SafeNet Authentication Service
Push OTP Integration Guide

Using RADIUS Protocol for Check Point Security Gateway
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013353-001, Rev. A
Release Date: November 2015
# Contents

Third-Party Software Acknowledgement .................................................................................................. 4
Description .................................................................................................................................................. 4
Applicability .................................................................................................................................................. 4
Environment ................................................................................................................................................ 5
Audience ....................................................................................................................................................... 5
RADIUS-based Authentication using SAS Cloud .......................................................................................... 5
RADIUS Authentication Flow using SAS .................................................................................................... 6
RADIUS Prerequisites .................................................................................................................................. 6
Push OTP Prerequisites ............................................................................................................................. 7
Configuring SafeNet Authentication Service .............................................................................................. 7
  Creating Users Stores in SAS ...................................................................................................................... 7
  Assigning an Authenticator in SAS ............................................................................................................. 7
  Adding Check Point Security Gateway as an Authentication Node in SAS .............................................. 8
  Checking the SAS RADIUS Server’s IP Address .................................................................................... 10
  Enabling the Software Token Push OTP Setting ...................................................................................... 11
  Enabling the Allowed Targets Policy ....................................................................................................... 12
Configuring Check Point Security Gateway ................................................................................................. 14
  Configuring Check Point Security Gateway to Use RADIUS Server Authentication ............................ 15
  Creating a RADIUS Server Object ........................................................................................................ 16
  Creating Networks ..................................................................................................................................... 17
  Creating a User .......................................................................................................................................... 20
  Creating a User Group ............................................................................................................................. 21
  Enabling Mobile Access .......................................................................................................................... 23
Configuring RADIUS Authentication for Mobile Access ............................................................................ 28
  Configuring the Office Mode .................................................................................................................. 30
  Performing Portal Settings ...................................................................................................................... 32
  Configuring for the Mobile Access Solution .......................................................................................... 33
  Rule for User Authentication .................................................................................................................. 44
  Configuring the VPN Client Solution ........................................................................................................ 54
Running the Solution ................................................................................................................................... 62
  VPN Client Connection .......................................................................................................................... 62
  Mobile Access Connection ...................................................................................................................... 64
Support Contacts ......................................................................................................................................... 66
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 (Virtual Edition).

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 Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

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:


- Configure Check Point Security Gateway to work with SafeNet Authentication Service 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 Service.

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

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It is likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to his or her smart phone.

- Assess the validity of the request with the information displayed on the screen.

- Respond quickly with a one-tap response to approve or deny the authentication.

Applicability

The information in this document applies to:

- SafeNet Authentication Service (SAS)—SafeNet’s cloud-based authentication service

- MobilePASS+ application
Environment

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

- **SafeNet Authentication Service (SAS)**
- **Check Point Security Gateway (Virtual Edition)—R77 for SSL VPN**

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 Service.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS Cloud environment and can be used without any installation or configuration requirements.

![Diagram of SAS cloud hosted RADIUS service](image)

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS Cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

![Diagram of Local RADIUS hosted on-premises](image)

For more information on how to install and configure SAS Agent for IAS/NPS, refer to:

For more details on how to install and configure FreeRADIUS, refer to the **SAS FreeRADIUS Agent Configuration Guide**.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.
RADIUS Authentication Flow using SAS

SafeNet Authentication Service 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 a Push OTP authenticator.
2. Check Point Security Gateway sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token’s PIN code).
4. The SAS authentication reply is sent back to Check Point Security Gateway.
5. The user is granted or denied access to Check Point Security Gateway based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service 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 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.
- On the client machine, set the RADIUS timeout value at least 60 seconds.
Push OTP Prerequisites

In order to use SAS Push OTP, you will need:

- SAS configured to enable Push OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Check Point Security Gateway using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 7
- Adding Check Point Security Gateway as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Server’s IP Address, page 10
- Enabling the Software Token Push OTP Setting, page 11
- Enabling the Allowed Targets Policy, page 12

Creating Users Stores in SAS

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Check Point Security Gateway.

The following authenticators are supported:
- MobilePASS+

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


### Adding Check Point Security Gateway as an Authentication Node in SAS

Add a RADIUS entry in the SAS **Authentication Nodes** module to prepare it to receive RADIUS authentication requests from Check Point Security Gateway. You will need the IP address of Check Point Security Gateway and the shared secret to be used by both SAS and Check Point Security Gateway.

**To add an Authentication Node in SAS:**

1. Log in to the SAS console with an Operator account.

2. Click the **COMMS** tab, and then select the **Auth Nodes** module.
3. In the **Auth Nodes** module, click the **Auth Nodes** link.

4. Click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

   - **Auth Node Name**: Enter a host description.
   - **Resource Name**: Enter a resource name which will identify in a push notification which authentication node it relates to.
   - **Low IP Address In Range**: Enter the IP address of the host that will authenticate with SAS.
   - **Configure FreeRADIUS Synchronization**: Select this option.
   - **Shared Secret**: Enter the shared secret key.
   - **Confirm Shared Secret**: Re-enter the shared secret key to confirm it.

The Auth Node is added to the system.
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in Check Point Security Gateway, check its IP address. The IP address will then be added to Check Point Security Gateway as a RADIUS server at a later stage.

1. Log in to the SAS console with an Operator account.

2. Click the **COMMS** tab, and then select **Auth Nodes**.

3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.
Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the setting must be enabled in the SAS token policy.

1. Log in to the SAS console with an Operator account.

2. Click the POLICY tab, and then select Token Policies.
3. In the **Token Policies** module, click the **Software Token Push OTP Setting** link.

![Software Token Push OTP Setting](image)

4. Select **Enable Push OTP communication with MobilePass+**, and then click **Apply**.

**Enabling the Allowed Targets Policy**

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.

1. Log in to the SAS console with an Operator account.
2. Click the **POLICY** tab, and then select **Token Policies**.

3. In the **Token Policies** module, click the **Allow Targets Settings** link.

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application, and then click **Apply**.
Configuring Check Point Security Gateway

For this integration, Check Point Security Gateway is used for the SSL VPN connection through Mobile Access and the VPN client.

Configuring Check Point Security Gateway requires the following:

- Configuring Check Point Security Gateway to Use RADIUS Server Authentication, page 15
- Creating a RADIUS Server Object, page 16
- Creating Networks, page 17
- Creating a User, page 20
- Creating a User Group, page 21
- Enabling Mobile Access, page 23
- Configuring RADIUS Authentication for Mobile Access, page 28
- Configuring the Office Mode, page 30
- Performing Portal Settings, page 32
- Configuring for the Mobile Access Solution, page 33
- Configuring the VPN Client Solution, page 53
Configuring Check Point Security Gateway to Use RADIUS Server Authentication

To use the RADIUS server authentication with Check Point Security Gateway, you must enable and specify the RADIUS server in the Check Point Security Gateway configuration.

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

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

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>

(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.

**To create a RADIUS server object:**

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

(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>Name</td>
<td>Enter a name for the RADIUS server.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter any applicable comments.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color of your choice.</td>
</tr>
<tr>
<td>Host</td>
<td>Select the RADIUS server host node configured previously.</td>
</tr>
<tr>
<td>Service</td>
<td>Select <strong>NEW_RADIUS</strong>, which is associated with the port number 1812.</td>
</tr>
</tbody>
</table>
| Shared Secret | Enter the shared secret value.  
The shared secret must be same as entered in SAS. |
| Version     | Select **RADIUS ver. 2.0 Compatible**.                                       |
| Protocol    | Select **PAP**.                                                              |

![RADIUS Server Properties](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 an Internal Network

1. On the Check Point SmartDashboard main window, in the left pane, click.
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>Name</td>
<td>Enter a name for the internal network.</td>
</tr>
<tr>
<td>Network Address</td>
<td>Enter the IP address of the internal network.</td>
</tr>
<tr>
<td>Net Mask</td>
<td>Enter the mask of the internal network.</td>
</tr>
</tbody>
</table>

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

(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.

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>Name</th>
<th>Enter a name for the external server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address</td>
<td>Enter the IP address of the external network.</td>
</tr>
<tr>
<td>Net Mask</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 ![User Management](image1.png).
2. Under Users and Administrators, right-click Users, and then click New User > Default.

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

3. On the User Properties window, in the right pane, in the User Name field, enter a name of the user; for example, Bob.

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
4. In the left pane, click **Authentication**.
5. In the right pane, complete the following details, 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 you created previously.</td>
</tr>
</tbody>
</table>

(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 .
2. Under **Users and Administrators**, right-click **User Groups**, and then click **New Group**.

![User Groups](image1)

*(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, and then click **OK**.

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

![Group Properties](image2)

*(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 📗.
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**.

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

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

   ![Web Portal Window](image)
   
   *(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**.

![Applications window](image)

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

7. On the **Active Directory Integration** window, select your active directory domain, user name, and password, and then click **Connect** to test the connectivity. Once the test is successful, click **Next**.

![Active Directory Integration](image)

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

![User window with Internal User Groups](image)

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

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

![User window with selected user group](image)

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

10. On the Check Point Gateway – Checkpoint-ssl window, click OK.
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 get authenticated.

To configure RADIUS authentication for Mobile Access:

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

   ![Screen Image](image.png)

   *(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 left pane, click **Mobile Access > Authentication**.

4. On the right pane, under **Authentication Method**, select **RADIUS**, and then specify the RADIUS server you created previously. (Refer to "Configuring Check Point Security Gateway to Use RADIUS Server Authentication" on page 15.)

5. Click **OK**.

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

Configuring the Office Mode enables the security gateway assign 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.

To configure the Office Mode:

1. On the Check Point SmartDashboard main window, in the left pane, click .
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 left pane, click **Mobile Access > Office Mode**.

![Check Point Gateway - Checkpoint-ssl window](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 **Manual (using IP pool)**.
   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 .
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 left pane, click Mobile Access > Portal Settings.
   
   (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`. Replace `<external_ip>` with the IP address of the external network you created previously.

5. Click **OK**.

**Configuring for the Mobile Access Solution**

Configuring for the Mobile Access solution requires:

- Configuring the Native Application, page 33
- Configuring Firewall Rules, page 38
- Creating the Mobile Access Policy, page 51
- Installing a Policy, page 52

**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 all examples of 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.

**To configure the native application:**

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

(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**.

![Native Applications window](image)

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

3. In the right pane, click **New**

![New Native Application](image)

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

![Native Application Window](image1)

*(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**.

![Authorized Locations Window](image2)

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

6. In the right pane, perform the following steps:
   a. Select **Simple**.
   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**.
7. 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.)*

8. In the right pane, perform the following steps:
   a. Select **Add a link to this file share in Mobile Access portal**.
   b. Select **Advanced**, 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><strong>Add a link to this file share in Mobile Access portal</strong></th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Link text (multi-language)</strong></td>
<td>Enter the text to be displayed as a link.</td>
</tr>
<tr>
<td><strong>Tooltip (multi-language)</strong></td>
<td>Enter any tooltip you want to display at solution runtime.</td>
</tr>
<tr>
<td><strong>Downloaded from Mobile Access</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Select the native application server of your choice; for example, <strong>telnet</strong>.</td>
</tr>
<tr>
<td><strong>Parameters</strong></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>

![Edit Endpoint Application](image)

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

e. Click **OK**.

9. 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.

To create a rule for client authentication:

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

![Screen shot of Check Point® software](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**.

![Screen shot of Check Point® software](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, add a name for the firewall rule. Click **OK**.

![Screen shot of Check Point® software](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 Objects > Add Legacy Users Access**.

![Add Legacy Users Access](image1.png)

(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 **No restriction**.
   c. Click **OK**.

![Legacy User Access](image2.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 menu](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 window](image2)

*(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**.

![Add Objects menu](image3)

*(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 one-by-one. When finished, click OK.

![Add Object window](image)

(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 Legacy > Client Auth. The value in the Action column changes to Client Auth.

![Action column](image)

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

13. Again, in the Action column, right-click and then click Edit Properties.

![Edit Properties](image)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
14. On the **Client Authentication Action Properties** windows, complete the following, and then click **OK**.

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

![Client Authentication Action Properties](image)

*(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**.

   ![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**.

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

   ![Check Point SmartDashboard](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**.

![Image of a table](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, add a name for the firewall rule. Click **OK**.

![Image of a 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 Objects > Add Legacy Users Access**.

![Image of source column with options](image)

*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 **No restriction**.
   c. Click **OK**.

   (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**.

   (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](Image)

*(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](Image)

*(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** one-by-one. When finished, click **OK**.

![Add Object Window](image1)

(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 **Legacy > User Auth**. The value in the **Action** column changes to **User Auth**.

![Action Column](image2)

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

13. Again, in the **Action** column, right-click, and then click **Edit Properties**.

![Edit Properties](image3)

(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
14. On the **User Authentication Action Properties** windows, complete the following fields, and then click **OK**.

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

![Check Point SmartDashboard](image1)

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

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

![Check Point Policy](image2)

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

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

![Check Point Add Applications](image3)

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

![](image1.png)

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

The application selected is displayed as below.

![](image2.png)

**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.

![](image3.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 window](image1.png)

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

3. When the installation has completed successfully, click **Close**.

![Installation Process - Standard](image2.png)

(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 54
- Configuring Firewall Rules for the VPN Client, page 55
- Installing a Policy, page 60

Enabling Authentication for the VPN Client

1. On the Check Point SmartDashboard main window, in the left pane, click .
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 – Checkpoint-ssl window, in the left pane, click VPN Clients > Authentication.
4. In the right pane, select **RADIUS**, and then search for and specify the RADIUS server object you created previously.

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**. Delete all 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**.

   ![Add Legacy Users Access](image1)

   (*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 **No restriction**.
   
   c. Click **OK**.

   ![Legacy User Access](image2)

   (*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 dropdown menu](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](image)

(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 dropdown menu](image)

(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 **Only connections encrypted in specific VPN communities**.
   b. Click **Add**.

   ![VPN Match Conditions](image1)

   *(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**.

   ![Add Community to rule](image2)

   *(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**.

![Image of Check Point SmartDashboard](image)

*(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 Check Point SmartDashboard](image)

*(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-ss1**), and then click **OK**.

   ![Install Policy Window](Image1)

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

3. When the installation is completed successfully, click **Close**.

   ![Installation Process Window](Image2)

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

VPN Client Connection

1. To connect to Check Point Security Gateway using the Check Point VPN Client and the OTP token, enter your username and any character in the Password field (otherwise, the Check Point VPN client’s Connect button will not be available), and then click Connect.

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

   The RADIUS request will be forwarded to SAS and SAS will trigger a Push OTP authentication request. You will then receive a push notification on the configured mobile device.

2. Tap Approve.
3. Type the token PIN, and then tap **Continue** to send the approval with OTP to SAS.

![Token Authentication Screen]

A successful message is displayed on the configured mobile device.

**Autosend passcode was successful.**

After the successful user authentication on SAS, you will be connected to the Check Point VPN client.

![Connection Success Message]

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

1. To connect to Check Point Mobile Access using the OTP token, browse to the Check Point Mobile Access portal, enter your username and any character in the Password field (otherwise, the sign in process will fail), and then click Sign In.

![Check Point Mobile Access portal](image)

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

The RADIUS request will be forwarded to SAS and SAS will trigger a Push OTP authentication request. You will then receive a push notification on the configured mobile device.

2. Tap Approve.

![MobilePASS+](image)
3. Type the token PIN and tap **Continue** to send the approval with OTP to SAS.

![Token Authentication Screen](image)

A successful message is displayed on the configured mobile device.

![Autosend passcode was successful](image)

After successful user authentication on SAS, you will be connected to the Check Point Mobile Access portal.

![Check Point Screen](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, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland  21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></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>