A link that opens the API reference guide. ■ Check Point community porta A link that opens the community portal.
Experience concurrent administrators	Lets you connect to the Demo cloud server using a different administrator account.
Demo Server information	Let you copy to the windows clipboard: ■ The server IP address ■ The server host name Use the IP address or DNS host name when testing the Management API. For more about tools available for testing the API, see the *Check Point Management API Reference* (at the top, select the correct version) .

Cloud Demo Server Option	Description
Copy Demo ID to clipboard	Copies the demo ID to the clipboard. Use this option if you want to share the Demo ID with other users.
Extend Demo expiration time	Extends the expiration time (by hours).

Extend Demo Expiration Time

What can I do here?

Use this window to extend the expiration date of the cloud demo server.

Getting Here - Cloud Demo Server menu > Extend Demo expiration time