SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for Check Point Security Gateway
Contents

Third-Party Software Acknowledgement .................................................................................. 5
Description ................................................................................................................................. 5
Applicability ............................................................................................................................... 5
Environment ............................................................................................................................... 5
Audience ..................................................................................................................................... 6
RADIUS-based Authentication using SafeNet Authentication Manager ............................. 6
RADIUS Authentication Flow using SafeNet Authentication Manager ............................... 6
RADIUS Prerequisites .............................................................................................................. 7
Configuring SafeNet Authentication Manager ........................................................................ 7
  Synchronizing Users Stores to SafeNet Authentication Manager ........................................... 7
  Configuring SafeNet Authentication Manager’s Connector for OTP Authentication ........... 8
  Assigning a Token in SafeNet Authentication Manager ......................................................... 8
  Adding Check Point Security Gateway as a RADIUS Client in IAS/NPS ............................ 9
Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client ... 11
Configuring Check Point Security Gateway ........................................................................... 11
  Configuring Check Point Security Gateway for RADIUS Server Authentication ............. 11
  Creating a RADIUS Server Object ....................................................................................... 13
  Creating Networks ................................................................................................................. 14
  Creating a User ....................................................................................................................... 17
  Creating a User Group .......................................................................................................... 18
  Enabling Mobile Access ...................................................................................................... 20
  Setting the Topology ............................................................................................................ 25
  Configuring RADIUS Authentication for Mobile Access ................................................... 29
  Configuring the Office Mode ............................................................................................... 31
  Performing Portal Settings ................................................................................................. 34
  Configuring the Mobile Access Solution ............................................................................. 35
  Configuring the VPN Client Solution .................................................................................. 56
Running the Solution .............................................................................................................. 64
  Using a Web Browser ........................................................................................................... 64
  Using a VPN Client .............................................................................................................. 67
Appendix ................................................................................................................................... 69
  User Authentication with the SafeNet SMS Token ............................................................... 69
  Enabling Identity Awareness Blade ..................................................................................... 69
## Content Index

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring RADIUS Authentication for VPN Client</td>
<td>73</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>82</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>85</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Check Point Security Gateway.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

Check Point Security Gateway (Virtual Edition) protects dynamic virtualized environments and external networks, such as private and public clouds, from internal and external threats by securing virtual machines and applications with the full range of Check Point Software Blades.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Check Point Security Gateway using SafeNet one-time (OTP) tokens managed by SafeNet Authentication Manager.
- Configure Check Point Security Gateway to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the Check Point Security Gateway environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager, and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Check Point Security Gateway can be configured to support multi-factor authentication in several modes. RADIUS protocol will be used for the purpose of working with SafeNet Authentication Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM that is used to deploy the solution on-premises in the organization.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Manager 8.2 HF 493**
- **Check Point Security Gateway**—R77 for SSL VPN
- **Check Point Endpoint Security Client**—Version E80.41 for VPN Client
Audience

This document is targeted to system administrators who are familiar with Check Point Security Gateway, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager (SAM).

RADIUS-based Authentication using SafeNet Authentication Manager

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

RADIUS Authentication Flow using SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Check Point Security Gateway.

1. A user attempts to log on to Check Point Security Gateway using an OTP token.
2. Check Point Security Gateway sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to Check Point Security Gateway.
4. The user is granted or denied access to Check Point Security Gateway based on the OTP value calculation results from SAM and is connected to Check Point Security Gateway.

RADIUS Prerequisites

To enable SafeNet Authentication Manager (SAM) to receive RADIUS requests from Check Point Security Gateway, ensure the following:

- End users can authenticate from the Check Point Security Gateway environment with a static password before configuring the Check Point Security Gateway to use RADIUS authentication.
- Ports 1812/1813 are open to and from Check Point Security Gateway.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SafeNet Authentication Manager (SAM) with Check Point Security Gateway using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SafeNet Authentication Manager, page 7
- Configuring SafeNet Authentication Manager’s Connector for OTP Authentication, page 8
- Assigning a Token in SafeNet Authentication Manager, page 5
- Adding Check Point Security Gateway as a RADIUS Client in IAS/NPS, page 9
- Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client, page 11

Synchronizing Users Stores to SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
• IBM Tivoli Directory Server

Configuring SafeNet Authentication Manager’s Connector for OTP Authentication

SafeNet Authentication Manager (SAM) is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

• Connectors—SAM Connector for OTP Authentication is installed
• SAM Back-end Service—Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

• OTP support (required for OTP) is selected in the Token Initialization settings.
• The SAM Connector for OTP Authentication is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Assigning a Token in SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Check Point Security Gateway.

The following tokens are supported:

• eToken PASS
• eToken NG-OTP
• SafeNet GOLD
• SMS tokens
• MobilePASS
• SafeNet eToken Virtual products
• MobilePASS Messaging
• SafeNet Mobile Authentication (iOS)
• SafeNet eToken 3400
• SafeNet eToken 3500

Tokens can be assigned to users as follows:

• SAM Management Center—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
• SAM Self-Service Center—Self-service site used by end users for managing their tokens.
• **SAM Remote Service**—Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**Adding Check Point Security Gateway as a RADIUS Client in IAS/NPS**

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Check Point Security Gateway.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Check Point Security Gateway.

Check Point Security Gateway must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Check Point Security Gateway for authentication.

---

NOTE: This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager (SAM).

The details below refer to NPS, and are very similar to IAS.

---

1. Click **Start > Administrative Tools > Network Policy Server**.
2. On the Network Policy Server web console, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and then click **New**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. On the **New RADIUS Client** window, on the **Settings** tab, complete the following fields:

<table>
<thead>
<tr>
<th><strong>Enable this RADIUS client</strong></th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly name</strong></td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td><strong>Address (IP or DNS)</strong></td>
<td>Enter the Check Point Security Gateway IP address or DNS.</td>
</tr>
<tr>
<td><strong>Manual/Generate</strong></td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in Check Point Security Gateway.</td>
</tr>
<tr>
<td><strong>Confirm shared secret</strong></td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

Check Point Security Gateway is added as a RADIUS client in NPS.
Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SafeNet Authentication Manager’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Configuring Check Point Security Gateway

Configuring Check Point Security Gateway requires:

- Configuring Check Point Security Gateway for RADIUS Server Authentication, page 11
- Creating a RADIUS Server Object, page 13
- Creating Networks, page 14
- Creating a User, page 17
- Creating a User Group, page 18
- Enabling Mobile Access, page 20
- Setting the Topology, page 25
- Configuring RADIUS Authentication for Mobile Access, page 29
- Configuring the Office Mode, page 31
- Performing Portal Settings, page 34
- Configuring the Mobile Access Solution, page 35
- Configuring the VPN Client Solution, page 56

Configuring Check Point Security Gateway for RADIUS Server Authentication

Enable and specify the RADIUS server in the Check Point Security Gateway configuration to use RADIUS server authentication with Check Point Security Gateway.

1. Open Check Point SmartDashboard R77.
2. On the login window, complete the following fields, and then click **Login**.

<table>
<thead>
<tr>
<th><strong>Username</strong></th>
<th>Enter your user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Enter your password.</td>
</tr>
<tr>
<td><strong>Server name or IP address</strong></td>
<td>Select the name or IP address of the server where Check Point Security Gateway is hosted.</td>
</tr>
<tr>
<td><strong>Read only</strong></td>
<td>Clear this option.</td>
</tr>
</tbody>
</table>

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

3. On the Check Point SmartDashboard main window, in the left pane, under **Network Objects**, click **Nodes > Node > Host**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
4. On the **Host Node** window, in the right pane, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the host node.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPv4 Address</strong></td>
<td>Enter the IP address of the RADIUS server.</td>
</tr>
</tbody>
</table>

![Host Node - radius](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

### Creating a RADIUS Server Object

A RADIUS server object is created to define the host, service, version, and protocol to be used. Once a RADIUS server object is created, it can be used to specify RADIUS object for authentication schemes for user authentication.

1. On the **Check Point SmartDashboard** main window, in the left pane, click the **Servers and OPSEC** icon.
2. Under **Servers and OPSEC**, expand **Servers**, right-click **RADIUS**, and then click **New RADIUS**.

![Servers and OPSEC](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
3. On the **RADIUS Server Properties** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the RADIUS server.</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>Enter any applicable comments.</td>
</tr>
<tr>
<td><strong>Color</strong></td>
<td>Select a color of your choice.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Select the RADIUS server host node that you configured in step 4 of “Configuring Check Point Security Gateway for RADIUS Server Authentication” on page 11.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>Select <strong>NEW-RADIUS</strong>, which is associated with the port number 1812.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret value. The shared secret must be same as entered in SAM.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>Select <strong>RADIUS Ver. 2.0 Compatible</strong>.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Select <strong>PAP</strong>.</td>
</tr>
</tbody>
</table>

![RADIUS Server Properties Window](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

### Creating Networks

Internal and external networks are used to configure the topology of the internal and external interfaces for the Check Point gateway. Creating networks includes:

- Creating an Internal Network, page 15
- Creating an External Network, page 16
Creating an Internal Network

1. On the **Check Point SmartDashboard** main window, in the left pane, click the icon.
2. Under **Network Objects**, right-click **Networks**, and then click **Network**.

![Network Objects](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

3. On the **Network Properties** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the internal network.</td>
</tr>
<tr>
<td><strong>Network Address</strong></td>
<td>Enter the IP address of the internal network.</td>
</tr>
<tr>
<td><strong>Net Mask</strong></td>
<td>Enter the mask of the internal network.</td>
</tr>
</tbody>
</table>

![Network Properties](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
Creating an External Network

1. On the **Check Point SmartDashboard** main window, in the left pane, click the icon.
2. Under **Network Objects**, right-click **Networks**, and then click **Network**.

3. On the **Network Properties** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the external server.</td>
</tr>
<tr>
<td><strong>Network Address</strong></td>
<td>Enter the IP address of the external network.</td>
</tr>
<tr>
<td><strong>Net Mask</strong></td>
<td>Enter the mask of the external network.</td>
</tr>
</tbody>
</table>

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
Creating a User

A user is created with the defined authentication scheme to be able to log in to the Mobile Access portal and access its applications.

1. On the Check Point SmartDashboard main window, in the left pane, click the icon.
2. Under Users and Administrators, right-click Users, and then click New User > Default.

3. On the User Properties window, in the right pane, in the User Name field, enter a name of the user (for example, Bob).
4. In the left pane, click **Authentication**.
5. In the right pane, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Authentication Scheme</th>
<th>Select RADIUS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a RADIUS Server or Group of Servers</td>
<td>Select the RADIUS server object that you created previously.</td>
</tr>
</tbody>
</table>

![User Properties - Bob](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

### Creating a User Group

A user group is a group of users with related responsibilities or who perform related tasks. You can specify a user group in policy rules in the same way as individual users.

**NOTE:** Creating a group is necessary if you want to permit some of your users to do certain things but not others. Firewall does not allow you to define rules for individual users, but you can define rules for groups.

1. On the **Check Point SmartDashboard** main window, in the left pane, click the user icon.
2. Under **Users and Administrators**, right-click **User Groups**, and then click **New Group**.

![Image of Users and Administrators with User Groups selected and New Group option highlighted.](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

3. On the **Group Properties** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the group (for example, <strong>Mobile_access_group</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available Members/Selected Members</strong></td>
<td>In the <strong>Available Members</strong> list, select the members that you want to add to the group, and then click <strong>Add</strong>. These members are moved to the <strong>Selected Members</strong> list.</td>
</tr>
</tbody>
</table>

![Image of Group Properties window with Name field, Comment field, Color selection, and Available Members and Selected Members lists.](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
Enabling Mobile Access

For a user to connect to the corporate applications over the Internet using a web, mobile, or desktop application, enable Mobile Access Software Blade.

1. On the Check Point SmartDashboard main window, in the left pane, click the icon.
2. Under Network Objects, expand Check Point, right-click your device (for example, Checkpoint-ssl), and then click Edit.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
3. On the **Check Point Gateway – Checkpoint-ssl** window, in the right pane, on the **Network Security** tab, select **Mobile Access**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
4. On the **Mobile Access** window, click **Next**.

5. On the **Web Portal** window, in the **Main URL** field, select the Mobile Access portal URL, and then click **Next**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
6. On the **Applications** window, under **Mail / Calendar / Contacts**, clear **Secure Container Mail**, and then click **Next**.

![Application Configuration Window]

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

7. On the **Active Directory Integration** window, perform the following steps:
   a. Select your active directory domain.
   b. In the **Username** field, enter your username.
   c. In the **Password** field, enter your password.
   d. Click **Connect** to test the connectivity.
   e. After the test is successful, click **Next**.

![Active Directory Integration Window]

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
8. On the **Users** window, click **Add**, and then on the search bar, select **Internal User Groups**. The users under **Internal User Groups** are listed.

9. In the **Internal User Groups** list, select your user group (for example, **Mobile_access_group**), and then click **Next**.

10. Click **Finish**.

11. On the Check Point Gateway – Checkpoint-ssl window, click **OK**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
Setting the Topology

Setting the topology helps you define which interface leads to which network. This setting is done manually with the network or group object so that it represents the network or subnet behind each port.

Settings for Internal Network

1. On the Check Point SmartDashboard main window, in the left pane, click the icon.
2. Under Network Objects, expand Check Point, right-click your device (for example, Checkpoint-ssl), and then click Edit.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
3. On the **Check Point Gateway** window, in the left pane, click **Topology**, and then in the right pane, in the list of topologies, select the internal network (for example, **eth1**) that you added previously.

![Check Point Gateway window](image)

*The screen image above is from Check Point® software. Trademarks are the property of their respective owners.*

4. Click **Edit**.
5. On the **Interface Properties** window, on the **Topology** tab, perform the following steps, and then click **OK**.
   a. Select the **Internal (leads to local network)** option.
   b. Select **Specific**, and then select the **Internal_network**.
   c. Select **Perform Anti-Spoofing based on interface topology**.

   ![Interface Properties Window](image)

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

**Settings for External Network**

1. On the **Check Point SmartDashboard** main window, in the left pane, click the **Settings** icon.
2. Under **Network Objects**, expand **Check Point**, right-click your device (for example, **Checkpoint-ssl**), and then click **Edit**.

3. On the **Check Point Gateway** window, in the left pane, click **Topology**, and then in the right pane, in the list of topologies, select the external network you added previously (for example, **eth2**).

4. Click **Edit**.
5. On the **Interface Properties** window, on the **Topology** tab, perform the following steps, and then click **OK**:
   
d. Select **External** (leads out to the Internet).
   
e. Select **Perform Anti-Spoofing based on interface topology**.

![Interface Properties](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

### Configuring RADIUS Authentication for Mobile Access

For a user to connect to the corporate applications over Internet using web, mobile, or desktop, the user needs to be authenticated.

1. On the **Check Point SmartDashboard** main window, in the left pane, click the icon.
2. Under **Network Objects**, expand **Check Point**, right-click your device (for example, **Checkpoint-ssl**), and then click **Edit**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
3. On the **Check Point Gateway** window, in the left pane, click **Mobile Access > Authentication**.

![Check Point Gateway window](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

4. In the right pane under **Authentication Method**, select the **RADIUS** option, and then specify the RADIUS server you created earlier in step 4 of “Configuring Check Point Security Gateway for RADIUS Server Authentication” on page 11.

5. Click **OK**.

### Configuring the Office Mode

Configuring the Office Mode enables the security gateway to assign an internal IP address to the remote client. It also allows the security administrator to control which addresses are used by remote clients inside the local network and make them a part of the local network.

When a user connects to a resource on the corporate network, a packet is routed through the virtual interface that Office Mode sets up with the IP allocated for the remote user.

1. On the **Check Point SmartDashboard** main window, in the left pane, click **Office Mode**.
2. Under **Network Objects**, expand **Check Point**, right-click your device (for example, **Checkpoint-ssl**), and then click **Edit**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
3. On the **Check Point Gateway** window, in the left pane, click **Mobile Access > Office Mode**.

   ![Check Point Gateway - Checkpoint-ssl](image)

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

4. In the right pane, perform the following steps:
   a. Select **Using one of the following Methods**.
   b. Select the **Manual (using IP pool)** option.
   c. In the **Allocate IP address from network** field, select **Internal_network**.

5. Click **OK**.
Performing Portal Settings

Configure the mobile portal so that the remote user is able to access it through an external IP address.

1. On the Check Point SmartDashboard main window, in the left pane, click the icon.
2. Under Network Objects, expand Check Point, right-click your device (for example, Checkpoint-ssl), and then click Edit.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
3. On the **Check Point Gateway** window, in the left pane, click **Mobile Access > Portal Settings**.

![Check Point Gateway - Checkpoint-ssl](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

4. In the right pane, in the **Main URL** field, enter `https://<external_ip>/sslvpn`, where, `<external_ip>` is the IP address of the external network you created previously.

5. Click **OK**.

---

**Configuring the Mobile Access Solution**

Configuring the Mobile Access solution requires:

- Configuring the Native Application, page 35
- Configuring Firewall Rules, page 40
- Creating the Mobile Access Policy, page 53
- Installing a Policy, page 54

---

**Configuring the Native Application**

A native application is any IP-based application that is hosted on servers within the organization and requires an installed client on the endpoint. The client is used to access the application and encrypt all traffic between the endpoint and Mobile access.

The SSL Network Extender client makes it possible to access the native application via Mobile Access.

Microsoft Exchange, Telnet, and FTP are the examples of the native application servers. Authorized users can use their native clients (for example, `telnet.exe`, `ftp.exe`, or **Outlook**) to access these internal applications from outside the organization.
1. On the **Check Point SmartDashboard** main window, click **More > Mobile Access**.

![Screen Image](image1.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

2. On the **Mobile Access** window, in the left pane, click **Applications > Native Applications**.

![Screen Image](image2.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
3. In the right pane, click **New**

4. On the **Native Application** window, in the right pane, in the **Name** field, enter a name for the native application (for example, **Mobile_access**).

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
5. In the left pane, click **Authorized Locations**, and then in the right pane, perform the following steps:
   a. Select the **Simple** option.
   b. In the **Host /Address Range/Group** field, select a machine in the corporate network where you want to access application after the VPN connection.
   c. In the **Service** field, select an application you want to access after the VPN connection (for example, **telnet**).

   ![Authorized Locations](image)

   *The screen image above is from Check Point® software. Trademarks are the property of their respective owners.*

6. In the left pane, click **Endpoint Applications**.

   ![Endpoint Applications](image)

   *The screen image above is from Check Point® software. Trademarks are the property of their respective owners.*
7. In the right pane, perform the following steps:
   a. Select **Add a link to the application in the Mobile Access portal**.
   b. Select the **Advanced** option, and then click **Edit**.
   c. On the **Endpoint Applications – Advanced** window, click **Add**.

   ![Endpoint Applications - Advanced](image)

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

   d. On the **Edit Endpoint Application** window, complete the following, and then click **OK**.

<table>
<thead>
<tr>
<th>Add a link to the application in the Mobile Access portal</th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link text (multi-language)</td>
<td>Enter the text to be displayed as a link.</td>
</tr>
<tr>
<td>Tooltip (multi-language)</td>
<td>Enter any tooltip you want to display at solution runtime.</td>
</tr>
<tr>
<td>Downloaded from Mobile Access</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Name</td>
<td>Select the native application server as per your preferred configuration (for example, <strong>telnet</strong>).</td>
</tr>
<tr>
<td>Parameters</td>
<td>Enter configuration based on the native application server you selected in the <strong>Name</strong> field. Refer to the Check Point documentation.</td>
</tr>
</tbody>
</table>
e. Click OK.

8. Click OK.

Configuring Firewall Rules

A security gateway object has at least a firewall blade installed that serves as an entry point to the corporate network.

The firewall rule is basically a policy definition of what is allowed and what is blocked by the firewall. Rules use objects. For example, networks objects can be used in the source and destination of rules.

You need to create the following three firewall rules:

- Rule for client authentication
- Rule for user authentication
- Stealth rule

Rule for Client Authentication

Client authentication allows access per host. It allows connections from specific IP addresses. After successful authentication, it can be used for any service, for any number of connections, and for any length of time. It is slightly less secure than user authentication.
1. On the **Check Point SmartDashboard** main window, click **Firewall**.

![Firewall icon](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

2. In the left pane, click **Policy**.

3. In the right pane, click the **Add rule at bottom** icon. A row is added below the **Policy** icon bar.

![Policy icon](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
4. In the **Name** column, right-click and then click **Edit**.

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

5. In the **Rule Name** window, in the **Rule Name** field, add a name for the firewall rule, and then click **OK**.

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

6. In the **Source** column, right-click and then click **Add Objects > Add Legacy Users Access**.

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
7. On the **Legacy Users Access** window, perform the following steps:
   a. Under **User Group**, select the user group that you created earlier (for example, **Mobile_access_group**).
   b. Under **Location**, select the **No restriction** option.
   c. Click **OK**.

   ![Legacy User Access](image)
   
   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

8. In the **Destination** column, right-click and then click **Network Object**.

   ![Network Object](image)
   
   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
9. On the **Add Object** window, select **Internal_network**, and then click **OK**. **Internal_network** is an alias for the corporate network in an organization.

![Add Object window](image1)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

10. In the **Service** column, right-click and then click **Add Objects**.

![Service column with Add Objects option](image2)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

11. On the **Add Object** window, click **New**, and then add **http** and **https**, separately.

![Add Object window with http and https](image3)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
12. Click OK.

13. In the **Action** column, right-click and then click **Legacy > Client Auth**. The value in the **Action** column changes to **Client Auth**.

14. In the **Action** column, right-click and then click **Edit properties**.

15. On the **Client Authentication Action Properties** windows, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Source</th>
<th>Select <em>ignore user database</em>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign on Method</td>
<td>Select the <em>Fully automatic</em> option.</td>
</tr>
</tbody>
</table>

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
Rule for User Authentication
User authentication is used to allow access as per user basis. This method is used for telnet, ftp, http, and https, and requires separate authentication for each connection. User authentication is a secure connection as different components are loaded with authentication.

1. On the Check Point SmartDashboard main window, click Firewall.

2. In the left pane, click Policy.

3. In the right pane, click the Add rule at bottom icon. A row is added below the Policy icon bar.
4. In the **Name** column, right-click and then click **Edit**.

<table>
<thead>
<tr>
<th>No.</th>
<th>Hits</th>
<th>Name</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>Any</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>Hide Column</td>
<td></td>
</tr>
</tbody>
</table>

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

5. In the **Rule Name** window, in the **Rule Name** field, add a name for the firewall rule, and then click **OK**.

6. In the **Source** column, right-click and then click **Add Objects > Add Legacy Users Access**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
7. On the **Legacy Users Access** window, perform the following steps:
   a. Under **User Group**, select a user group that you created earlier (for example, **Mobile_access_group**).
   b. Under **Location**, select **No restriction**.
   c. Click **OK**.

   ![Legacy User Access Window](image1.png)
   
   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

8. In the **Destination** column, right-click and then click **Network Object**.

   ![Network Object Context Menu](image2.png)
   
   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
9. On the **Add Object** window, select **Internal network**, and then click **OK**. **Internal network** is an alias for the corporate network in an organization.

![Add Object window](image1)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

10. In the **Service** column, right-click and then click **Add Objects**.

![Service column](image2)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
11. On the **Add Object** window, click **New**, and then add **http** and **https**, separately.

12. Click **OK**.

13. In the **Action** column, right-click and then click **Legacy > User Auth**. The value in the **Action** column changes to **User Auth**.

14. In the **Action** column, right-click and then click **Edit properties**.
15. On the **User Authentication Action Properties** windows, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Source</th>
<th>Select <em>ignore user database</em>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Select <em>ignore user database</em>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

**Stealth Rule**

The firewall stealth rule is the explicit rule near the top of the policy denying access to the firewall beyond what is required to manage the device.

All traffic that is NOT from the internal company network to one of the Security Gateways is dropped. When a connection matches the stealth rule, an alert window opens in the SmartView Monitor.

1. On the **Check Point SmartDashboard** main window, click **Firewall**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
2. In the left pane, click **Policy**.

3. In the right pane, click the **Add rule at bottom** icon. A row is added below the **Policy** icon bar.

4. In the **Name** column, right-click and then click **Edit**.

5. In the **Rule Name** window, in the **Rule Name** field, add a name for the firewall rule, and then click **OK**.
Creating the Mobile Access Policy

The Mobile Access policy applies to the Mobile Access portal. Users can access applications remotely as defined by policy rules.

1. On the **Check Point SmartDashboard** main window, click **More > Mobile Access**.

2. In the left pane, click **Policy**.

3. In the right pane, in the first row, in the **Applications** column, right-click, and then click **Add Applications**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
4. In the search box, search for the application you created previously (for example, Mobile_access), and then select it.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

The selected application is displayed.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

**Installing a Policy**

The policy installation process does the following:

- Performs a heuristic verification on rules to ensure that they are consistent and no rule is redundant.
- Confirms that each of the security gateways on which the rule is enforced (known as Install On object) enforces at least one of the rules.
- Converts the security policy into an inspection script and compiles this script into an inspection code.
- Distributes inspection codes to the selected installation targets.

1. On the Check Point SmartDashboard main window, click Install Policy on the top icon bar.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
2. On the **Install Policy** window, in the **Network Security** column, select the option for your device (for example, **Checkpoint-ssl**), and then click **OK**.

![Install Policy window](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

3. On the **Installation Process – Standard** window, a success message is displayed. Click **Close**.

![Installation Process – Standard window](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
Configuring the VPN Client Solution

Configuring the VPN client solution requires:

- Enabling Authentication for the VPN Client, page 56
- Configuring Firewall Rules for the VPN Client, page 57
- Installing a Policy, page 62

Enabling Authentication for the VPN Client

1. On the Check Point SmartDashboard main window, in the left pane, click the icon.

2. Under Network Objects, expand Check Point, right-click your device (for example, Checkpoint-ssl), and then click Edit.

3. On the Check Point Gateway window, in the left pane, click VPN Clients > Authentication.
4. In the right pane, select the **RADIUS** option, and then search for and select the RADIUS server object you created earlier.

5. Click **OK**.

**Configuring Firewall Rules for the VPN Client**

A security gateway object has at least one firewall blade installed that serves as an entry point to the corporate network.

The firewall rule is basically a policy definition of what is allowed and what is blocked by the firewall. Rules use objects. For example, networks objects can be used in the source and destination of rules.

1. On the **Check Point SmartDashboard** main window, click **Firewall**.

   ![Check Point SmartDashboard](image)

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

2. In the left pane, click **Policy**, and then delete all the previously created rules.
3. In the right pane, click the **Add rule at bottom** icon. A row is added below the **Policy** icon bar.

4. In the **Name** column, right-click and then click **Edit**.

5. In the **Rule Name** window, in the **Rule Name** field, add a name for the firewall rule. Click **OK**.
6. In the **Source** column, right-click and then click **Add Objects > Add Legacy Users Access.**

![Source column with Add Objects option highlighted]

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

7. On the **Legacy Users Access** window, perform the following steps:
   a. Under **User Group**, select a user group you created previously (for example, **Mobile_access_group**).
   b. Under **Location**, select the **No restriction** option.
   c. Click **OK**.

![Legacy Users Access window]

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
8. In the **Destination** column, right-click and then click **Network Object**.

   ![Network Object](image1)

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

9. On the **Add Object** window, select **Internal_network**, and then click **OK**. **Internal_network** is an alias for the corporate network in an organization.

   ![Add Object](image2)

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

10. In the **VPN** column, right-click and then click **Edit Cell**.

   ![Edit Cell](image3)

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
11. On the **VPN Match Conditions** window, perform the following steps, and then click **OK**.
   a. Select the **Only connections encrypted in specific VPN Communities** option.
   b. Click **Add**.

11a. (The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

   c. In the **Add Community to rule** window, select **RemoteAccess**, and then click **OK**.

11c. (The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
12. In the **Action** column, right-click and then click **accept**.

![Screen Image](image.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

**Installing a Policy**

The policy installation process does the following:

- Performs a heuristic verification on rules to ensure they are consistent and that no rule is redundant.
- Confirms that each of the security gateways on which the rule is enforced (known as Install On object) enforces at least one of the rules.
- Converts the security policy into an inspection script and compiles this script into an inspection code.
- Distributes inspection codes to the selected installation targets.

1. On the **Check Point SmartDashboard** main window, click **Install Policy** on the top icon bar.

![Screen Image](image.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
2. On the **Install Policy** window, in the **Network Security** column, select the option for your device (for example, **Checkpoint-ssl**), and then click **OK**.

![Install Policy](image1)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

3. On the **Installation Process – Standard** window, a success message is displayed. Click **Close**.

![Installation Process](image2)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
Running the Solution

You can use the following methods to securely connect to the Check Point Mobile Access application:

- Using a Web Browser, page 64
- Using a VPN Client, page 66

For this integration, the SafeNet MobilePASS token is configured for authentication with the SAM solution.

NOTE: For this integration, Windows 7 is used for verifying the solution. Administrator privileges are required when installing the Check Point SSL Extender.

Using a Web Browser

1. Open a web browser and enter the following URL:
   
   https://<IP Check Point FW External Address>/sslvpn
   
   If you are connecting for the first time, the SSL VPN gateway imposes the installation of the Check Point SSL Extender Active X component. This is a virtual interface that encapsulates all the communication inside an SSL tunnel.

2. On the log in window, in the **User name** field, enter the user name you have defined in Check Point.

3. Generate an OTP using the SafeNet MobilePASS token, enter it in the **Password** field, and then click **Sign In**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
4. If the user is authenticated successfully, the Check Point Mobile window is displayed. Under Native Applications, click Connect. The SSL Network Extender installation begins.

![Check Point Mobile window](image1)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

5. If the SSL Network Extender installation displays the message below, click Trust Server.

![Check Point Network Extender window](image2)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
6. If the firewall alert is displayed, click **Allow access**.

![Windows Security Alert](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

When SSL Network Extender is successfully installed, the following window is displayed:

![SSL Network Extender](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
Using a VPN Client

1. Open the **Check Point Endpoint Security** application.
2. On the log in window, perform the following steps:
   a. In the **Site** field, enter the IP address of Check Point Security Gateway.
   b. In the **Username** field, enter the name you have defined in Check Point.
   c. In the **Password** field, enter the OTP generated using the SafeNet MobilePASS token.
   d. Click **Connect**.

   ![Check Point Endpoint Security login window](image)

   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

If authentication is successful, you are logged in.

![Connection succeeded](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
NOTE: If you are using the SafeNet MobilePASS Messaging token and get the “Negotiation with site failed” error, it means that the Initial or Default policy is loaded on Check Point. Run the following command on the Check Point console, to unload the Initial or Default policy, and then connect again:

```
fw unloadlocal
```

Uninstalling Security Policy from all.all@Chkpoint-ssl
Done.

3. On the task bar, right-click the icon, and then click Show Client.

The connection status is displayed as Connected.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
Appendix

User Authentication with the SafeNet SMS Token

To securely connect to the Check Point Mobile Access application authenticating from the SAM solution using the SafeNet SMS token, you can use a VPN client.

Enabling Identity Awareness Blade

Identity Awareness enables you to easily configure network access and it is applicable for both Active Directory and non-Active Directory based networks.

In this section, you will enable the Identity Awareness blade to be able to access the Active Directory with its' users' properties.

1. On the Check Point SmartDashboard main window, in the left pane, click the icon.
2. Under Network Objects, expand Check Point, right-click your device (for example, Checkpoint-Dec1), and then click Edit.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
3. On the **Check Point Gateway** window, in the right pane, on the **Network Security** tab, select **Identity Awareness**.

4. On the **Identity Awareness Configuration** window, under **Methods For Acquiring Identity**, click **Next**.
5. Under **Integration with Active Directory**, enter the credentials of domain administrator, and then click **Connect**.

6. After the “**Successfully connected!**” message is displayed, click **Next**.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
7. Click **Finish**.

![Identity Awareness Configuration](image)

Identity Awareness is Now Active!

Identity Awareness is now enabled on gateway Checkpoint-Dec1.

Selected methods for acquiring identity:

• Active Directory Query with domain sfmt.com

**What’s Next?**

- Add Access Role to the Security Policy
- Install Policy
- Watch Users Counters
- View Logs

(The screen image above is from Check Point* software. Trademarks are the property of their respective owners.)
8. On the Check Point Gateway window, click OK.

![Check Point Gateway window](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

**Configuring RADIUS Authentication for VPN Client**

For a user to connect to the corporate applications over Internet using web, mobile, or desktop, the user needs to be authenticated.

1. On the Check Point SmartDashboard main window, in the left pane, click the **`>`** icon.
2. Under **Network Objects**, expand **Check Point**, right-click your device (for example, **Checkpoint-Dec1**), and then click **Edit**.

![Diagram of Check Point interface](image)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
3. On the Check Point Gateway window, in the left pane, click VPN Clients > Authentication.

![](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

4. In the right pane, under Authentication Method, select the RADIUS option, and then specify the RADIUS server you created earlier in step 4 of “Configuring Check Point Security Gateway for RADIUS Server Authentication” on page 11.

5. Click OK.

**Configuring Firewall Rules**

A security gateway object has at least a firewall blade installed that serves as an entry point to the corporate network.

The firewall rule is basically a policy definition of what is allowed and what is blocked by the firewall. Rules use objects. For example, networks objects can be used in the source and destination of rules.
1. On the **Check Point SmartDashboard** main window, click **Firewall**.

![Check Point SmartDashboard](image1.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

2. In the left pane, click **Policy**.

3. In the right pane, click the **Add rule at bottom** icon. A row is added below the **Policy** icon bar.

![Check Point SmartDashboard](image2.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
4. In the **Name** column, right-click and then click **Edit**.

![Edit dialog box](image)

*The screen image above is from Check Point® software. Trademarks are the property of their respective owners.*

5. In the **Rule Name** window, in the **Rule Name** field, enter a name for the firewall rule and then, click **OK**.

![Rule Name window](image)

*The screen image above is from Check Point® software. Trademarks are the property of their respective owners.*

6. In the **Source** column, right-click and then click **Add User/Access Role**

![Source selection](image)

*The screen image above is from Check Point® software. Trademarks are the property of their respective owners.*
7. On the **Access Role** window, in the **Name** field, enter a name (for example, **Auth_users_group**).

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
8. On the Users tab, select the **Specific users/groups** option, and then click the icon.

*The screen image above is from Check Point® software. Trademarks are the property of their respective owners.*
9. On the user record bar, select the group (for example, auth_group) under your Active Directory (for example, sfnt.com).

10. After successful addition, click OK.
11. In the **Action** column, right-click and then click **accept**

![Image of SmartDashboard](image.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

**Installing a Policy**

The policy installation process does the following:

- Performs a heuristic verification on rules to ensure they are consistent and that no rule is redundant.
- Confirms that each of the security gateways on which the rule is enforced (known as Install On object) enforces at least one of the rules.
- Converts the Security Policy into an Inspection Script and compiles this script into an Inspection Code.
- Distributes Inspection Codes to the selected installation targets.

1. On the **Check Point SmartDashboard** main window, click **Install Policy** on the top icon bar.

![Image of Install Policy](image.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

2. On the **Install Policy** window, in the **Network Security** column, select the option for your device (for example, **Checkpoint-Dec1**), and then click **OK**.

![Image of Install Policy window](image.png)

*(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
3. Click Close.

![Installation Process - Standard](image1)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

**Running the Solution**

For this integration, the SafeNet MobilePASS Messaging is configured for authentication with the SAM solution.

1. Open the Check Point Endpoint Security application.
2. On the log in window, perform the following steps:
   a. In the **Site** field, enter the IP address of Check Point Security Gateway
   b. In the **Username** field, enter the name you have defined in Check Point.
   c. In the **Password** field, enter the Windows Active Directory password for the user.
   d. Click **Connect**. The user will receive an SMS on the registered mobile device.

![Check Point Endpoint Security](image2)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
3. Under **Authentication**, in the **Response** field, enter windows password + OTP that you received on your mobile device. Click **Connect**.

4. On successful authentication, you will be successfully logged in and the “**Connection Succeeded**” message is displayed.
5. On the task bar, right-click the icon, and then click **Show Client**.

The connection status is displayed as **Connected**.

![Screen image of SafeNet Authentication Manager](image)

*The screen image above is from Check Point® software. Trademarks are the property of their respective owners.*
**Support Contacts**

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto&lt;br&gt;4690 Millennium Drive&lt;br&gt;Belcamp, Maryland  21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>