SafeNet Authentication Service
Integration Guide

SAS Using RADIUS Protocol with Check Point Security Gateway
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012883-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>January 2015</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet 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 (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

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

The 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 the 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.

The 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 SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version 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 Service – Private Cloud Edition (SAS-PCE)**—Version 3.3.393.23552
- **Check Point Security Gateway (Virtual Edition)**—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 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.

- **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.

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-based Authentication using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)** – An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.

- **SafeNet Authentication Service – Private Cloud Edition (PCE)** – An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:


- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

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 an OTP authenticator.
2. The Check Point Security Gateway sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS 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 SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Check Point Security Gateway, ensure the following:

- End users can authenticate through the Check Point Security Gateway environment with a static password before configuring Check Point Security Gateway to use RADIUS authentication.
- Ports 1812 are open to and from the 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 the RADIUS client for encryption, decryption, and digital signature purposes.

Configuring SafeNet Authentication Service

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

- Synchronizing User Stores to SAS, page 7
- Authenticator Assignment in SAS, page 8
- Adding Check Point Security Gateway as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS IP Address, page 11

Synchronizing User Stores to 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 further details on importing users to SafeNet Authentication Service, refer to the section on “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.
Authenticator Assignment in SAS

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

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrIDsure authentication
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manually provision** – Assign an authenticator to users one by one.
- **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**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key to confirm it.</td>
</tr>
</tbody>
</table>

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

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

To check the IP address of the SAS RADIUS server:

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

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

3. Click the Auth Nodes link.
The SAS RADIUS server details are displayed.

### 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:

- Configuring Check Point Security Gateway to Use RADIUS Server Authentication, page 13
- Creating a RADIUS Server Object, page 15
- Creating Networks, page 16
- Creating a User, page 19
- Creating a User Group, page 20
- Enabling Mobile Access, page 22
- Setting the Topology, page 27
- Configuring RADIUS Authentication for Mobile Access, page 32
- Configuring the Office Mode, page 34
- Performing Portal Settings, page 36
- Configuring for the Mobile Access Solution, page 37
- Configuring the VPN Client Solution, page 57
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><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**.

![Network Objects](image)

(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](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.

To create a RADIUS server object:

1. On the Check Point SmartDashboard main window, in the left pane, click 📊.
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 NEW_RADIUS, which is associated with the port number 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret value.</td>
</tr>
<tr>
<td></td>
<td>The shared secret must be same as entered in SAS.</td>
</tr>
<tr>
<td>Version</td>
<td>Select RADIUS ver. 2.0 Compatible.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select PAP.</td>
</tr>
</tbody>
</table>

SafeNet Authentication Service: Integration Guide
SAS Using RADIUS Protocol with Check Point Security Gateway
Document PN: 007-012883-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.
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 [image].
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 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>

(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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the external server.</td>
</tr>
<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 Users.
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**.

![Screen shot of User Groups](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, 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>

![Screen shot of Group Properties](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 🔄.
2. Under **Network Objects**, expand Check Point, right-click your device (for example, Checkpoint-ssl), and then click Edit.

![Screen image](image)

(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)

**Configure applications that will be available for Web and Mobile remote users**

**Web Applications**
- [x] Default web application (world clock)
- [ ] Custom web application (e.g., your internet site)

**Application URL:** http://www.example.com/safecontainer

**Display name:**

**Mail / Calendar / Contacts**
- [x] Secure Container Mail
- [ ] ActiveSync Applications
- [ ] Outlook Web App

![Mail / Calendar / Contacts](image)

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)

**Enter your active directory domain details and test connectivity:**
- **Domain:** example.com
- **Username:** administrator
- **Password:** ********

![Connect](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.

![Image of Users window with Add and Remove buttons]

Select which users are allowed to access the applications you have configured:

![Image of Users window with user groups listed]

(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**.

![Image of Users window with selected user group]

(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**.
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.

For Internal Network

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 **Topology**.

4. In the right pane, in the list of topologies, select the internal network you added previously; for example, `eth1`.

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

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

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 Topology.

4. In the right pane, in the list of topologies, select the external network you added previously; for example, eth2.
5. Click **Edit**.

6. On the **Interface Properties** window, on the **Topology** tab, perform the following steps, and then click **OK**:  
   a. Select **External (leads out to the Internet)**.
   b. Select **Perform Anti-Spoofing based on interface topology**.

(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 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.

(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.

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

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

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 13.)

4. Click OK.
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**.

![Checkpoint 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 **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 ![Check Point SmartDashboard](image).

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 **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 37
- Configuring Firewall Rules, page 42
- Creating the Mobile Access Policy, page 55
- Installing a Policy, page 56

**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**.

   ![Screen Image](image-url)  
   
   *(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**.

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

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

   (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](image)

*(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](image)

*(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**.

![Native Application - Mobile_access](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>Add a link to this file share in Mobile Access portal</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, telnet.</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 window](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.

2. In the left pane, click Policy.

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

![Image of the SafeNet Authentication Service: Integration Guide](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**.

![Image of the Legacy User Access window](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**.

(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.

(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**.

(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 <em>ignore user database</em>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign on Method</td>
<td>Select <em>Fully automatic</em>.</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.

(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. 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 a user group you created previously; for example, **Mobile_access_group**.
   b. Under **Location**, select **No restriction**.
   c. Click **OK**.

   ![Legacy User Access Window](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 Window](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 **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](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 > User Auth**. The value in the **Action** column changes to **User 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 **User Authentication Action Properties** windows, complete the following fields, and then click **OK**.

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

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

2. In the left pane, click Policy.

   (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.

   (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.

   ![Policy](image)

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

   The application selected is displayed as below.

   ![Policy](image)

   **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.

   ![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-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 window](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 58
- Configuring Firewall Rules for the VPN Client, page 59
- Installing a Policy, page 64

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.

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

   ![Screen Image](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 Image](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 Image](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**.

![Screenshot of adding 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**.

![Screenshot of legacy user access window](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 dialog box](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 dialog box](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**.
   c. In the **Add Community to rule** window, select **RemoteAccess**, and then click **OK**.
12. In the **Action** column, right-click and then click **accept**.

![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.

![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 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 Window](image2.png)

*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 66
- Using a VPN Client, page 68

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

   ![Check Point Mobile Access Login](image)

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

3. Generate an OTP using the SafeNet MobilePASS token and enter it in the **Password** field.
4. Click **Sign In**.
   If the user is authenticated successfully, the **Check Point Mobile** window is displayed.

5. Under **Native Applications**, click **Connect**. The SSL Network Extender installation begins.

6. If the SSL Network Extender installation shows the message below, click **Trust Server**.

   (The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)
7. If the firewall alert is shown, 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.

   ![Image of Check Point Endpoint Security login window](image)
   
   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*

3. Click Connect.

   If authentication is successful, you are logged in.

   ![Image of successful connection](image)
   
   *(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)*
4. On the task bar, right-click the icon and then click **Show Client**.

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

![Status](https://example.com/status.png)

*(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 SafeNet Customer Support. SafeNet 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 SafeNet 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>SafeNet, 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</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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>