



2 August 2022

# SAML for Remote Access VPN

*R80.40, R81, R81.10 Hotfix*

---

Release Notes

---



INFINITY VISION



QUANTUM



CLOUDGUARD



HARMONY

© 2022 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and recompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

**RESTRICTED RIGHTS LEGEND:**

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

**TRADEMARKS:**

Refer to the Copyright page <http://www.checkpoint.com/copyright.html> for a list of our trademarks.

Refer to the Third Party copyright notices [http://www.checkpoint.com/3rd\\_party\\_copyright.html](http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

# SAML for Remote Access VPN

This release provides support for compliance check with Azure Active Directory authentication for VPN clients and Mobile devices.

## Prerequisites

For the latest information, see [sk172909](#).

### 1. Check Point Endpoint Security Client:

- Endpoint Security Client for Windows - version E84.70 build 986102705 or higher
- Endpoint Security Client for macOS - version E85.30 or higher

### 2. Check Point Security Gateway:

- For Gateway mode:
  - [R81.10](#) with the [R81.10 Jumbo Hotfix Accumulator](#), Take 9 or higher
  - [R81](#) with the [R81 Jumbo Hotfix Accumulator](#), Take 42 or higher
  - [R80.40](#) with the [R80.40 Jumbo Hotfix Accumulator](#), Take 114 or higher
- For VSX mode:
  - [R81.10](#) with the [R81.10 Jumbo Hotfix Accumulator](#), Take 9 or higher
  - [R81](#) with the [R81 Jumbo Hotfix Accumulator](#), Take 42 or higher
  - [R80.40](#) with the [R80.40 Jumbo Hotfix Accumulator](#), Take 119 or higher

### 3. Check Point Security Management or Multi-Domain Server:

- [R81.10](#) with the [R81.10 Jumbo Hotfix Accumulator](#), Take 9 or higher
- [R81](#) with the [R81 Jumbo Hotfix Accumulator](#), Take 42 or higher
- [R80.40](#) with the [R80.40 Jumbo Hotfix Accumulator](#), Take 114 or higher

### 4. SmartConsole:

- [R81.10 SmartConsole Releases](#) - Build 400 or higher
- [R81 SmartConsole Releases](#) - Build 553 or higher
- [R80.40 SmartConsole Releases](#) - Build 423 or higher

## Installation

1. Install this hotfix package on the Management Server.
2. Install this hotfix package on the Security Gateway / **each** Cluster Member.

**Important** - If you are installing this release on Cluster Members or VPN Remote Access MEP members, you must make sure all members of a Cluster / MEP are the same. If you install this release on one Cluster / MEP member, you must do the same on all the members.

Follow the applicable installation procedure in [sk168597](#).

## Uninstall

1. Uninstall this hotfix package from the Security Gateway / **each** Cluster Member.
2. Uninstall this hotfix package from the Management Server.

For uninstall instructions, see [sk111158](#) (for CDT) or [sk92449](#) (for CPUSE).

# Configuration

Workflow for the SAML Configuration:

[Step 1: Configure an External User Profile object](#)

[Step 2: Configure the Remote Access VPN](#)

[Step 3: Configure an Identity Provider object](#)

[Step 4: Configure the Identity Provider as an authentication method](#)

[Step 5: Install and configure the Remote Access VPN client](#)

[Step 6 \(Optional\): Configure the group authorization](#)

## Step 1: Configure an External User Profile object

The **External** User Profile represents all the users authenticated by the Identity Provider.



**Note** - Follow this section only if you do not want to use an on-premises Active Directory (LDAP).

**Configure a generic user profile in the Legacy SmartDashboard:**

- a) In SmartConsole, go to **Manage & Settings > Blades**.
- b) In the **Mobile Access** section, click **Configure in SmartDashboard**. The Legacy SmartDashboard opens.
- c) In the **Network Objects** pane, click **Users**.



- d) Right-click on an empty space and select **New > External User Profile > Match all users**.
- e) Configure the **External User Profile** properties:
  - i. On the **General Properties** page:
    - In the **External User Profile name** field, leave the default name **generic\***
    - In the **Expiration Date** field, set the applicable date
  - ii. On the **Authentication** page:
 

From the **Authentication Scheme** drop-down list, select "undefined"
  - iii. On the **Location, Time, and Encryption** pages:
 

Configure other applicable settings

- iv. Click **OK**.
- f) From the top toolbar, click **Update** (or press **Ctrl + S**).
- g) Close the SmartDashboard.
- h) In SmartConsole, install the Access Control Policy.

## *Step 2: Configure the Remote Access VPN*

**Note:** Even if your Security Gateway is already configured to support Remote Access VPN, it is important to open the Security Gateway object and click OK to enable the SAML portal on the Security Gateway.

- a) Open the object of the applicable Security Gateway.
- b) On the General Properties page, enable the **IPSec VPN** Software Blade.
- c) From the left tree, click the **IPSec VPN** page.
- d) In the section **This Security Gateway participates in the following VPN communities**, click **Add** and select **Remote Access Community**.
- e) From the left tree, click **VPN clients > Remote Access**.
- f) Enable **Support Visitor Mode**.
- g) From the left tree, click **VPN clients > Office Mode**.
- h) Select **Allow Office Mode** and select the applicable Office Mode Method.
- i) From the left tree, click **VPN Clients > SAML Portal Settings**.
- j) Make sure the Main URL contains the fully qualified domain name of the gateway.

This domain name should end with a DNS suffix registered by your organization. For example:

<https://gateway1.company.com/saml-vpn>

- k) Make sure the Certificate is trusted by the end users' browser.
- l) Click **OK**.

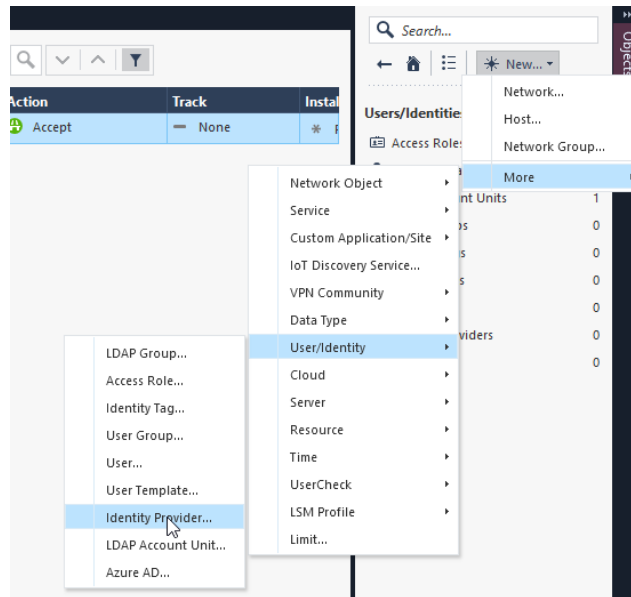
## Step 3: Configure an Identity Provider object

**Important** – Do this step for each Security Gateway that participates in Remote Access VPN.

a) Create a new Identity Provider object.

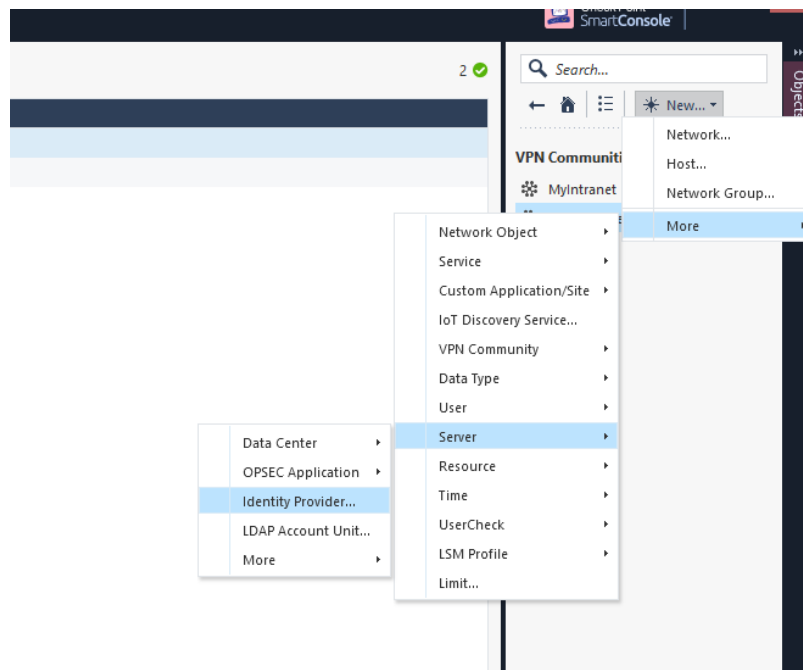
- In SmartConsole R81 and higher:

**More > User/Identity > Identity Provider**




- In SmartConsole R80.40:

**More > Server > Identity Provider**



A **New Identity Provider** window opens:

New Identity Provider

 \* Enter Object Name  
Enter Object Comment

**Data required by the SAML Identity Provider** .....

Gateway: \* No item selected. ▾  
Service: \* No item selected. ▾

Enter the following data in the provider's website:


Identifier (Entity ID):  
Reply URL:

**Data received from the SAML Identity Provider** .....

Enter data for the fields below based on your provider data:

Import Metadata File: \* Import From File...  
 Insert Manually

Identifier (Entity ID):  
Login URL:  
Certificate File: Import From File...

 Add Tag

OK Cancel



- b) In the **New Identity Provider** window, in the **Data required by the SAML Identity Provider** section, configure these settings:
- i. In the **Gateway** field, select the Security Gateway that needs to perform the SAML authentication.
  - ii. In the **Service** field, select the service, through which to authenticate (**Remote Access VPN**).

SmartConsole automatically generates the data in these fields based on the previous two fields:

- i. **Identifier (Entity ID)** – This is a URL that uniquely identifies a service provider (the Security Gateway, in our case).
  - ii. **Reply URL** – This is a URL, to which the SAML assertions are sent.
- c) Configure the SAML Application on an Identity Provider website.



**Important** - Do *not* close the **New Identity Provider** window while you configure the SAML application in your Identity Provider's website.

Continue the configuration later with the information you receive from the Identity Provider.

Follow the Identity Provider's instructions.

- You must provide the values from the **New Identity Provider** window from the **Identifier (Entity ID)** and the **Reply URL** fields.

Copy these values from SmartConsole and paste them in the corresponding fields on the Identity Provider's website.



**Notes:**

- The exact names of the target fields on the Identity Provider's website might differ between Identity Providers.
- When working with Microsoft Azure, and you configure two or more Identity Provider objects for the same Security Gateway.
- Make sure to paste all Entity IDs and all Reply URLs in the same Enterprise Application.
- Make sure to configure the Identity Provider to send the authenticated username in the email format:  
alias@domain.
- **Optional:** If you wish to receive the Identity Provider's groups, in which the user is defined, make sure to configure the Identity Provider to send the group names as values of the attribute called `group_attr`.

- Make sure that at the end of the configuration process you get this information from the Identity Provider:
  - **Entity ID** - a URL that uniquely identifies the application.
  - **Login URL** - a URL to access the application.
  - **Certificate** – for validation of the data exchanged between the Security Gateway and the Identity Provider



**Note** - Some Identity Providers supply a metadata XML file, which contains this information.

d) In the **New Identity Provider** window, in the **Data received from the SAML Identity Provider** section, configure one of these settings:

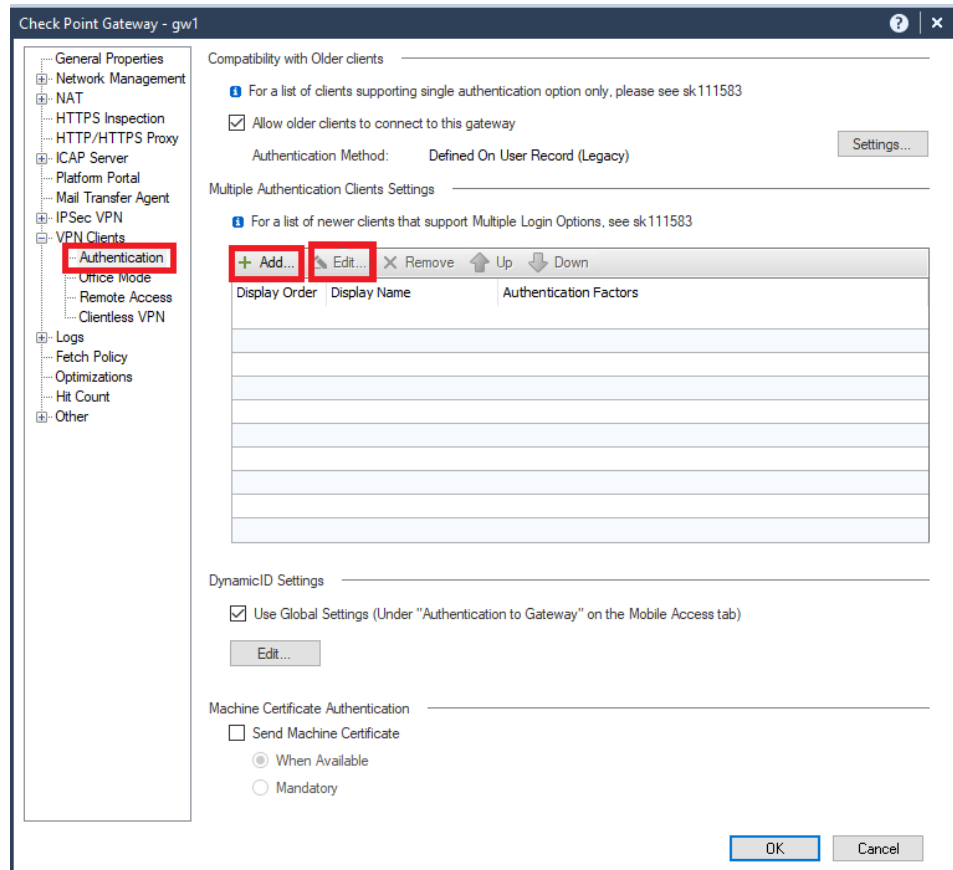
- Select **Import the Metadata File** to upload the metadata file supplied by the Identity Provider.
- Select **Insert Manually** to paste manually the **Entity ID** and **Login URL** into the corresponding fields, and to upload the **Certificate File**. All these are supplied by the Identity Provider.



**Note** - Identity Provider object in SmartConsole does not support the import of RAW Certificate.

## Step 4: Configure the Identity Provider as an authentication method

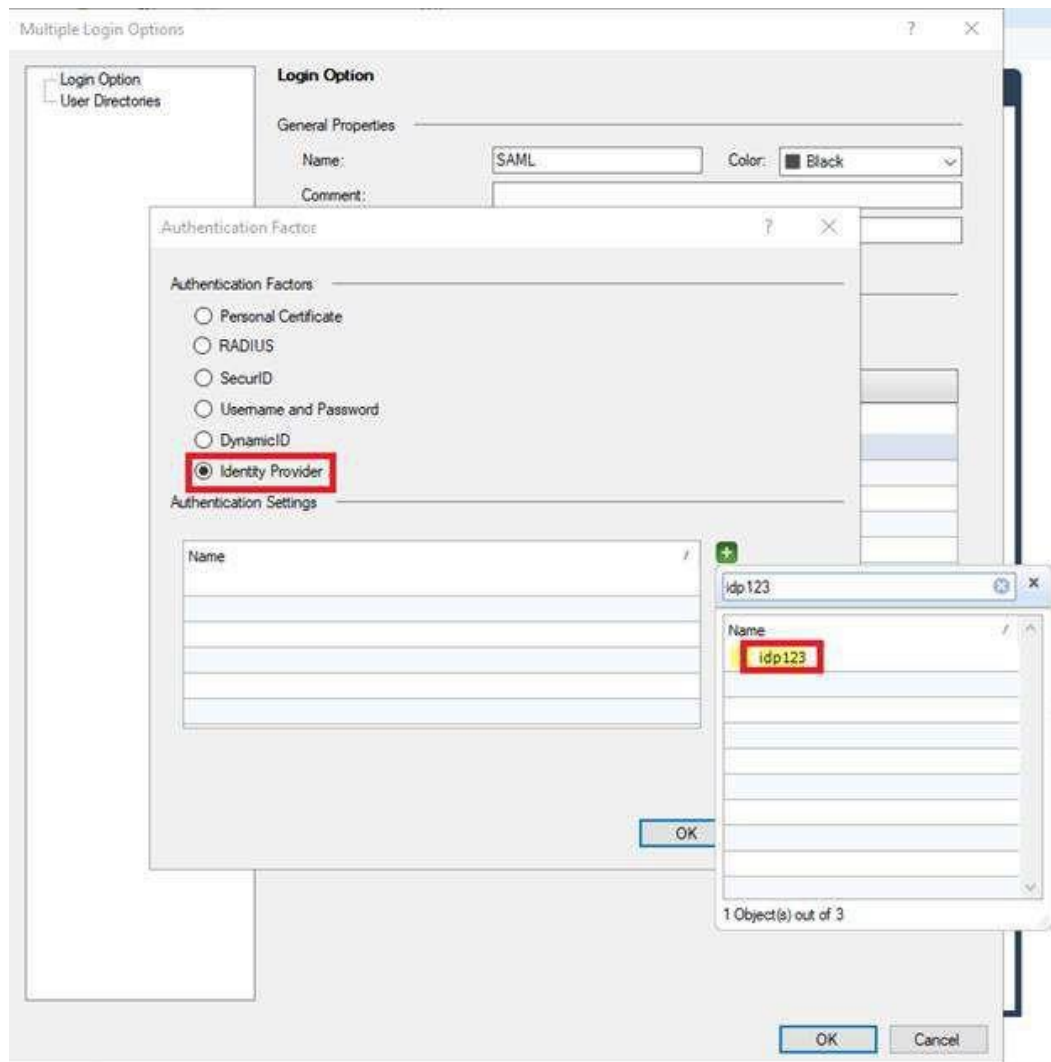
- a) Open the object of the applicable Security Gateway.
- b) On the **VPN Clients > Authentication** page:
  - i. Clear the checkbox "**Allow older clients to connect to this gateway**"
  - ii. Add a new object or edit an existing realm



- c) Enter a **Name** and a **Display Name**, and click **Add** or **Edit** for an authentication method:

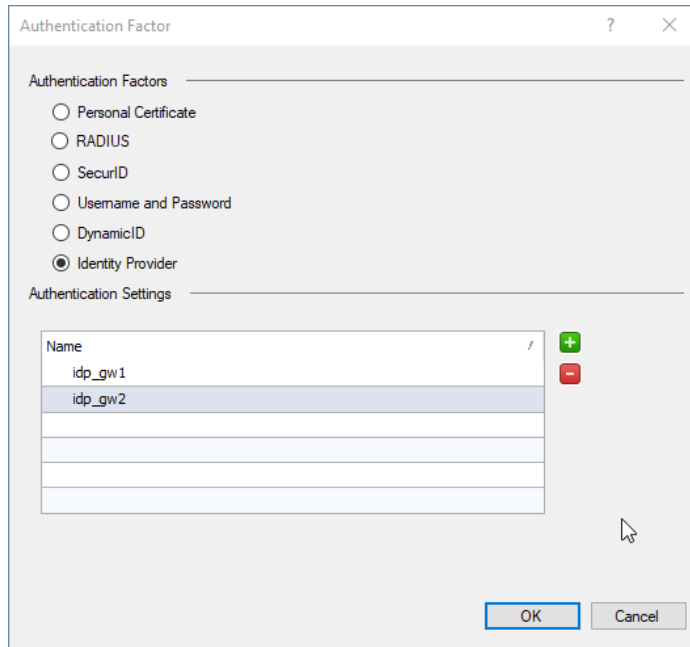
The screenshot shows the 'Multiple Login Options' dialog box. On the left is a tree view with 'Login Option' and 'User Directories'. The main area is titled 'Login Option' and contains two sections: 'General Properties' and 'Authentication Methods'. In 'General Properties', there are fields for 'Name', 'Comment', and 'Display Name' (containing 'New Login Options'), and a 'Color' dropdown set to 'Black'. The 'Authentication Methods' section includes a warning: '"Personal Certificate" can only be used as a first authentication method. "Dynamic ID" can not be used as a first authentication method.' Below this is a toolbar with '+ Add...', 'Edit...', 'Remove', 'Up', and 'Down' buttons. The '+ Add...' button is highlighted with a red box. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- d) Select the option **Identity Provider**, click the green '+' button, and select the applicable Identity Provider object.



**Note** - For RA MEP, as the same Login Option needs to be configured on all MEP participant GWs for smooth user experience, add all relevant Identity Provider objects (one per GW) to a dedicated Login Option.

## An example of Login Option with 2 different Identity Provider objects

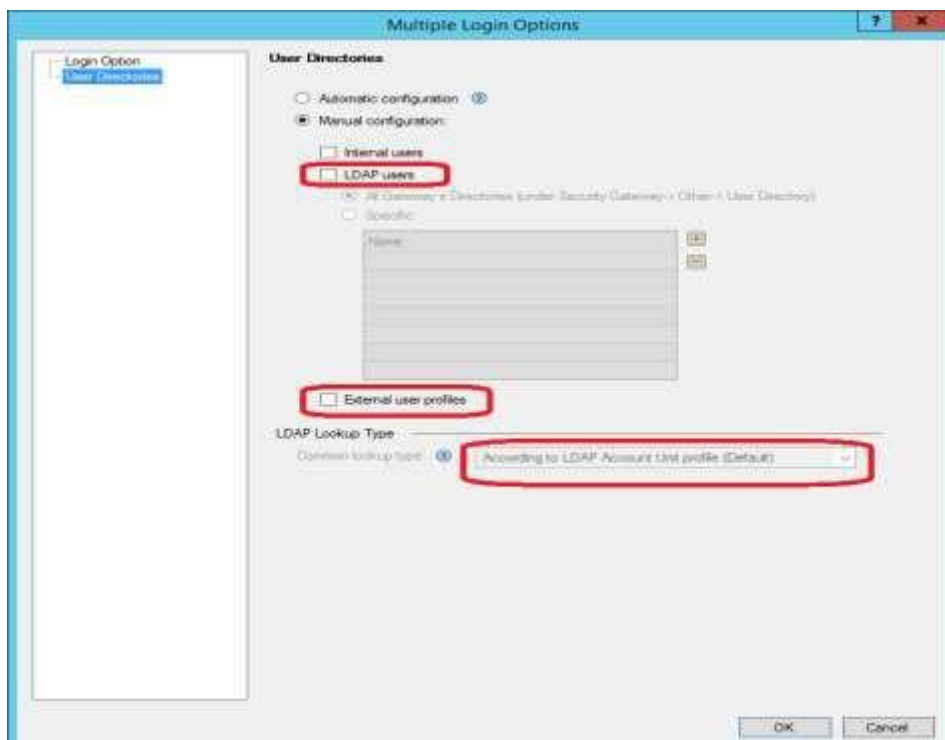


e) In the **Multiple Logon Options** window:

From the left, click **User Directories** and select **Manual configuration**.

There are two options:

- Option 1: If you do not want to use an on-premises Active Directory (LDAP), select only **External User Profiles** and click **OK**.
- Option 2: If you do want to use an on-premises Active Directory (LDAP), select only **LDAP users** and in the **LDAP Lookup Type** select **email**. Then click **OK**.



- f) Configure the required settings in the management database:
- i. Close the SmartConsole.
  - ii. Connect with the GuiDBEdit Tool to the Management Server (see [sk13009](#)).
  - iii. In the top left pane, go to **Edit > Network Objects**.
  - iv. In the top right pane, select the Security Gateway object.
  - v. In the bottom pane, go to **realms\_for\_blades > vpn**.

**Important Note:** If the attributes **do\_generic\_fetch** and **do\_internal\_fetch** do not exist under the attribute **fetch\_options**, then right-click the attribute **fetch\_options**, select **Edit**, and just click **OK**.



- vi. Configure the required settings
  - If **not** using LDAP:
    - Set the value of the **do\_internal\_fetch** to **false**
    - Set the value of the **do\_ldap\_fetch** to **false**
  - If **using** LDAP:
    - Select **userLoginAttr** and replace it with the applicable email
    - Set the value of the **do\_generic\_fetch** to **false**
- vii. Repeat the steps iv-vi for all applicable Security Gateways.
- viii. Save all changes (click the **File** menu > **Save All**).
- ix. Close the GuiDBEdit Tool.

- g) Each Security Gateway and each Software Blade have separate settings, similar to step "4-e" above.

Review the settings in each Security Gateway and each Software Blade that use authentication (VPN, Mobile Access, and Identity Awareness).

- Make sure to select the option **LDAP users** only for Software Blades that use LDAP.
- Make sure to select the option **External user profiles** only for Software Blades that do not use LDAP.

- h) Enable feature usage, make sure to do so only after all the Security Gateways have the required Jumbo Hotfix Accumulator installed:

- i. Download the required script from [sk172909](#):

```
allow_VPN_RA_for_R8040_and_above_gateways_V2.sh
```

- ii. Copy the script to the Management Server.  
iii. Connect to the command line on the Management Server.

Note - If this is a multi-Domain Server, make sure to connect to the IP address of the main Multi Domain Server.

- iv. Log in to the Expert mode.  
v. If this is a Multi-Domain Server, go to the MDS context. Run:

```
mdsenv
```



**Note** – If this is a Multi-Domain Server, and you do not want to enable SAML on all existing Domains, the run the “`mgmt_cli show domains`” API command and write down the UIDs of each domain.

- vi. Go to the directory where you put the script.  
vii. Assign the ‘execute’ permission to the script:

```
chmod -v u+x allow_VPN_RA_for_R8040_and_above_gateways_V2.sh
```



- viii. Run the script (the first argument must be "1"):

```
./allow_VPN_RA_for_R8040_and_above_gateways_V2.sh 1
```



**Note** – If the Management API is configured using a TCP port other than the default 443 (see output of the "api status" command), then use one of these options:

- Add the port number as the second argument to the script:

```
./allow_VPN_RA_for_R8040_and_above_gateways.sh 1 <Apache  
Port Number>
```

- Add '--port <Apache Port Number>' in the syntax of each **mgmt\_cli API** command in this script

- ix. The script prompts you to enter the username and password. Enter your SmartConsole credentials.
- x. When the script prompts you for the Domain UID:
- If you are working on a multi-Domain Server, and it is necessary to enable SAML only on one of the domains, then enter this domain's UID (see the output of the "mgmt\_cli show domains" API command).
  - If you are working on a Multi-Domain Server, and it is necessary to enable SAML on all existing domains (and in any other case), then leave this prompt empty, and press the Enter key.
- i) In SmartConsole, install the Access Control Policy on each Security Gateway.

## Step 5: Install and configure the Remote Access VPN client

- a) Install the required Remote Access VPN client for Windows OS or for macOS.
- b) **Optional:** Configure the Identity Provider browser mode. By default, the Windows OS client uses its embedded web browser, and the macOS client uses the Safari browser to authenticate in the Identity Provider's portal.

It is possible to configure the Windows OS client to use the Internet Explorer browser instead:

- i. On the Windows client computer, open a plain-text editor as an Administrator.
- ii. Open the **trac.defaults** file in a plain-text editor.
  - On 32-bit Windows:
 

```
%ProgramFiles%\CheckPoint\Endpoint
Connect\trac.defaults
```
  - On 64-bit Windows:
 

```
%ProgramFiles(x86)%\CheckPoint\Endpoint
Connect\trac.defaults
```
- iii. Change the value of the "**idp\_browser\_mode**" attribute from "**embedded**" to "**IE**":
- iv. Save the changes in the file and close the text editor.
- v. Open the Windows Command Prompt as an Administrator and run these commands to restart the Check Point Endpoint Security VPN client service:

```
net stop TracSrvWrapper

net start TracSrvWrapper
```

- c) **Optional:** Start authentication with a web browser running in the background.

By default, during authentication, the client opens the browser in the foreground to allow the user to authenticate in the Identity provider's portal.

Client can run the browser in the background, as user interaction might not be required. For example, in case the user is logged in already in the Identity Provider's portal. In case the user interaction is required, the browser is brought to the foreground, so the user can enter the credentials.

To enable the web browser to run in the background:

- i. On the client machine, open the **trac.defaults** file in a plain-text editor.

- On 32-bit Windows:

```
%ProgramFiles%\CheckPoint\Endpoint  
Connect\trac.defaults
```

- On 64-bit Windows:

```
%ProgramFiles(x86)%\CheckPoint\Endpoint  
Connect\trac.defaults
```

- On macOS:

```
/Library/Application Support/Checkpoint/Endpoint  
Security/Endpoint Connect/Trac.defaults
```

- ii. Change the value of the **"idp\_show\_browser\_primary\_auth\_flow"** attribute to **"false"**.

- iii. Save the changes in the file.

- iv. Restart the Check Point Endpoint Security VPN client service.

- On Windows clients:

Open the Windows Command Prompt as an Administrator and run these commands:

```
net stop  
TracSrvWrapper
```

```
net start  
TracSrvWrapper
```

- On macOS clients:

Open the Terminal and run these commands:

```
sudo launchctl stop com.checkpoint.epc.service
```

```
sudo launchctl start  
com.checkpoint.epc.service
```

## Step 6 (Optional): Configure the group authorization

Authorization can refer to two types of groups:

- **Identity Provider** groups - The groups that the Identity Provider sends.
- **Internal** groups - The groups, which are received from User Directories configured in SmartConsole (internal user groups or LDAP groups).

To configure the Identity Provider groups:

- a) Configure Azure roles according to:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-add-app-roles-in-azure-ad-apps>

Example of a new Azure role:

```
{
  "allowedMemberTypes": [ "User"
  ],
  "displayName": "my_group",
  "id": "<Enter the new unique GUID here>", "isEnabled":
  true,
  "description": "my_group", "value": "my_group"
```

- b) Configure a SAML claim on Azure:

Go to **Enterprise Applications > <Your SAML App> > SSO Settings** and add a new claim.

- i. In the **Name** field, enter **group\_attr**
- ii. In the **Source** attribute field, select **user.assignedroles**

- c) In SmartConsole, create an internal User Group object with this name (case- sensitive):

**EXT\_ID\_<Name\_of\_Azure\_Role>**

For example, for an Azure role with the name **my\_group**, create an internal User Group object with the name **EXT\_ID\_my\_group**.

**Note** – In this release, Identity Tags are not supported for Remote Access connections.

Both Identity Provider groups and Internal groups (for example, LDAP) are used for authorization.

There are two kinds of authorization:

- **Remote Access community** – Determines if a user can connect to VPN.

To apply this type of authorization, add the relevant group to the Remote Access VPN community.

- **Access Roles** (requires the Identity Awareness Software Blade)  
– Grants access to users based on policy rules and user identities.

To apply this type of authorization, add the relevant group to an Access Role in the Access Control Policy.

---

# Upgrade of a Security Management Server

**Upgrade only to versions that support this SAML for Remote Access VPN feature.**

To upgrade to the relevant Jumbo Hotfix Accumulator, use one of these alternatives:

- Perform an upgrade with CPUSE using a Blink image that contains the required Jumbo Hotfix Accumulator (or a Jumbo Hotfix Accumulator of a higher Take).

You can download the latest Blink image from [sk170114](#).

- Advanced Upgrade:
  - a. Perform an Advanced Upgrade using the commands described in [sk135172](#) in the "Advanced Upgrade Only" section.
  - b. Make sure to install the Jumbo Hotfix Accumulator on the target machine before performing the import action.

**Note:** Upgrading to a version without SAML for Remote Access VPN results in validation errors to the Identity Provider object, and SmartConsole crashes when trying to edit Security Gateway objects.

# Known Limitations

## *PC solution*

- The solution supports only IPsec VPN clients (not VPN GOST clients).
- All Remote Access VPN users and PCs (both managed and non-managed) must be defined in an Identity Provider for authentication.
- The SAML-based authentication flow presents an authentication method, where the Identity Provider issues the SAML ticket after one or multiple verification activities.
- SAML authentication cannot be used with more authentication factors in the same login option. Multiple Factor Authentication can be configured in the external IDP

The complexity and number of verification activities is subject to the configuration details of the Identity Provider (here, Azure Active Directory).

- For macOS and Windows PCs (managed and non-managed), Check Point Remote Access VPN client must be installed.
- Enforcing the identities acquired from remote access SAML authentication in the security rulebase is only possible on the VPN termination point.

Creating an identity-sharing infrastructure is subject to a dedicated planning session with the presales team.

- Connecting from a CLI to a realm with Identity Provider is not supported.
- Remote Access VPN client for ATMs is not supported.
- Supported web browsers are the VPN client's embedded browsers and Internet Explorer 11 (the latest version).
- Simultaneous Domain Login (SDL) with Identity Provider is not supported.

## *General*

- Customizations may be overwritten with standard functionality and the system stability cannot be guaranteed.
- Identity Tags are not supported for Remote Access connections.
- SAML for Remote Access VPN does not support:
  - Quantum Spark appliances with Gaia Embedded OS
  - Scalable Platforms (Maestro and Chassis)